ICANN85 Mumbai | Forum de la communauté – Comment ça marche : les opérations du serveur racine
Mardi 10 mars 2026 – 15h00 à 16h00 IST

JENNIFER BRYCE

Bonjour et bienvenue à cette séance qui s'intitule, comment cela fonctionne? Opération des serveurs racine. Je m'appelle Jennifer et je suis responsable de la participation à cette séance. Sachez que cette séance est enregistrée et qu'elle est régie par les normes de comportement attendues de l'ICANN et par les politiques anti harcèlement. Il y a des règles qui seront affichées donc dans le chat. Les questions qui sont donc posées de la façon appropriée seront lues. Si vous souhaitez prendre la parole, veuillez lever la main sur Zoom ou veuillez attirer mon attention pour que je vous donne la parole. Lorsque vous prendrez la parole, veuillez vous exprimer à un débit modéré. Veuillez indiquer votre nom. Sur ce, je donne la parole à Ken. Merci.

KEN RENARD

Merci et bienvenue à cette séance d'information sur le système des serveurs racines. Je suis donc dans l'équipe H-Root. J'encourage les questions. Nous pouvons passer à la diapositive suivante de l'ordre du jour.

Aujourd'hui, nous allons parler du système de nom de domaine et de Anycast, et c'est une des raisons pour lesquelles le système est

résistant. Nous allons parler donc de ce système des serveurs racines. Nous allons parler du RSSAC, du caucus RSSAC et nous allons aussi parler de la façon dont vous pouvez utiliser le système, dont vous utilisez le système. Passons aux diapositives suivantes. Pour commencer, tout d'abord, je m'excuse si vous connaissez déjà tout cela. C'est bien d'avoir quand même les fondamentaux du fonctionnement du DNS et de comprendre comment s'intègre le système des serveurs racines.

Et donc, les adresses IP, ce sont les identificateurs sur Internet. En général, on voit des numéros, des chiffres. En fait, ce sont des séries de uns et de zéros. Et c'est ainsi que les ordinateurs échangent les uns avec les autres. C'est un petit peu comme un numéro de téléphone. Actuellement, nous ne connaissons plus le numéro de téléphone des gens. On clique simplement sur un bouton. Mais en général, c'est comme ça que cela fonctionne avec ces séries de numéros. Diapositive suivante. Le DNS a été déployée en 1984, je crois, et le problème qu'on cherchait à résoudre initialement, c'est que ces adresses IP sont difficiles à retenir. Et par exemple, je ne me souviens plus de ce que j'ai mangé au petit déjeuner, alors je ne vais pas me souvenir de ces longues adresses. Mais le problème, c'est que l'Internet a évolué et un ordinateur, une adresse IP peut donc s'appliquer à cinq, dix ou cent serveurs web différents. Et donc, il y aura des noms DNS différents. Donc, le DNS nous aide à résoudre ces problèmes-là. Diapositive suivante.

Ici, nous voyons quelque chose de très familier, et il y a donc la hiérarchie de l'espace des noms. Il y a la racine, ensuite le domaine

de premier niveau, on a .uk, .org. Les différents types de caractères. Ces domaines de premier niveau, deuxième niveau, troisième niveau. L'objectif principal, c'est de cartographier ce nom, comme par exemple www.example.org et de convertir cela en adresse IP. Il y a de nombreux usages du DNS, par exemple l'IPv6. Donc, ce sont des serveurs d'adresses email. Il y a des clés chiffrées. Sur ce, passons aux diapositives suivantes. Ici, il y a le processus de résolution des noms de domaine.

Dans cette séance, nous allons utiliser le diagramme que l'on retrouve dans tous les ouvrages. Vous retrouvez cette image assez souvent. Elle est très simple. Et, je vais vous parler de cette image et de ce qu'elle signifie vraiment. Cela commence par un appareil d'utilisateur final. Cela peut être votre téléphone, votre ordinateur portable, votre grille-pain, votre frigo, tout ce qui est configuré, tout ce qui est connecté à l'Internet est donc un appareil de l'utilisateur final qui est connecté au DNS. Donc, il y a ici un résolveur récursif. Il peut y en avoir un ou plus dans le réseau de votre organisation. Donc, la configuration est automatique. Ce résolveur DNS, il y en a des milliers, des millions dans le monde. Et, bien, c'est le DNS en lui-même. Donc, ce résolveur récursif, vous lui demandez quelle est l'adresse www.example.com?

Diapositive suivante. Ici, c'est quelque chose qui nous induit en erreur dans les ouvrages. On nous dit qu'il faut aller au serveur racine faisant autorités qui nous demandent quel est ce www.exemple.com. Et, nous nous disons nous ne savons pas et on sait simplement où se trouve .com. L'étape suivante, c'est que le

résolveur récursif obtient cette réponse qu'il va intégrer dans son cache. À partir de là, le résolveur récursif va au serveur .com qu'on a aidé à localiser. Donc c'est l'adresse trois www.example.com et .com va dire, je ne sais pas où cela se trouve, mais voici les exemples. Et enfin, le résolveur récursif va donc aux serveurs de noms faisant autorité pour revenir ensuite vers l'utilisateur final. Donc, c'est le schéma répété. Donc, le résolveur récursif va rechercher les réponses pour le compte donc de l'utilisateur final. Et tout cela se déroule en 1000 millisecondes, microsecondes.

