MONTREAL – Comment ça marche : les opérations du serveur racine
Dimanche 3 novembre 2019 – 15h15 à 16h45 EDT
ICANN66 | Montréal, Canada

STEVE CONTE : Nous allons commencer dans quelques minutes. Nous sommes dans une très grande salle, donc si vous voulez vous rapprocher pour qu'on puisse vous voir. Alors, comment est-ce qu'on va fonctionner pour cette séance ? Le RSSAC va faire une présentation, ensuite on aura des blocs pour des questions et réponses. J'ai suffisamment marché pour aujourd'hui, donc si vous voulez bien vous rapprocher pour raccourcir les distances, on va commencer d'ici quelques minutes.

ANDREW MCCONACHIE : Bonjour. Je m'appelle Andrew McConachie, je travaille pour l'ICANN pour soutenir le comité consultatif des serveurs racine. Et je vais vous parler aujourd'hui du tutoriel sur les systèmes de serveurs racine comme vous pouvez le voir ici.

Je ne vais pas m'asseoir. Excusez-moi pour les gens qui suivent à distance si vous devez me suivre avec la caméra, mais je vais marcher un petit peu pendant cette présentation.

Je vais faire cette présentation en coordination avec mon collègue Ozan Sahin qui va faire la deuxième partie. Moi, je vais vous parler d'abord du DNS. Plusieurs d'entre vous connaissent certainement le contenu de cette présentation, mais on va revenir là-dessus. Ensuite,

une explication sur Anycast et sur la manière dont Anycast et différent d'Unicast et des autres systèmes. Ensuite, le système des serveurs racine aujourd'hui, des exemples et un peu d'historique. Ensuite, Ozan va prendre la relève, va vous parler du RSSAC, du caucus RSSAC et du travail en cours avec l'évolution du système de serveurs racine. Donc on commence.

Aperçu du DNS. Comme la plupart d'entre vous le savez, les identificateurs sur l'internet, il y a différents types d'identificateurs. Sur cette diapositive, vous voyez les adresses IP et la manière dont elles sont connectées sur l'internet, qui est connecté à l'internet. Il y a une requête d'adresse IP, il y a deux types, IPv4 et IPv6. C'est une étiquette numérique, ce n'est pas un nom, et c'est un identificateur fondamental sur l'internet.

Pourquoi le DNS ? Quel était le problème dans le fait d'utiliser simplement les adresses IP ? Les adresses IP sont difficiles à se souvenir, elles changent. Et il y a des problèmes modernes aussi qui se posent, qui sont venus après l'introduction du DNS, qui est la manière dont on peut partager les adresses IP. Les clients peuvent avoir plusieurs adresses IP, donc quelle adresse IP utiliser. Vous pouvez utiliser un nom qui existe pour résoudre cela.

Et comme vous l'aurez certainement découvert, le système DNS est hautement hiérarchique. Il y a la racine en haut et en-dessus, vous avez ce qu'on appelle les noms de premier niveau. Là, vous avez des exemples, .uk, .org, .edu. Et en dessous, vous avez les noms de deuxième niveau, plus troisième niveau, etc. D'une manière générale,

on peut penser à une carte entre les adresses IP. Et il y a d'autres cartes aussi comme les cartes entre les serveurs noms.

Là, vous avez quelques définitions. Sachez qu'il va y avoir deux diapositives pleines de définitions. Et avant de rentrer dans le fond du sujet, je vais vous donner l'occasion de vous familiariser un petit peu avec ces termes. Ces termes, on les utilise fréquemment, non seulement dans les documents mais dans la présentation.

Le premier terme que j'ai déjà utilisé, c'est le système de serveurs racine. C'est la série de serveurs racine qui, de manière collective, mettent en œuvre le service racine.

Ensuite, je vous ai parlé de la hiérarchie DNS. Il s'agit des données que le RSS aide à distribuer. Et la zone racine, ce sont les données que le RSS aide à distribuer et contient toutes les informations nécessaires pour contacter les domaines de premier niveau qui se trouvent en dessous.

Ensuite, on a l'instance Anycast de serveurs racine. Lorsqu'on fait référence à des serveurs individuels ou à des machines physiques, on parle d'instance Anycast.

