Note : ce contenu est la traduction en français du document publié dans sa version originale en anglais sur ***icann.org***. Seule fait foi la version originale en langue anglaise, sur ***icann.org***.

FAQ DU RSSAC

Cette page apporte des réponses à bon nombre des questions les plus fréquemment posées sur le RSSAC. Elle sera mise à jour dès lors que les réponses changent ou dès que de nouvelles questions deviennent récurrentes.

Si vous avez une question qui ne figure pas ci-dessous, ou si vous voulez obtenir des informations complémentaires ou des précisions, vous pouvez envoyer un e-mail directement à ask-rssac@icann.org. Si vous souhaitez évoquer une question de cette FAP, veuillez inclure le numéro et le titre de la question dans votre e-mail.

Liste de sujets

1. Nombre d'opérateurs

1.1 Pourquoi y a-t-il 13 serveurs de noms racine ?

En 1985, il y avait quatre serveurs racine. Entre 1987 et 1991, il y en avait sept, tous situés aux États-Unis. En 1993, il y en avait huit. À ce moment-là, un problème s'est posé. Le RFC 1035 stipule que « les messages du [DNS] transmis par l'UDP sont limités à 512 octets ». Ajouter plus de serveurs de noms racine engendrerait une réponse initiale supérieure à 512 octets. Le RFC 1035 ne fournit pas de justification à la limite de 512 octets, mais il convient aussi de noter qu'à l'époque, il existait une norme commune imposant aux paquets IP sur Internet d'être limités à 576 octets.

Les opérateurs de serveurs racine se sont rendu compte que davantage de serveurs racine pourraient être ajoutés s'ils pouvaient tirer profit de la compression des noms du DNS. Ainsi, il a été proposé de donner des noms aux serveurs racine dans la zone root-servers.net. En 1995, les neuf serveurs racine existants ont été renommés « a.root-servers.net », « b.root-servers.net », et ainsi de suite. En 1997, quatre autres serveurs racine ont été ajoutés, portant le nombre total d'identificateurs de serveur racine (RSI) à 13.

Jusqu'en 1998, c'est Dr. Jon Postel, en sa qualité d'administrateur de l'IANA, qui était chargé de désigner les opérateurs de serveurs racine. Après son décès en 1998, le nombre d'opérateurs n'a pas bougé, bien qu'un petit nombre d'entre eux ait changé de mains au fil des ans.

Depuis 1998, le paysage a été modifié de plusieurs façons. Chaque serveur racine a ajouté sa propre adresse IPv6, et l'ICANN a signé la zone avec les extensions de sécurité DNS (DNSSEC). De même, la taille des messages transmis sur l'UDP a augmenté à l'aide de l'extension de protocole EDNS (mécanismes d'extension pour le DNS). Toutes ces changements ont fait perdre de l'importance à la limite de 512 octets de l'UDP et à la limite de 13 RSI.

En 2002, Internet Software Consortium (ISC, désormais Internet Systems Consortium) est devenu le premier opérateur de serveur racine à déployer l'adresse anycast IP, même si le projet WIDE avait déjà expérimenté cette technologie. Au fil des ans, les autres opérateurs de serveurs racine en ont fait de même. Anycast permet à chaque opérateur de fournir le service à partir de multiples instances distinctes. Alors qu'il reste aujourd'hui 13 RSI, il y a en fait plus de 1000 instances anycast en activité à travers le monde.

Afin de mieux comprendre l'histoire du système des serveurs racine (RSS), veuillez consulter le RSSAC023v2 : Histoire du système des serveurs racine. Si vous souhaitez en savoir davantage sur l'évolution continue du RSS, veuillez consulter le RSSAC037 : Proposition de modèle de gouvernance pour le système des serveurs racine du DNS.