Et, ce qui nous induit en erreur dans les ouvrages, c'est que le rôle du résolveur est incroyablement important. Donc, ce résolveur minimum nous est vraiment utile. Nous n'avons pas besoin d'aller vers le serveur racine. Donc, la réponse elle est dans notre cache. Nous savons où se trouve le .com. Donc, les choses se reproduisent encore et encore et encore. Nous développons le cache et il y a beaucoup d'informations. L'autre élément intéressant dans ce diagramme, c'est le nombre d'utilisateurs dans ce résolveur récursif. Ça n'est pas une seule personne, c'est des centaines, des milliers, des millions d'appareils d'utilisateurs finaux qui utilisent ce serveur récursif. Et, se cache, cette mémoire se développe très rapidement. Et donc, si vous envoyez une requête à ce résolveur récursif, et bien elle va très peu probablement se transformer en requête vers le serveur racine. Peut-être que c'est 0,00002 %. Chacune de ces réponses que l'on obtient de la racine de .com donc s'intègre dans un temps de validité et cela donne une information au résolveur récursif. Ça lui dit quel sera le temps de vie. Et pour la

racine, cette durée de validité est de 48 heures. Et donc, toutes les requêtes qui sont faites donc au serveur racine sont très rares en fait.

Diapositive suivante. Ici, on parle du cache et de l'importance du temps de validité. Pour les serveurs racine, on ne connaît que la formation des serveurs de domaine de premier niveau. Et donc ces résolveurs récursifs permettent une efficacité vraiment incroyable. Voilà, c'était le DNS classique des années 1980. Donc les choses ont évolué. Il y a donc le DNSSEC. Il y a le fait qu'on ne peut pas éliminer le risque. On réduit le risque et le résolveur peut valider les réponses. Il vérifie les signatures cryptographiques. Il y a peut-être quelqu'un qui va essayer d'usurper une identité.

Dans le monde de la confidentialité, on l'a vu dans le diagramme précédent, donc la requête allait vers les serveurs racine, mais les serveurs racine ne s'intéressent qu'au .com, ils ne s'intéressent pas aux www. Il y a donc un standard qui est intitulé minimisation, donc de nom de requête, et cela veut dire qu'on ne voit que ce que vous demandez pour .com. Donc, nous ne nous intéressons pas à ce que vous recherchez. Le serveur racine ne doit pas forcément recevoir ces informations, donc vous ne posez que la question à laquelle vous souhaitez une réponse. Et donc pour des questions de protection des données confidentielles, on chiffre les données, il y a le chiffrement, donc des informations tout au long de la transmission. En ce qui concerne la résilience, il y a beaucoup de

mesures que nous prenons. Il y a donc un grand nombre de serveurs qui ont la même adresse IP.

Donc parlons de Anycast. Anycast, c'est une des parties du travail que nous faisons pour déployer le système de serveurs racine, et c'est ce qui rend les choses plus robustes, c'est à dire qu'il y a une source et une destination. C'est un petit peu comme un coup de fil mon téléphone parle à votre téléphone, c'est tout. Donc il n'y a pas d'autre copie de votre téléphone. Donc, il y a une seule communication. Donc avec Anycast, il y a plusieurs endroits qui hébergent la même adresse et donc c'est comme si vous alliez à Starbucks. Vous pouvez aller dans n'importe quel Starbucks, dans le plus proche des Starbucks. Vous n'avez pas à aller au plus proche des Starbucks. Soyez dans n'importe quel Starbucks. Alors, quand j'envoie un paquet, une demande DNS de mon ordinateur ou à partir d'un résolveur qui est un serveur d'autorisation, et bien le routage Internet va décider de la procédure à suivre. Donc, de ce côté-là, on a vraiment beaucoup de résilience.

Donc, voilà ici un diagramme du parcours. Vous voyez qu'il y a les petits cercles qui représentent des routeurs. Donc, vous voyez qu'il y a de multiples destinations, mais vous voyez le parcours suivi. Le trafic emprunte l'itinéraire le plus court vers une destination unique. Avec Anycast, maintenant, j'ai trois endroits différents. Si ma destination au bas de la page, comme vous le voyez ici, disparaît, le routage sur l'Internet va automatiquement envoyer les demandes aux autres destinations. Donc. C'est ce que nous faisons pour permettre aux identifiants des treize serveurs racine d'avoir

plus de 2000 endroits où il y a du réseau, en fait, en utilisant Anycast, nous en sommes à 2000 points. Plus de 2000 points. Donc, il y a un autre avantage. Pour le scénario, Anycast sous les attaques DDoS. S'il y a un déni de service, puisqu'il y a un attaquant, il y a quelqu'un qui va essayer d'attaquer via DDoS. Le trafic de ces attaques DDoS emprunte également le chemin le plus court vers la destination la plus proche et c'est ainsi réparti entre toutes les destinations. Et voilà, c'est Anycast! Je vais passer la parole à Liman pour le reste de la présentation. Vous avez peut-être des questions? Pour l'instant, non. Très bien.

