# Bref aperçu du système des serveurs racine

Bureau du directeur de la technologie de l'ICANN

David Conrad
OCTO-010
6 mai 2020

ICANN

# TABLE DES MATIERES



Ce document fait partie de la série de documents de l'OCTO. Veuillez consulter la page de publication de l'OCTO
pour obtenir la liste des documents compris dans la série. Si vous avez des questions ou des suggestions sur ces documents, veuillez les envoyer à octo@icann.org.

*Un serveur racine répond aux premières questions du processus qui traduit les noms de domaine en adresses IP (Protocole Internet) ou autres données utilisées dans le fonctionnement de l'Internet.*

# 1 Processus de résolution du système des noms de domaine

Alors que les gens préfèrent utiliser des noms pour s'identifier, les ordinateurs utilisent généralement des numéros. Lorsque vous naviguez sur le Web, votre navigateur doit connaître les adresses IP, ou les numéros globalement uniques, des serveurs Web qui hébergent les sites Web que vous visitez. Après avoir saisi le nom de domaine d'un site Web dans la barre de navigation du navigateur ou cliqué sur un lien URL, le navigateur lance le processus de *résolution du DNS* pour trouver ces adresses IP.

Le navigateur envoie une question à un « résolveur », un logiciel qui met en œuvre le processus de résolution du DNS. Les résolveurs conservent une copie locale des réponses aux questions qu'ils ont précédemment recherchées, appelée *cache*, de sorte que le résolveur peut désormais être en mesure de répondre au navigateur sans besoin d'actions supplémentaires. Toutefois, si la réponse ne se trouve pas dans ce cache, une description de ce qui se passe lorsque le résolveur n'a pas de réponses dans son cache local illustre le processus complet de résolution du DNS. La première étape[1] est d'envoyer une question qui inclut le nom de domaine[2] du site Web à l'un des 13 serveurs racine[3], demandant la ou les adresses IP associées au site Web. Cependant, les serveurs racine contiennent uniquement des informations sur les domaines de premier niveau (TLD), en particulier une liste des TLD et des serveurs de noms qui hébergent le contenu, c'est-à-dire les noms de domaine de second niveau, dans ces TLD. Le serveur racine interrogé répond par une « référence », qui est une liste des serveurs de noms correspondant au TLD du nom du site Web. Par exemple, si vous essayez de visiter le site Web à l'adresse « www.example.com », votre résolveur enverra une requête à l'un des serveurs racine demandant l'adresse IP de ce nom de domaine et le serveur racine répondra avec une liste de tous les serveurs de noms pour « .com », le TLD de notre exemple.

1 Pour être techniquement précis, dans la plupart des cas, il y a une étape préalable. Lorsque le résolveur démarre, il lit (généralement) un fichier préconfiguré (appelé « fichier hints ») qui possède les 26 adresses IP (13 IPv4 et 13 IPv6) des 13 serveurs racine. Une fois ce fichier lu, le résolveur envoie une requête à l'une de ces adresses pour voir si les adresses des serveurs racine ont changé. Cette étape, appelée « requête initiale », est la façon dont les résolveurs disposent d'informations à jour sur les serveurs racine.

2 Une norme récente appelée « Minimisation du nom de la requête » (voir le RFC 7816) recommande que, pour améliorer la confidentialité, les résolveurs n'envoient que la partie du nom qui est pertinente pour les serveurs de noms demandés, par exemple, qu'ils n'envoient qu'une requête pour les serveurs de noms des TLD aux serveurs racine, le second niveau (avec le TLD) vers les serveurs de noms de TLD, etc. Les détails sur cette norme et son impact sont en dehors de la portée de ce document.

3 Un « serveur de noms » est un logiciel sur une machine qui répond aux requêtes DNS. Dans le cas des serveurs de noms racine, on les appelle souvent simplement les serveurs racine, même si un « serveur racine » est en fait un certain nombre de machines (comme cela sera décrit plus loin). Pour confondre un peu les choses, les résolveurs sont également appelés serveurs de noms, en particulier dans les routeurs domestiques et les divers fichiers de configuration, mais dans ce document, nous y ferons référence comme « résolveurs ».