1.2 Quelle logique justifiait la limite de 13 identificateurs de serveurs racine ?

En 1997, les serveurs racine faisaient également office de serveurs faisant autorité pour les zones .COM, .NET et .ORG, et cette fonction supplémentaire limitait considérablement le nombre potentiel de RSI. Tout comme avec la requête initiale pour la zone racine, l'envoi d'une requête au NS RRSET pour les zones .COM, .NET et .ORG ne pouvait dépasser la limite de 512 octets, et comme les mêmes serveurs desservaient ces zones, la même limite s'appliquait à tous.

Un paquet de réponses DNS contient également l'ensemble de la question posée dans la section Question. Une réponse à une requête initiale racine utilisera toujours 5 octets pour la section Question. Le QNAME utilise 1 octet, et le QTYPE et le QCLASS utilisent chacun 2 octets, pour un total de 5 octets. Toutefois, pour une requête initiale .COM, la section Question pourrait être bien plus grande.

Finalité	**Octets**
En-tête DNS	12
Premier enregistrement NS	31

12 Enregistrements NS compressés	(12 * 15) 180
13 Enregistrements A	(13 * 16) 208
Section Question QTYPE et QCLASS	4
Section Question QNAME	?
	=
	435

Tableau 1 : Explication des octets utilisés dans la réponse initiale racine

Avec 435 octets en fonctionnement, 77 octets étaient alors disponibles pour la section Question QNAME. À ce moment-là, il était déterminé que 64 octets seraient suffisants pour prendre en charge la plupart des requêtes envoyées pour .COM, .NET et .ORG. L'ajout d'un autre serveur requerrait 25 octets, et comme 435 + 64 + 25 > 512, il a été décidé de ne pas ajouter un autre serveur.

2. **Anycast**

2.1 Pourquoi certains opérateurs possèdent de nombreuses instances anycast alors que d'autres en ont peu ?

Les opérateurs de serveurs racine (RSO) sont des organisations indépendantes avec des mandats différents, des modèles opérationnels différents et différentes sources de financement. Ces différences peuvent avoir un impact sur le nombre d'instances anycast ainsi que sur d'autres choix opérationnels. Les opérateurs de serveurs racine disposent d'une grande indépendance dans leur mode de déploiement de leur réseau. Voir le RSSAC042 : Déclaration du RSSAC sur l'indépendance des opérateurs de serveurs racine. Tous les RSO s'engagent à fournir un service de zone racine du DNS de qualité.

2.2 Comment s'assurer que la zone racine est dûment reproduite ? Est-il possible que les fichiers de zone racine soient corrompus par une attaque ou un logiciel malveillant ?

Le transfert du fichier de zone racine du responsable de la maintenance de la zone racine (RZM) aux RSO s'effectue via les protocoles de transfert de zone de DNS (AXFR dans le RFC 5936 et IXFR dans le RFC 1995). Ces messages de transfert de zone sont protégés par l'utilisation d'enregistrements de ressources TSIG tel que décrit dans le RFC 2845. Il s'agit d'un protocole fiable et aucun cas de corruption de données n'a été recensé jusqu'à présent. En outre, la zone racine étant signée, des réponses incorrectes ou falsifiées peuvent être détectées

par des validateurs des DNSSEC. Lorsque cela est possible, le RSSAC encourage le recours à la validation des DNSSEC.

2.3 Le nombre de nœuds anycast est-il ou non limité ?

Le fonctionnement anycast est défini et décrit dans le RFC 4786 « Fonctionnement des services anycast » et dans le RFC 7094 « Considérations architecturales liées à Anycast IP ». Il n'y a pas de limite intrinsèque au nombre de nœuds dans un service anycast.

2.4 Les serveurs racine reproduisent la zone racine faisant autorité et la republie, puis les instances anycast republient les données des serveurs. Quelle est la différence entre ces deux types de republication ?

Les RSO reçoivent les données de la zone faisant autorité du responsable de la maintenance de la zone racine (RZM). Chaque RSO utilise alors son propre système de distribution interne afin de transmettre la zone à l'ensemble de ses sites et instances anycast.