LARS JOHN-LIMAN Merci. Je suis Lars-Johan Liman. Je travaille pour Netnod, une organisation d'opérateurs de serveurs racine. Dans mon cas, je suis basé à Stockholm, en Suède. On va commencer tout d'abord par parler de plusieurs noms importants, de plusieurs mots importants, de plusieurs termes importants. Vous avez certainement entendu parler de l'autorité chargée de l'attribution des numéros Internet. Il s'agit de l'IANA, le gestionnaire de la zone racine du DNS. C'est là où le travail se fait au niveau technique, travail pour la zone racine. Alors, dans ce contexte de la zone racine, il s'agit des noms des TLD. Et donc c'est la partie de la zone racine qui est importante pour ce qui est de l'IANA. La zone racine, c'est la base de données du serveur racine qui envoie des réponses. Il y a donc un ensemble de données assez limité. D'ailleurs, c'est très minimum. C'est vraiment petit. Avant, quand je faisais mes premières présentations, il y a 20 ans, je faisais ça avec une petite

disquette, un floppy disk comme on disait. Mais en fait, il y a un petit montant de données qui… Tout cela est disponible. Ce sont des données publiques. Vous pouvez les télécharger. C'est vraiment le dossier de la zone actuelle qu'on utilise pour les opérateurs de serveur racine. Donc, c'est de l'information qui est intéressante.

Ce système de serveur racine, c'est l'ensemble du système de 2000 et quelques serveurs que l'on a aujourd'hui. De 2015 à aujourd'hui, je crois, il y a 2000 et quelques serveurs. Donc, tous ces serveurs rassemblés forment un système continu. Vous pouvez parler à tous les serveurs. Sur ces 2000 serveurs, vous pouvez obtenir la même information venant de la zone racine. Donc, ils desservent collectivement la zone [Inaudible]. Si vous avez ensuite les deux organisations qui sont les opérateurs de serveurs racine, ce sont les organisations qui gèrent toutes ces zones à travers le monde, tous ces serveurs à travers le monde. Ce sont des organisations différentes, dans des endroits différents. On essaie d'avoir une certaine diversité. Donc pour nous, la diversité, c'est une bonne chose car nous voulons éviter des points de choc, des points de défaillance. Donc, tous les opérateurs devraient être différents pour qu'il n'y ait pas de points communs lorsqu'il y a des défaillances que ce soit une manière de penser au niveau logique, que ce soit un problème juridique dans un pays où il y a une défaillance au niveau des machines, etc. On essaie de faire les choses différemment. Excepté bien sûr pour ce qui est de la zone

racine, parce que le service est le même pour ce qui est des données.

Quand on parle d'exemplaires de serveurs racine, et bien, on a des machines, des machines à travers le globe depuis 2015 qui fournissent ce service. Donc, nous avons le RSSAC. C'est le comité qui appartient à l'organisation ICANN et qui est responsable pour donner des informations ou des avis, des opinions au conseil d'administration de l'ICANN et à la communauté ICANN, par rapport à tout ce qui est lié au système de services racines et aux opérateurs de services racines qui sont représentés eux-mêmes par le RSSAC. Nous avons treize identifiants qui sont dénotés par des lettres. Chacun de ces identifiants a une adresse IP, et ce sont les identifiants de serveur racine qui ont toutes une… Il y a la version IPv4 et IPv6 bien sûr. Vous voyez ces lettres. Vous voyez les adresses IP à l'écran. Vous voyez le nom des organisations qui sont responsables pour gérer ces identifiants de serveur racine. Comme vous le voyez, vous avez là des grosses organisations, des grosses entreprises, des universités, des agences gouvernementales, des entreprises, des organisations de membres. Il y a ICANN d'ailleurs, qui gère un de ces serveurs. Donc, il y a quand même une grande diversité dans ces opérateurs. Alors, beaucoup de ces représentants sont là durant les conférences de l'ICANN et nous sommes là d'ailleurs pour vous parler. N'hésitez pas à nous contacter et nous demander, nous poser des questions telles que J'ai cette question au sujet du serveur racine. Nous voulons. Nous sommes-là pour nous engager avec la communauté, bien entendu.

MOHIT

Je suis Mohit. Vous avez parlé de diversité, mais je vois quand même que tous ces organismes opérateurs sont situés aux États-Unis. Donc ça pose un risque parce qu'Internet est global et mondial. Donc, quelles sont les implications du fait que tous ces opérateurs soient situés aux États-Unis?

LARS-JOHAN LIMAN

Oui, c'est vrai qu'il y a beaucoup de ces opérateurs qui ne sont basés aux États-Unis, mais pas tous tout de même, trois ne le sont pas. Netnod, qui est en Suède, il y a RIPE NCC qui est basé à Amsterdam et il y a M Root qui est basé aussi au Japon. Donc, je suis d'accord, il y a tout de même une présence assez importante aux Etats-Unis. Mais bien sûr, nous sommes heureux de voir qu'il y en a quelques unes qui ne sont pas basées aux États-Unis. Donc, de manière historique, de toute façon, on sait que le système a évolué durant les années passées. Ça revient aux années 1984. À l'époque, il y avait quatre serveurs racines. D'ailleurs, les informations étaient minimums et comme vous le voyez, cela a évolué durant les années… En 98, il y avait treize serveurs racine. C'était des machines physiques. Ce n'était pas avant 2001, que nous avons commencé à avoir plus de treize machines sur le réseau. Et donc, c'est là où on a introduit le système Anycast. Nous, nous avons donc commencé à travailler avec Anycast à ce moment-là, et maintenant nous en sommes à plus de 2000. N'est ce pas?