Et là, vous avez quelques rôles d'un point de vue organisationnel. D'abord, vous avez l'administrateur de la zone racine. C'est l'administrateur de la gestion des données contenues dans la zone racine. Donc cela, ce sont les fonctions IANA essentiellement. Cela implique la distribution des opérateurs des domaines de premier niveau et la maintenance de leurs caractéristiques techniques

administratives, c'est-à-dire la manière dont vous résolvez un domaine de premier niveau, ce qui implique qu'il y a un serveur pour ce domaine de premier niveau qui répond aux requêtes et que les personnes qui administrent vont devoir parler à l'administrateur de la zone racine.

Il y a également le responsable de la maintenance de la zone racine, actuellement VeriSign, qui est chargé d'accepter les données de service de la part de l'administrateur de zone racine et ensuite de le formater dans un format de fichier zone puis de le distribuer aux opérateurs de serveurs racine.

Les opérateurs de serveurs racine, il y en a 12. Il s'agit des organisations responsables de la gestion des services racine sur les adresses IP spécifiées dans la zone racine. Donc il s'agit des organisations qui gèrent les serveurs racine physiques.

Donc cela, j'en ai un petit peu parlé déjà. De quoi s'agit-il ? De la différence entre les données et la manière dont on obtient les données. Il y a des serveurs qui servent des données et il y a les données elles-mêmes. La zone racine, elle, porte sur ces données, c'est-à-dire un fichier zone dans le système des serveurs racine où vous avez des serveurs qui à leur tour servent des données. Par rapport à la zone racine, c'est le point de départ, c'est la liste des TLD et la manière dont vous allez au TLD pour résoudre les noms sous ce TLD. Et la zone racine est gérée par l'ICANN et elle est administrée par le responsable de la maintenance de la zone racine.

Maintenant, le système de serveurs racine, c'est le système constitué de serveurs qui répond aux requêtes. À l'heure actuelle, il y a 26 adresses IP qui constituent ce système de serveurs racine, 13 pour l'IPv4 et 13 pour l'IPv6. Et il y a plus de 1 000 instances physiques. Vous savez, les chiffres varient et augmentent un petit peu au fil du temps donc maintenant, on dit un peu plus de 1 000 instances physiques. Avant, on avait une diapositive qui donnait le chiffre exact mais on a cessé de modifier ce chiffre. Donc maintenant, on dit tout simplement un peu plus de 1 000. Il s'agit d'un rôle purement technique pour servir cette zone racine.

Sur cette diapositive, on passe en revue tous les détails d'une requête DNS et réponse DNS. Donc je vais passer peu de temps sur cette diapositive pour vous présenter brièvement ce qui se passe lorsqu'un ordinateur veut résoudre un nom.

On commence à droite, on voit notre utilisateur internet, donc le client qui utilise un ordinateur. Et il aimerait arriver sur www.exemple.com. Donc si on part du fait que ce serveur récursif n'avait rien dans son cache donc il ne sait rien, si ce n'est comment parvenir à ce serveur, alors ce que va faire l'ordinateur d'abord, c'est prendre contact avec le serveur de noms récursif qui est ici au milieu de l'écran. Il va envoyer une requête à ce serveur de noms récursif pour lui dire quelle est l'adresse IP de www.exemple.com.

Et ce serveur de noms récursif, parce qu'il vient d'être allumé et n'a rien dans son cache, va d'abord prendre contact avec le serveur de noms de la racine et va envoyer toute une requête à ce serveur en

demandant : « Quelle est l'adresse IP de www.exemple.com ? » Et le serveur de noms racine va dire : « Je ne sais pas quelle est l'adresse pour www.exemple.com mais je sais comment vous pouvez parler à .com. Et d'ailleurs, voilà la signature de cette donnée. » et va donc renvoyer cette réponse au serveur de noms récursifs.

Donc le serveur de noms récursif dit : « Très bien, je sais comment contacter .com, j'ai la signature. Donc je vais comparer cela d'un point de vue cryptographique à la partie publique de la signature de la clé KSK pour vérifier si la réponse du serveur racine est bonne et je vais prendre contact avec le .com. »

Donc le serveur de noms récursif s'adresse au serveur de noms .com pour poser la question. Le serveur de noms .com dit : « Je ne sais pas où c'est mais je sais où se trouve www.exemple.com. Et d'ailleurs, j'ai la signature de cette donnée. » Donc le serveur de noms récursif va faire la même chose, il dit : « Très bien, j'ai le contact de www.exemple.com, j'ai la signature de cette donnée. » et va contacter ensuite contacter le serveur de noms .com pour enfin obtenir une réponse pour www.exemple.com avec la signature qui l'accompagne. Donc cela repart vers le serveur de noms récursif qui dit : « Très bien, j'ai une adresse IP pour www.exemple.com et j'ai une signature, je fais une comparaison cryptographique, je fais les vérifications. » Et ce n'est que maintenant que le serveur de noms récursif revient vers l'ordinateur de l'utilisateur et dit : « Voilà ton adresse IP. »

Donc ce qu'on veut vous montrer ici, c'est que par une simple requête qui est initiée par l'utilisateur, il y a tout un processus récursif et autre

et jusqu'à ce que le processus ne soit pas finalisé, il ne revient pas vers l'utilisateur final.