2.5 Nous hébergeons l'instance anycast d'un serveur racine dans une municipalité. Nous observons qu'elle répond à des requêtes des quatre coins de la planète. Que dois-je faire afin qu'elle ne réponde qu'à des requêtes provenant de l'environnement local ?

Cela dépend du routage IP et de la façon dont le RSO exploite son service anycast. Certains RSO configurent leurs routeurs et leurs sessions d'appairage de sorte que l'instance anycast ne reçoit que du trafic local. D'autres les configurent de sorte à recevoir le trafic global, en se reposant sur le système de routage pour choisir le meilleur chemin d'accès au réseau. Si vous observez des comportements indésirables de la part d'un serveur hébergé, vous devez en discuter avec le RSO assurant la fourniture du service.

2.6 En 2016, s'est produite une attaque de grande envergure sur Dyn. Les instances anycast du serveur racine pourraient-elles subir une attaque du même type ?

Oui, au moins en théorie. C'est l'une des raisons pour lesquelles le RSS a de nombreux opérateurs et de nombreuses instances du serveur racine. Un nombre élevé d'instances anycast augmente la capacité du RSS et est d'une grande aide en cas d'attaque.

2.7 Comme faire une demande d'instance anycast d'un serveur racine pour mon organisation ?

Veuillez contacter directement les opérateurs de serveur racine dont les coordonnées sont indiquées ci-dessous. De la même façon que pour la question 3.4, vous pouvez aussi envisager d'exploiter une copie locale de la zone racine, tel que décrit dans le RFC 7706, sans faire officiellement partie du système anycast de serveur racine.

Cogent Communications	
Département de la défense des États-Unis (NIC)	
ICANN	https://www.dns.icann.org/imrs/host/
Internet Systems Consortium, Inc.	https://www.isc.org/f-root/hosting-an-f-root-node/
Centre de recherche Ames de la NASA	
Netnod	https://www.netnod.se/i-root/i.root-servers.net
RIPE NCC	https://www.ripe.net/analyse/dns/k-root/hosting-a-k-root-node
Université du Maryland	
Université de Californie du Sud, Institut des sciences de l'information	https://b.root-servers.org/
Laboratoire de recherche de l'armée des États-Unis	
Verisign, Inc.	https://www.verisign.com/rirs
Projet WIDE	

3. **DNS et mise en réseau**

3.1 Comment les serveurs récursifs choisissent-ils le serveur racine à interroger, et quel identificateur de serveur racine mon serveur récursif devrait-il privilégier ?

On appelle ça « l'algorithme de sélection du serveur ». Le protocole DNS ne précise pas comment un serveur de nom récursif doit choisir parmi un ensemble pour une requête donnée. Ainsi, chaque fournisseur de logiciel récursif détermine son propre algorithme de sélection du serveur. Certaines mises en œuvre de résolveurs se « bloqueront » sur le serveur avec le moins de temps d'attente, ou sur l'un des serveurs ayant un temps d'attente similaire au serveur le plus rapide. Certaines mises en œuvre de résolveurs choisissent toujours le serveur de manière aléatoire, et d'autres distribuent les requêtes en se fondant sur des formules complexes. Un rapport de 2012 décrit l'algorithme de mises en œuvre prisées à cette époque.

Il est probablement plus fiable de laisser votre logiciel récursif faire le travail pour lequel il a été conçu que d'essayer de l'influencer afin de privilégier ou d'éviter certains serveurs.

3.2 Nous savons que le DNS fonctionne sur l'UDP 53, pouvez-vous nous expliquer quand le DNS fonctionne sur le TCP 53 ?

Presque tous les clients DNS utilisent par défaut le transport UDP pour les requêtes. Toutefois, dans certains cas, c'est le TCP qui doit être utilisé.