	Alors, le service des serveurs racine, donc les opérateurs pour ce serveur racine ont une page web qui s'appelle rootserver.org. Ce n'est pas la même chose que rootserver.net. Comme vous voyez, il y a les rootserver.net à l'écran et ça c'est un site qui est utilisé pour le service. Donc, rootserver.org., on utilise cette adresse car ce ne sont pas des données aussi cruciales. Vous savez, nous essayons de… C'est juste une page Web qui illustre un petit peu le fonctionnement. Et nous, en tant qu'opérateur de serveurs, nous pouvons obtenir les informations dont nous avons besoin. Vous voyez, ici, il y a une carte. Vous pouvez cliquer sur les instances, sur les différents serveurs racines. Vous pouvez voir où ils se situent et qui gère, qui opère ce serveur
PERSONNE NON-IDENTIFIÉE	C'est une vieille. C'est une carte qui n'est pas à jour.
LARS-JOHAN LIMAN	Oui, je pense qu'elle n'a pas été mise à jour, mais bon la carte est la même mais les chiffres sont un petit peu différents aujourd'hui. Je suis désolé.
PERSONNE NON-IDENTIFIÉE	Merci pour clarifier quelque chose. Toutes ces instances, et bien, sont gérées par un des opérateurs de de serveur. Donc, tous ces systèmes sont attachés à un des treize serveurs racine, n'est-ce pas?

LARS-JOHAN LIMAN

Oui. Par exemple, nous avons un serveur à Singapour et nous opérons celui de Singapour. Quelqu'un d'autre va réagir celui de Kuala Lumpur. Parfois, nous sommes au même endroit pour créer une redondance à tel ou tel endroit. On peut utiliser, on peut avoir les deux… On peut avoir deux… Deux groupes peuvent avoir le même serveur et on peut avoir un serveur qui se trouve à Johannesburg, par exemple. En fait, c'est un graphique ici qui est assez nouveau, avec des données qui sont quand même à jour. Comme vous voyez ici, il y a des requêtes reçues par semaine. Ça, c'est en milliards. Ce sont des moyennes quotidiennes. Comme vous le voyez, c'est 2000 serveurs ont du travail, mais d'un autre côté, ils peuvent gérer bien plus que ça. C'est un système qui travaille de manière massive. On peut gérer cette charge. On peut multiplier cette charge sans problème. Nous pouvons gérer toutes sortes d'attaques. Et jusqu'à présent, on a pu faire face à ces attaques de façon positive. Je suis sûr que vous avez noté que le système de serveur racine, fonctionne toujours.

Est-ce qu'il y avait une question dans la salle? Non, peut-être pas. Il y a eu une baisse en 2021. Je pense qu'il s'agit là d'un moment où il y a une reconfiguration de Chrome. Où le moteur de recherche Chrome. On faisait toujours des requêtes intéressantes sur le DNS pour essayer de trouver un petit peu ce qui était intéressant, ce qu'on trouvait sur l'Internet public. Donc, à chaque fois que quelqu'un commençait à utiliser son moteur de recherche Chrome, on recevait des demandes, des requêtes. Donc, avec Google, ils

nous ont expliqué le problème et nous, on a réglé cela en réajustant les codes. Et donc après ça, vous voyez que les requêtes ont baissé.

Donc, il y a bien sûr des mythes sur le système de serveurs racine. Voilà, certains de ces mythes à l'écran. Il y a un mythe qui dit que les serveurs racine contrôlent la destination du trafic Internet. Ce n'est pas le cas. Ces deux serveurs ne pourraient pas gérer une petite fraction du trafic Internet qui existe aujourd'hui. Les serveurs racine n'avaient pas été créé dans cette intention. Les serveurs racine, on leur parle pour essayer de comprendre où est-ce qu'on doit aller. Où est le site web que je cherche? Où est la vidéo que je cherche, où est le message courriel que je recherche, etc. Donc, la machine qui gère vraiment le trafic sur l'internet, et bien ça s'appelle un routeur. Et vous avez un petit capteur à la maison en général pour contrôler la wifi dans votre maison. Donc le plus près, vous êtes du routeur, le mieux ça fonctionne, vous le savez.

Alors ensuite, le mythe suivant, c'est que la plupart des requêtes DNS sont gérées par le serveur racine. Mais en réalité, c'est le cache qui se charge de toutes ces requêtes DNS. Le cache se développe très rapidement et là, les requêtes sont principalement traitées par le cache. Elles reçoivent une réponse par le cache et donc on réduit les informations jusqu'au moment où le temps de validité est écoulé et il faut rafraîchir les données. Et donc il y a une nouvelle série d'informations qui arrivent avec un nouveau temps de validité. L'administration de la zone racine est gérée par les opérateurs de services racines. En réalité, non, ce n'est pas le cas. Nous ne faisons rien de ces données. L'administration est gérée par

l'IANA. Nous laissons les informations. Ainsi, la totalité de l'Internet peut demander, faire des demandes, faire des requêtes. Et en fait, nous ne serions pas en mesure de faire un changement et ce serait immédiatement noté si nous essayons. En raison des signatures de sécurité, nous n'avons pas accès à ces clés de sécurité. Donc, si nous essayons de changer quelque chose, ces signatures ne seraient plus donc correctes, et alors le serveur se méfierait.