L'étape suivante du processus de résolution consiste à envoyer la même question à l'un des serveurs de noms TLD qui ont été reçus dans la réponse de référence. De la même manière que les serveurs racine, les serveurs de TLD ne contiennent généralement que des informations sur les serveurs de noms pour les domaines dont ils sont responsables, dans le cas du serveur de TLD, les domaines de second niveau au sein du TLD. En tant que tel, et tout comme la requête qui a été envoyée au serveur racine, la requête au serveur de noms TLD entraînera une référence à la liste des serveurs de noms pour le domaine de second niveau de la question. En utilisant notre exemple précédent, le résolveur enverra une requête pour « www.example.com » à l'un des serveurs de noms « .com », demandant l'adresse IP de ce nom de domaine, et le serveur de noms « .com » répondra avec une liste de tous les serveurs de noms pour « example.com ».

Ce processus de résolution se poursuit jusqu'à ce qu'une requête soit envoyée à un serveur de noms qui ait la réponse, c'est-à-dire l'adresse IP du serveur Web, ou bien que le serveur de noms puisse déclarer avec autorité que le nom n'existe pas. Dans notre exemple, le résolveur enverrait une requête pour « www.example.com » à l'un des serveurs de noms « example.com », qui connaît vraisemblablement la ou les adresses IP associées à « www.example.com », et répondrait avec ces adresses.

Bien évidemment, chacune de ces étapes prend du temps, mais le cache local des réponses décrites ci-dessus accélère les choses : avant qu'une question soit envoyée à un serveur de noms, le résolveur vérifie dans son cache local pour voir si la même question a été posée récemment. Si c'est le cas, la réponse reçue la dernière fois que la question a été posée est renvoyée. Si ce n'est pas le cas, lorsque la réponse est renvoyée par le serveur de noms, elle est enregistrée dans un cache local de réponses et ce cache est examiné par le résolveur avant l'envoi d'une requête à un serveur de noms. Cette mise en cache est essentielle au succès du DNS. Pour ajouter plus de complexité, si les extensions de sécurité des noms de domaine (DNSSEC) ont été activées, le résolveur vérifie les signatures cryptographiques sur les données qu'il reçoit pour vérifier que les données n'aient pas été modifiées par un attaquant.

# 2 Le système des serveurs racine

Comme on peut le voir ci-dessus, le rôle des serveurs racine (fondamentalement, de répondre à la première étape du processus de résolution) est assez limité. Toutefois, malgré ce rôle limité, les serveurs racine sont essentiels au fonctionnement de l'Internet. Sans la possibilité d'obtenir la référence initiale fournie par les serveurs racine, il ne serait pas possible de rechercher des noms de domaine sur Internet[4].

Le système de serveurs racine comprend plus de 1000 machines individuelles (appelées « instances » de serveur racine), qui contiennent des données de la racine du DNS. Ces instances répondent aux requêtes des résolveurs d'Internet par des renvois vers les serveurs de noms pour les domaines de premier niveau, comme indiqué précédemment.

[4] Certains opérateurs de réseau utilisent des techniques telles que celles décrites dans le RFC 7706 (https://tools.ietf.org/html/rfc7706) ou similaires pour faire une copie locale de la racine de sorte que leurs résolveurs n'aient pas besoin d'interroger les serveurs racine. Cependant, le déploiement de ces techniques demeure relativement rare et hors de la portée du présent document.

Douze organisations, appelées « opérateurs de serveur racine », administrent 13 « identités »[5], chacune portant les lettres « a » à « m » dans le domaine « root-server.net »" c'est-à-dire « a.root-servers.net » à « m.root-servers.net ». Chacune de ces identités de serveur racine, connues sous le nom de services racine, a deux adresses IP uniques associées, une adresse IPv4 et une adresse IPv6. Ces adresses IP sont préconfigurées dans tous les résolveurs sur Internet, ce qui leur permet de trouver les services racine pour les interroger. Et les services racine reçoivent un grand nombre de ces questions : plus de 70 milliards par jour.