Le plus souvent, on a recours au TCP lorsqu'une réponse UDP est tronquée. Une telle troncation survient lorsque la réponse d'un serveur est trop grande pour tenir dans un seul message UDP. Cela dépend de la mémoire tampon UDP spécifiée du client et de toute limite de mémoire tampon que le serveur peut s'imposer. Lorsqu'un client reçoit une réponse avec l'ensemble de bits tronqué, le protocole DNS invite à retenter la requête sur le TCP afin d'obtenir la réponse complète.

Le TCP pour le DNS est également utilisé pour les transferts de zone. Comme l'ensemble des zones est généralement bien plus grand que la limite autorisée pour un seul message UDP, il est logique d'effectuer ces transferts sur le TCP.

Le TCP peut aussi entrer en jeu lorsqu'un serveur fait l'objet d'une attaque. Le serveur peut envoyer aux clients des réponses tronquées afin de déterminer si oui ou non il s'agit de sources frauduleuses. Les clients qui établissent des connexions TCP peuvent être qualifiés de sources non frauduleuses. De plus, via la technique de limitation du taux de réponse (RRL), des réponses tronquées seront de temps en temps envoyées afin que les clients légitimes aient la possibilité de recevoir des réponses sur le TCP, tandis que le trafic d'attaque ne fera pas de nouvelle tentative.

Il est obligatoire de mettre en œuvre le DNS sur TCP dans les logiciels DNS. Pour plus d'informations, veuillez consulter le RFC 7766.

3.3 Comment réduire le temps d'attente entre le serveur récursif que j'exploite et un serveur racine ?

Premièrement, vous devez procéder à un examen minutieux vous permettant de déterminer s'il est réellement avantageux d'être plus proche de (plus de) serveurs racine. Analysez le trafic sortant de votre serveur de nom récursif pour des requêtes qui sont envoyées à des serveurs de noms racine. Si vous observez plus de trafic que prévu, vous pouvez régler vos applications ou les configurations de votre réseau afin qu'ils n'aient pas à interroger la racine si souvent. Utilisez des programmes tels que l'utilitaire « dig » afin de mesurer les temps d'attente réels. Si le temps d'attente d'au moins deux serveurs racine est inférieur ou égal à 100 millisecondes, cela est en général suffisant.

Utilisez des outils tels que « traceroute » afin d'explorer le chemin d'accès réseau entre votre serveur récursif et les serveurs racine que votre serveur de nom récursif utilise. Si quelque chose vous semble illogique (par exemple un routage vers des emplacements éloignés), demandez à votre FSI si le routage peut être ajusté.

Pour de plus amples informations sur les mesures de la qualité de service du DNS, le projet

Atlas du RIPE (Réseaux IP européens) assure un suivi de la qualité du service racine avec son projet DNSMON. Le temps d'attente de la plupart des serveurs tel que mesuré par des centaines d'ancres RIPE Atlas est inférieur à 60 ms.

S'il n'y a pas de serveurs racine raisonnablement proches, vous pouvez alors essayer d'identifier un point d'échange ou un centre de traitement de données proche où pourrait se trouver un serveur racine. Demandez à un ou plusieurs des opérateurs de serveurs racine s'ils souhaiteraient y placer un serveur. Toutefois, notez que si un emplacement a déjà un serveur racine, les opérateurs ne veulent en général pas en placer un autre. Vous pouvez trouver des coordonnées d'opérateurs en vous rendant sur http://www.root-servers.org et en appuyant sur les boutons « E-mail » dans la section Serveurs racine en bas de page.

3.4 Pouvez-vous configurer un serveur racine vous-même en téléchargeant le fichier de zone racine et en validant la signature vous-même ?

Le RFC 8806 décrit comment s'y prendre tout en mettant en garde contre les éventuels inconvénients liés à cette pratique. Veuillez noter que la validation des DNSSEC est requise. Consultez aussi le LocalRoot Project.