Ensuite, les identificateurs de serveurs racine ont une signification spéciale. On croyait qu'il y avait des significations spéciales. Donc en fait, il y a une égalité entre les différents identificateurs. Ils sont tous identiques. Nous avons des lettres pour que le trafic soit bien distribué parmi ces 26 adresses IP. Le mythe suivant, c'est qu'il n'y a que treize serveurs racines. C'était vrai à un moment donné. C'était il y a 25 ans. Nous en avons plus de 2000 aujourd'hui. Les opérateurs de services de serveurs racines mènent des opérations indépendantes. Oui, nous fonctionnons de façon indépendante dans une certaine mesure, mais nous collaborons beaucoup. Souvenez-vous que le système de serveurs racines, ces milliers de machines doivent répondre de la même façon. Cela veut dire que nous devons collaborer. Nous avons des réunions régulières, nous nous rencontrons trois fois par an, donc nous nous réunissons en général dans le cadre de l'IETF et pas aux réunions de l'ICANN. Nous parlons des questions techniques et des questions de sécurité. Nous discutons de notre mode de collaboration, nous avons des outils de collaboration et donc je peux passer un coup de fil ici et maintenant et le téléphone va sonner donc dans 50 lieux différents

dans le monde. Donc, nous avons mené ce type d'exercice à chaque réunion. Nous faisons donc des exercices. Nous avons des listes de diffusion, nous avons des vidéoconférences, des visioconférences et grâce à ces réunions fréquentes, nous nous connaissons. Si Ken m'appelle, je reconnais sa voix, car nous avons participé ensemble à de nombreuses visioconférences au cours des 25 dernières années. Ainsi, nous nous connaissons très bien.

Donc, les instances de serveurs racine reçoivent des requêtes de l'ensemble du DNS. Donc, nous avons des requêtes qui viennent du résolveur minimum. Votre ordinateur portable va envoyer la requête intégrale et le résolveur minimum va uniquement envoyer la partie nécessaire, c'est à dire le domaine de premier niveau qui va être envoyé au serveur de racine.

JENNIFER BRYCE Je lis la question. Si la plupart des requêtes sont traitées sans le besoin de serveur racine et qu'il y en a plus de 1900 instances au niveau mondial. Qu'est-ce que cela veut dire pour les opérations de l'Internet? Qu'est-ce que cela nous dit sur le rôle et la répartition de la charge de travail, donc du système des serveurs racines dans les opérations quotidiennes de l'Internet?

LARS-JOHAN LIMAN Et, bien, la charge pour chaque serveur varie. Tout dépend d'où il se situe, de combien de résolveurs l'entourent. Cela dépend de ce que les utilisateurs demandent. Et cela dépend aussi du nombre de

requêtes auxquelles on peut répondre par le cache. En fait, les serveurs sont déployés dans un but de redondance. Évidemment, il y a des limites dans ce que nous pouvons faire en tant qu'opérateur de serveurs racine. Donc, pour un déploiement dans une région géographique, dans un lieu géographique, et bien il y a des limites en ce qui concerne le temps de réponse, cela dépend aussi de la proximité du résolveur par rapport aux serveurs racine. Et dans un scénario d'attaque par exemple, si quelqu'un essaie de surcharger le système, le fait d'avoir de nombreux serveurs, et bien cela peut être utile pour recevoir tout ce trafic et pouvoir gérer tout ce trafic sans qu'il y ait de surcharge. C'est l'une des raisons pour lesquelles il est utile d'avoir un grand nombre de serveurs.

Mais je suis d'accord, l'importance des serveurs racine est en déclin. En partie parce qu'il y a d'autres mécanismes qui servent à faire des recherches, trouver des choses sur le réseau. Quand est-ce que pour la dernière fois, vous avez tapé la totalité d'un nom de domaine dans votre navigateur? Donc en fait, cela diminue la dépendance envers le système de nom de domaine. Pour le moment, il y a encore cette dépendance qui va probablement durer jusqu'à ma retraite, mais il y a un déclin de cette dépendance. Autre raison à cela, c'est qu'il est donc possible de faire fonctionner un résolveur, d'exploiter un résolveur sans parler à un serveur de nom racine pour une résolution DNS. Vous pouvez télécharger donc la zone racine, et il n'y a pas beaucoup de données et l'information peut être utilisée sans même parler avec un serveur de nom racine, vous pouvez faire une mise à jour plusieurs fois par

jour et ainsi vous avez votre propre copie mise à jour et cela est appelé donc une racine hyper locale. Et je peux vous donner davantage d'informations.