Les 13 services racine répondent aux requêtes qu'ils reçoivent soit avec des informations trouvées dans la zone racine, car elles sont gérées par les fonctions IANA exploitées par l'ICANN, soit dans le cas où le TLD interrogé n'a pas été délégué, un message indiquant que le nom n'existe pas. Ces informations sont protégées par les DNSSEC : toute modification des données par qui que ce soit permettra que les résolveurs DNSSEC activés ignorent la réponse, empêchant ainsi la modification de la zone racine ou les attaques qui tentent d'insérer des informations non authentiques dans une réponse.

La résilience du système de serveurs racine est essentielle car le système doit être capable de répondre à un vaste flux de questions et de résister à diverses cyberattaques. Les opérateurs de serveur racine ont satisfait à cette exigence de résilience en distribuant des instances de serveur racine dans le monde entier à l'aide d'une technique de routage appelée *anycast.* Le routage anycast permet aux machines connectées à l'Internet d'utiliser les mêmes adresses IP pour fournir des réponses identiques, permettant ainsi aux instances de serveur racine d'être situées dans des centaines de villes et de pays différents. Aujourd'hui, avec le grand nombre d'instances de serveur racine autour du monde entier, le système des serveurs racine est extrêmement résilient. Pour plus d'informations sur la distribution des instances des serveurs racine, consultez le site https://root-servers.org.

# 3 Implication de la communauté de l'ICANN

L'un des comités consultatifs de l'ICANN, le Comité consultatif du système des serveurs racine (RSSAC), est composé d'opérateurs de serveur racine, ainsi que d'autres. Le RSSAC conseille le Conseil d'administration de l'ICANN sur des questions liées au fonctionnement, à la gestion, la sécurité et l'intégrité du système des serveurs racine de l'Internet. Le RSSAC nomme également des experts intéressés de l'industrie au Caucus RSSAC, un groupe qui produit des documents du RSSAC, y compris des rapports et des avis. Pour plus d'informations sur le RSSAC et le Caucus RSSAC, consultez le site https://www.icann.org/groups/rssac ; une liste des documents produits par le RSSAC est disponible à l'adresse https://www.icann.org/groups/rssac/documents.

# 4 Mon organisation peut-elle demander une instance anycast de serveur racine ?

[5] Pour des raisons (principalement) historiques, il existe une organisation qui administre deux identités.

Un certain nombre d'opérateurs de serveurs racine ont des programmes qui vous permettent de déployer une instance de serveur racine localement. Vous trouverez une liste des opérateurs des serveurs racine à l'adresse https://root-servers.org.

L'hébergement d'une instance de serveur racine bénéficie les utilisateurs de grands réseaux tels que les fournisseurs de services Internet (FSI) et les réseaux de grandes entreprises, et contribue à améliorer la sécurité, la stabilité et la résilience de l'infrastructure DNS de l'Internet dans le pays et/ou la région. L'un des avantages de l'hébergement d'une instance de serveur racine est qu'elle peut réduire les temps de réponse aux requêtes DNS pour vos réseaux, en particulier pour les noms qui n'existent pas, et peut réduire l'utilisation de la bande passante pour les requêtes DNS qui seraient autrement envoyées aux instances de serveur racine en dehors de votre réseau.

# 5 Le rôle de l'organisation ICANN

Au-delà de l'opération des fonctions IANA qui (entre autres activités) met à jour la zone racine qui est distribuée aux 13 services racine, sur le plan opérationnel, l'organisation ICANN administre l'une des 13 identités de serveur racine (« l.root-servers.net »), connue sous le nom de serveur racine géré par l'ICANN (IMRS), et participe aux discussions entre les opérateurs de serveur racine. En outre, l'organisation ICANN soutient le RSSAC dans ses délibérations sur les politiques et autres activités et le Caucus RSSAC dans son travail.

Pour aider à maintenir une infrastructure DNS sécurisée, stable et résiliente, l'organisation ICANN encourage les organisations qui répondent à certains critères opérationnels à déployer une instance de serveur racine gérée par l'ICANN. Pour plus d'informations sur l'hébergement d'une instance anycast d'un serveur racine géré par l'ICANN (IMRS), veuillez consulter https://www.dns.icann.org/imrs/faq/.