3.5 Pendant combien de temps un serveur récursif mettra en cache les informations ?

Chaque enregistrement DNS à un temps à vivre (TTL) qui lui est attribué par l'opérateur de la zone. Cela détermine la durée pendant laquelle un serveur de nom récursif ou un autre client doit mettre en cache les données à des fins de réutilisation. À l'issue de cette période, le serveur de nom récursif doit contacter de nouveau le serveur faisant autorité pour obtenir des données à jour.

Dans le cas de la zone racine, certains enregistrements sont servis avec un TTL de 24 heures et d'autres avec un TTL de 48 heures. Certains résolveurs ont des durées de vie de mise en cache maximums, en général 24 heures.

3.6 La mise en cache donnant de fausses informations après un certain temps, comment un résolveur peut-il être mis à jour avec les informations correctes du DNS ?

Si vous pensez que les données d'un cache d'un serveur de nom récursif sont obsolètes, vous pouvez vous débarrasser de son cache ou redémarrer le processus du serveur.

3.7 Que sont les requêtes et réponses initiales du DNS ?

Les résolveurs récursifs du DNS doivent lancer leurs caches avec des données spécifiques de la zone racine avant de pouvoir commencer à répondre à des requêtes régulières. Le RFC 8109 décrit quelles requêtes les résolveurs récursifs envoient et les réponses qu'ils attendent des serveurs racine.

4. **DNSSEC**

4.1 Les DNSSEC peuvent-elles protéger contre les attaques fast flux ?

Pas vraiment. Les DNSSEC sont conçues afin de protéger contre la falsification de données, pas contre les attaques fast flux.

4.2 Avec les DNSSEC, est-il plus compliqué de transmettre une copie de la zone racine au niveau local ?

Non, transmettre une copie locale de la zone racine signifie simplement transmettre des copies à jour de la zone racine sans changements. La zone racine provient du responsable de la maintenance de la zone racine (RZM) avec toutes les signatures DNSSEC requises en place.

Pour de plus amples informations sur la façon de transmettre la zone racine au niveau local, consultez la question 3.4 et le RFC 8806.

4.3 On dirait que le DNS sur UDP est limité à 512 octets et que le DNS sur TCP est limité à 4096 octets. Si je signe ma zone, la taille dépassera peut-être la MTU. Sera-t-elle alors effacée par un pare-feu ?

Le DNS sur UDP n'est plus limité à 512 octets. Les mécanismes d'extension pour DNS (EDNS), décrits dans le RFC 2671 avant d'être mis à jour dans le RFC 6891, définissent la façon dont les clients et les serveurs peuvent prendre en charge des messages d'une taille supérieure à 512 octets.

Le TCP n'a jamais été limité à 4096 octets. Il est conçu pour fournir des données de taille arbitraire.

Il existe des craintes légitimes concernant la taille des réponses signées. Lorsqu'une réponse DNS sur UDP dépasse la taille MTU du réseau, elle est fragmentée. On considère qu'il existe alors un risque d'empoisonnement du cache qui porterait atteinte à la sécurité. Certains pare-feux bloqueront ces fragments. De ce fait, des résolveurs récursifs modernes sont conçus afin d'utiliser des mémoires tampons EDNS inférieures, et de retenter les requêtes avec des mémoires tampons plus petites. Lorsque la mémoire tampon devient assez petite, le serveur de nom récursif recevra soit une réponse non fragmentée soit une réponse avec l'ensemble de bits tronqué, indiquant qu'il doit retenter sur le TCP.