JENNIFER BRYCE Je voudrais donc insérer quelque chose. Tout d'abord, sachant que les opérateurs de serveur racine coordonnent leurs opérations, donc en tant que collectif et non pas indépendant, et que l'IANA et non pas les RSO, gère l'administration de la zone racine. Donc, comment est-ce que les responsabilités sont réparties pour assurer la stabilité et la sécurité de l'infrastructure du DNS?

KEN RENARD Donc, la division des responsabilités et la répartition de ces responsabilités est délibérée. Nous ne souhaitons pas qu'une seule organisation et le contrôle sur la totalité du système ou qu'une seule entité puisse faire des changements. Donc, l'IANA contrôle le contenu et il y a aussi le mainteneur, le chargé de maintenir cette zone racine. Ainsi donc, nous, nous sommes en gros, le département des technologies de l'information qui gère ces ordinateurs. Donc, nous parvenons ainsi à éviter qu'un acteur malveillant ait trop de contrôle.

JENNIFER BRYCE Merci. Autre question, est-ce que ces RSO rentabilisent leur activité en ayant accès à ces serveurs de racine? Et si ce n'est pas le cas,

comment ils peuvent assurer la maintenance de toutes ces instances de serveurs racine?

LARS-JOHAN LIMAN

Et, bien, ces opérateurs de services racine ne sont pas payés. Personne ne les paye. L'ICANN ne les rémunère pas et ils ne sont rémunérés par personne. Ce sont des services pro-bono. Ils sont faits à titre bénévole, mais donc exploités 2000 serveurs dans le monde et cher, ce n'est pas bon marché. Cela coûte de l'argent et il faut trouver un financement quelque part. Et c'est là que nous avons un grand degré de diversité. Les différents opérateur de serveurs racine finance leur travail, chacun à sa manière, pour, par exemple, Netnod, nous déployons nos serveurs dans le monde entier et ainsi nous faisons l'installation d'une plateforme. Et donc, vous voyez que nous avons une façon donc d'exploiter la racine, si vous connaissez RIPE NCC, et bien RIPE NCC est responsable d'allouer des adresses IP dans la zone européenne. Et c'est une organisation où il y a des membres, des frais d'adhésion, des droits d'adhésion, et à partir de ces cotisations, de ces droits d'adhésion les opérations sont financées. Y a-t-il une autre question?

KEN RENARD

Nous ne tirons pas de bénéfices financiers. Nous considérons que les données sont privées. Nous utilisons les données pour soutenir le service, pour continuer de l'exploiter de façon efficace. Nous ne

vendons pas les données, nous ne les divulguons pas en échange de quelconques rémunérations, c'est très important à souligner.

LARS-JOHAN LIMAN Donc, aucun opérateur de services racines ne vend des données. Nous contribuons aux efforts de recherche ici et là, mais cela se passe toujours dans le cadre d'un accord de non-divulgation très strict et quand nous livrons des données, elles sont donc anonymisées. Et donc, il y a donc cette confidentialité. On ne voit pas les adresses IP qui ont envoyé les données, et il y a donc beaucoup de choses qui font qu'il est important de comprendre le risque de collision de noms.

PERSONNE NON-IDENTIFIÉE Je pense que pour l'audience, il y a une question intéressante. C'est la limite de treize?

LARS-JOHAN LIMAN Pourquoi y a-t-il treize serveurs, treize identifiants de serveurs racine? Ça, c'est dû aux limitations qui avaient été mises sur le système de noms de domaine. On veut que cela corresponde aux anciens serveurs racine pour que tout ça soit efficace en un seul paquet sur le réseau. Alors bien sûr, le réseau a évolué, les protocoles DNS ont évolué et aujourd'hui on peut faire les choses d'une manière différente. Mais, depuis le début de cette évolution, il n'y a pas eu de processus qui a pu remplacer les opérateurs de serveur racine. Donc personne ne sait comment rajouter ou retirer

des opérateurs de services racine. Je ne peux pas. Je ne peux pas abandonner. Je suis coincé. Donc, pour faire face à ce problème, le Comité pour les systèmes de serveur racine doit faire un inventaire de problème. Vous savez, ça, c'est un projet qui dure depuis longtemps. C'est un projet à long terme. Le RSSAC fait donc un inventaire des problèmes et dit voilà, nous aimerions changer le système de gouvernance des serveurs racine pour qu'il puisse évoluer avec le temps, pour qu'il soit plus transparent. Et les résultats de ce document ont été publié et a vu une consultation publique au sein du groupe de travail. Donc, je pense qu'il y a deux semaines, on a reçu le dernier rapport qui a été envoyé au conseil d'administration. Ce rapport comprend des recommandations sur la manière d'avancer et de créer de nouvelles structures autour de ces opérateurs de serveurs racine. Justement, j'espère qu'il y aura un processus dans l'avenir qui va nous permettre de rajouter, de retirer, de changer, etc. Il n'y a pas vraiment de bonnes raisons pour faire des changements, parce que c'est un système qui fonctionne assez bien et depuis 2001. Nous ne sommes pas à 99.99 %, mais à 100 % donc… Et ça fonctionne toujours. Donc on touche du bois, n'est-ce pas?

KEN RENARD

En 2013, je crois qu'on avait vu un document, on avait on avait publié un document. On savait que dans les années 80-90, on a dû rajouter plus et plus et plus, mais en ajoutant Anycast chacun... Oui, on a tous évolué en différentes dimensions. Maintenant, on est passé de 13 à 2000 et quelques. Donc le besoin d'infrastructure

technique est suffisant. Donc aller au delà de treize. Bon, c'est pas forcément, il n'y a pas vraiment besoin d'aller au-delà de 13. Voilà. Merci.

PERSONNE NON-IDENTIFIÉE Y a-t-il d'autres questions? Il y a une question dans la salle.

SUNCICA ROSIC J'ai une question à propos d'Anycast et de la fragmentation de paquets. Je comprends l'importance de la résilience de l'Internet et du coup que ça comprend, mais quand on a une adresse IP qui qui comprend plusieurs paquets. Qu'est-ce qui va se passer si ces paquets sont envoyés à un Anycast différent? Alors, surtout sous certains UDP, la vitesse compte beaucoup.

LARS-JOHAN LIMAN Oui, vous avez raison, cela peut se produire. Ces paquets peuvent passer à des nodes Anycast différents. C'est tout à fait possible. C'est inhabituel, mais c'est possible. Mais, cela se produit lorsque l'on a soit un système de partage de charge ou donc le trafic est partagé sur différents liens, sur des liens séparés. Enfin… Et cela peut se produire aussi lorsqu'on a des flaps dans le système de routage. Si vous n'avez pas de chance, les paquets vont se croiser et peuvent aller dans des directions différentes. Mais, si on parle de requêtes UDP unique, ça fonctionne assez bien. Oui, on a des paquets fragmentés, mais bon, deux fragments peuvent se produire et aller vers des serveurs différents. Mais, vous n'allez pas

recevoir une réponse de toute façon, parce que si les paquets ne sont pas complets, le serveur ne va pas pouvoir générer une réponse. Donc il y a tout un problème là-dessus, autour de cela, mais c'est vraiment un tout petit problème. C'est un problème minuscule. Théoriquement, ça peut se produire, mais en pratique, tout fonctionne assez bien. Mieux que je le pensais dans les 20 dernières années d'ailleurs. Alors, une autre question?

PERSONNE NON-IDENTIFIÉE Il y a eu quelques attaques DDoS sur les serveurs racine en 2015, et ça s'est produit parce qu'il y avait deux ou trois petits problèmes. Ça a été résolu assez rapidement. Oui, cela fonctionne à 100 % pratiquement. Cela fait donc dix ans. Est-ce que vous pensez qu'il pourrait y avoir de nouveaux problèmes, de nouveaux enjeux? Parce qu'il y a une nouvelle technologie? Quel est le potentiel de vulnérabilité? Est-ce que ça existe théoriquement? Qu'est-ce qu'on peut faire? Qu'est-ce qui pourrait être utilisé pour nuire à ce système?

LARS-JOHAN LIMAN Oui, c'est un champ de mines cette question. Alors, il y a plein de choses qu'on ne connaît pas. Ce sont des inconnues, des notions inconnues. Il y a des opérateurs qui sont impliqués dans différents endroits, différents espaces. Vous allez nous retrouver dans les réunions ICANN, dans les réunions l'IETF. Nous sommes impliqués à l'élaboration des protocoles du DNS, les protocoles BGP pour le routing, etc. Les réunions en OARC, toutes les réunions sur les

thèmes liés au DNS, on essaye de rester au courant de ce qui se passe, des menaces, etc. Je suis un membre de deux organisations qui travaillent sur la sécurité en Suède, deux organisations ISP, une organisation sur la sécurité physique et une sur la cybersécurité. Donc, on est impliqué dans beaucoup d'espaces. Bien sûr, les menaces, il y en aura toujours. Il y a toujours de nouvelles manières de menacer tous les jours de menacer l'Internet, et je n'ai aucune idée à savoir comment l'intelligence artificielle va gérer tout cela. Tout ce qu'on peut faire, c'est rester au courant, si on peut dire, et être prêt. Les systèmes sont bien faits, mais il y a des tas de manières logiques pour attaquer le DNS, les serveurs DNS que nous connaissons déjà. On peut truquer le serveur pour lui faire faire des choses étranges, et on peut mettre des bugs vraiment, vraiment malveillants. Il y a plein de choses qui peuvent se produire. Ça fait partie de la vie des opérateurs, n'est-ce pas?

PERSONNE NON-IDENTIFIÉE Quand on parle des risques cyber, et bien vous l'avez bien expliqué. Vous avez expliqué la diversité des différentes organisations qui financent ces systèmes. Est-ce que vous voyez un risque d'augmentation potentielle d'hébergement des données de mémoire ou de l'impact de l'IA? Pas forcément du côté de la cybersécurité, mais aussi du côté financier, du côté qui va faire augmenter les prix, si vous voulez. On a parlé de la gouvernance des serveurs racines, et bien dans ce sens y a-t-il une manière de prévoir les revenus pour les opérateurs, au cas où vraiment il y

aurait un grand problème? Comment est-ce que cela sera financier?