5. **RSSAC**

5.1 En quoi sont liés le RSSAC et le RZERC ? Le RZERC est-il un sous-ensemble du RSSAC ?

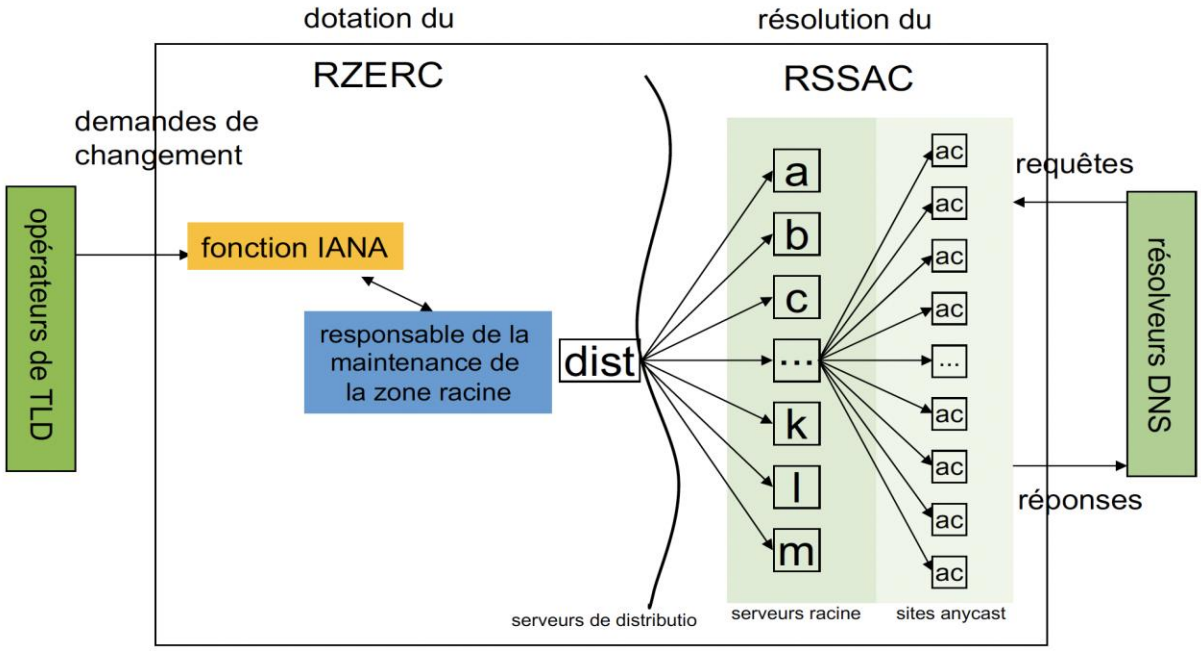
Le Comité consultatif du système des serveurs racine (RSSAC) et le Comité de révision de

l'évolution de la zone racine (RZERC) sont des comités distincts au sein de l'ICANN, bien qu'il existe des liens entre eux et qu'il soit possible de siéger aux deux comités.

En vertu de sa charte, le RSSAC :
« ...conseille le Conseil d'administration de l'ICANN et la communauté sur des questions liées au fonctionnement, à la gestion, à la sécurité et à l'intégrité du système des serveurs racine. »
Pour de plus amples informations sur le rôle du RSSAC, veuillez consulter le [RSSAC033 : Déclaration du RSSAC sur la distinction entre RSSAC et Root-Ops].

En vertu de sa charte, le RZERC :
« doit examiner les changements architecturaux proposés au contenu de la zone racine du DNS, aux systèmes (matériel et logiciel) utilisés pour modifier la zone racine du DNS et aux mécanismes utilisés pour la distribution de la zone racine du DNS. »

Le schéma suivant aide à comprendre les rôles de chaque groupe.



5.2 Existe-t-il une date à laquelle nous pouvons connaître le nombre de serveurs racine que le RSSAC souhaite avoir ? Quand l'évaluation sera-t-elle menée afin de déterminer le nombre de lettres ?

Le RSSAC n'a pas d'avis arrêtés sur le nombre de serveurs racine ou le nombre de RSO qu'il devrait y avoir. La limite actuelle du nombre d'opérateurs est technique et non pas administrative.

6. **RSSAC Caucus**

Des informations sur le Caucus RSSAC sont disponibles sur sa page web principale.

6.1 Existe-t-il une limite au nombre de membres du Caucus RSSAC ?

Non.

6.2 Quel temps les membres du Caucus RSSAC doivent-ils consacrer à ces activités ?

Les membres du Caucus RSSAC doivent participer aux équipes de travail et à la liste de diffusion du Caucus RSSAC. Certains membres pourront consacrer plus de temps que d'autres, et certaines équipes de travail et révisions de documents requièrent plus de temps que d'autres. Toutefois, le RSSAC souhaite, de manière générale, que ses membres consacrent au moins 4 heures par mois aux activités du Caucus.

7. Idées reçues courantes

Pour une présentation du mode de fonctionnement du DNS, veuillez consulter Le système des noms de domaine d'Internet expliqué aux profanes de Daniel Karrenberg.

7.1 Les serveurs racine contrôlent-ils la destination du trafic d'Internet ?

Non, les routeurs et le protocole BGP déterminent le chemin d'accès que les paquets empruntent jusqu'au réseau, entre le point de départ et le point d'arrivée. Le DNS fournit un mappage des noms axés sur l'humain vers les adresses IP, et ce sont ces adresses IP que les routeurs utilisent en fin de compte pour déterminer la destination des paquets.

7.2 La plupart des requêtes DNS sont-elles traitées par un serveur racine ?

Non, la plupart des requêtes DNS sont traitées par des résolveurs récursifs sans interaction avec un serveur racine à partir des données qu'ils possèdent déjà dans leurs caches. Un résolveur récursif interagit uniquement avec un serveur racine s'il a des informations arrivées à expiration relatives aux domaines de premier niveau ou aux racines mêmes dans son cache. Presque toutes les requêtes reçues par les serveurs racine engendrent une réponse de renvoi qui indique au serveur de nom récursif où il doit maintenant poser sa question.

7.3 Y a-t-il des identificateurs de serveur racine qui ont des significations spécifiques ?

Aucun identificateur de serveur racine n'est spécial.

7.4 N'y a-t-il que 13 serveurs racine ?

Il y a plus de 1000 serveurs dans le monde, mais uniquement 13 identificateurs de serveur racine (RSI), chacun d'entre eux utilisant une adresse IPv4 et une adresse IPv6 et un routage

anycast.

7.5 Les opérateurs de serveurs racine mènent-ils leurs activités en toute indépendance ?

Les RSO mènent leurs activités en toute indépendance, mais une coordination étroite entre eux est assurée par le RSSAC et d'autres forums. Pour plus d'informations, consultez le RSSAC042 : Déclaration du RSSAC sur l'indépendance des opérateurs de serveurs racine.

7.6 Les serveurs racine ne reçoivent-ils que la partie TLD de la requête DNS ?

Actuellement, les serveurs racine (et de fait tous les serveurs DNS) reçoivent en général l'intégralité du nom de requête dans la requête DNS. Toutefois, de nouveaux efforts sont en cours afin de n'envoyer, lorsque cela s'avère nécessaire, que la partie TLD du nom de domaine aux serveurs racine.

En 2016, l'IETF a publié le RFC 7816, qui décrit la façon dont les serveurs DNS récursifs peuvent envoyer uniquement la partie la plus infime nécessaire du nom de requête. On appelle cela la minimisation du nom de requête ou minimisation QNAME. Avec la minimisation QNAME, des serveurs DNS récursifs n'envoient que les parties nécessaires d'un nom de domaine aux serveurs qu'ils interrogent. Les serveurs DNS récursifs qui ont recours à la minimisation QNAME ne doivent envoyer que la partie TLD de la requête des serveurs racine. Cela minimise la quantité d'informations sur le réseau et renforce donc la protection de la vie privée des utilisateurs interrogeant le DNS. En 2020, la minimisation QNAME est relativement récente et pas encore largement mise en œuvre.