LARS-JOHAN LIMAN Quand il s'agit des prix, et bien oui, on voit, ça commence à se sentir. On se limite au nombre de serveurs qu'on achète ou qu'on déploie, mais c'est un très bon point. Je pense vraiment que cette augmentation de prix sera temporaire, parce qu'il y a de l'argent à faire, si on peut dire, en produisant ces choses. Et il y a des gens qui font des puces de mémoire. Enfin, vous savez, il y a des technologies qui peuvent être faites, qui peuvent être produits, et donc ça va permettre une certaine compétition. Je pense que dans deux ou trois ans, les prix vont commencer à baisser. En attendant, nous sommes vraiment en bonne position. Moi, j'ai arrêté d'acheter des serveurs il y a à peu près trois ans.

PERSONNE NON-IDENTIFIÉE Il nous reste cinq minutes.

LARS-JOHAN LIMAN Oui, j'allais dire quelque chose à ce sujet. On va essayer de résumer un peu la chose. Alors, la zone racine contre le système de serveur racine. Alors, ce que l'on reçoit des personnes qui maintiennent la zone racine. Là, on parle des bases de données, des informations, des paquets d'informations. Alors, il y a la liste des TLD et le serveur de noms. Il y a les informations pour chaque TLD, à savoir quels sont les serveurs responsables de ce TLD. Et, ça, c'est géré par

l'ICANN à travers l'IANA et c'est géré en suivant les politiques communautaires. Donc, la politique qui est mise en œuvre par l'ICANN et mis en œuvre par l'IANA. Et ensuite on a la distribution des systèmes qui ressort de cela. Alors, tout cela est mis en œuvre à travers 26 adresses, et cela se fait à partir d'un rôle technique, purement technique. Rien à voir avec l'administration des données. On ne change rien, on n'ajoute rien, on ne choisit rien. Et le système de serveurs racines est donc responsable de ces douze organisations.

Voilà le calendrier, ou du moins la chronologie de la zone racine. Le parcours de la zone racine. Pardon. Alors, tout commence par l'opérateur du TLD. Alors, par exemple, pour nous, l'opérateur en Suède veut faire un changement à son ensemble de serveurs, par exemple, .se dans notre cas, et bien on contactera ICANN et il y a un portail web pour faire cela. Et là, un changement pourrait être demandé. L'IANA révisera la requête, fera le changement, enverra l'information de changement à la personne qui maintient, au groupe qui maintient la zone racine. Et là, bien sûr, l'information sera envoyée avec les crypto signatures et cela ressortira dans la zone racine. Ce sera publié. Donc les douze opérateurs choisissent le dossier de zone à partir de la zone racine, distribuent à tous les serveurs. Dans notre cas, nous sommes responsables pour un bon nombre, pour un grand nombre et au bout du compte, on a 2000 machines qui répondent à ces demandes sur l'Internet, à ces requêtes sur l'Internet. Donc tout ça est automatique à partir du moment où la zone racine est disponible, en deux minutes, la

requête est remplie. C'est automatique. De toute façon, le transfert de la zone racine est aussi vérifié avec des signatures supplémentaires. On a donc un système de sécurité double pour nous assurer que le parcours se fasse sans faille.

On doit… le RSSAC. Alors, RSSAC, c'est un groupe au sein de l'ICANN et de la communauté ICANN. Et à partir des statuts constitutifs de l'ICANN, RSSAC doit envoyer des conseils à la communauté ICANN et au conseil d'administration sur tout ce qui est lié aux opérations, à l'administration de la sécurité et l'intégrité du système de services Internet. C'est ce qu'on fait. On n'élabore pas des politiques, on est seulement un groupe, un comité de conseil. On donne nos avis. Donc, les opérateurs de services de racines sont représentés au sein de RSSAC. RSSAC ne s'implique pas en lui-même. On collabore. Nous sommes des personnes qui se retrouvent et qui collaborent dans le travail. Il y a deux représentants de chacun des opérateurs de serveurs racine. Donc, on est douze membres principaux. Il y a aussi des membres suppléants. Donc, moi, j'ai un suppléant si je suis malade, par exemple. On a aussi des liaisons, nous avons des liaisons de RSSAC avec SSAC, bien sûr. On a aussi des liaisons avec l'IANA, etc. Nous sommes un petit comité, nous avons des ressources pour faire quelques recherches et pour rédiger certains documents, etc. Nous avons des experts dans beaucoup de domaines, donc nous avons des membres. Donc, si vous voulez postuler à la RSSAC, vous pouvez nous envoyer votre cv, à savoir si vous avez l'expertise pour faire partie du groupe.

PERSONNE NON-IDENTIFIÉE Il nous reste peu de temps si vous voulez bien passer à la suite.

LARS-JOHAN LIMAN Voilà, on a parlé des liaisons, on a parlé de tout ça. On a parlé de tout ce que vous voyez à l'écran. Il y a des ressources supplémentaires que vous pouvez trouver sur cette diapositive. Pour ce qui est du RSSAC avec la page Web principale du RSSAC, icann.com, si vous n'avez pas en plus eu le temps de poser votre question durant cette séance, vous pouvez l'envoyer à l'adresse que vous voyez ici à l'écran. Je vous remercie beaucoup.

[FIN DE LA TRANSCRIPTION]