Là, on rentre un petit peu plus dans le détail de ce dont je viens de vous parler. Les serveurs racine ne savent que ce que les serveurs ont besoin de savoir et de demander. Ils ne savent pas comment résoudre tout le nom. Toutefois dans les serveurs récursifs, ils se souviennent des réponses. Il y a des caches et dans les caches, il y a des réponses. Donc inutile d'aller dans le serveur racine aussi souvent que cela.

Et le TTL, pour cette information en cache, est de deux jours. Donc si le serveur récursif demande au serveur racine une question, il va se souvenir pendant deux jours de cette réponse. Donc il ne va pas devoir reposer la même question, en tout cas pendant deux jours.

Vous voyez ici quelques évolutions modernes du DNS. On parle de signature cryptographique par rapport aux données DNS. Tout cela, c'est défini par le DNSSEC. Le DNSSEC est utilisé comme un terme plus court pour parler de toute cette signature, validation, processus qu'il faut mettre en place pour s'assurer que d'un point de vue cryptographique, le client reçoit la bonne réponse de la part des serveurs. Il y a eu des renforcements en termes de confidentialité par rapport au DNS parce que les DNS traditionnels étaient en texte clair uniquement. Donc maintenant, on a DNS sur TLS et DNS sur HTTPS.

Anycast, c'est une autre évolution moderne du DNS et tous les serveurs ont mis en œuvre Anycast. On a toute une présentation sur Anycast, donc on va pouvoir en plus parler plus avant par la suite, ce qui m'amène à une explication sur Anycast. Au début, il y avait

simplement Unicast. Et Unicast, cela veut dire que les paquets provenant de sources vont tous dans la même direction, vers la même destination. Donc tous les paquets des différentes sources vont vers les mêmes destinations et correspondent à un même serveur. Donc jusque là, pas de problème à moins que vous ne vouliez échelonner les choses.

Anycast permet d'échelonner les choses et cela, c'est important si vous voulez avoir des requêtes plus valides et c'est bon aussi si vous voulez qu'il y ait des attaques des dénis de service et que vous voudriez que ce trafic soit accéléré pour pouvoir mieux gérer les choses.

Sur Anycast, la cartographie entre une adresse IP et le point d'entrée change. Et maintenant, vous avez une cartographie d'adresses IP vers des serveurs multiples. Donc il y a différentes sources qui vont parvenir à différentes destinations mais elles continuent d'envoyer le trafic vers les mêmes adresses IP ; c'est juste l'adresse physique qui change. Donc les sources obtiennent des données plus rapidement et le trafic d'attaques DDoS est en envoyé vers l'instance la plus proche et ne va pas être envoyé vers d'autres destinations.

Il y a une route unique pour parvenir à destination ; donc une source, une destination. Et si vous ajoutez une autre source, elle va aller vers la même destination. Et là, vous voyez Anycast. Vous avez plusieurs destinations. Ce sont les points bleus que vous voyez, la destination. Une seule source mais vous pouvez imaginer une même source proche

de la même destination qui va vers la même destination. Donc c'est beaucoup plus simple de distribuer le trafic.

Là, vous voyez l'un des grands avantages d'Anycast. C'est ce qui se passe en cas d'attaque de déni de service. Les sources qui utilisent des destinations qui se trouvent loin des attaques DDoS ne sont pas affectées par ces attaques. Donc admettons que ce soit une attaque locale, elle va affecter un serveur et pas d'autres serveurs de par le monde. Cela, c'est l'un des grands avantages d'Anycast. Bien.

Maintenant, je vais vous parler d'un petit historique par rapport au système de serveurs racine et de ce qu'est ce système de serveurs racine aujourd'hui. Entre 1983 et 1986, le système de serveurs racine avait quatre adresses. Et vous pouvez le voir, depuis, ce chiffre n'a cessé d'augmenter jusqu'en 1998, avec 13 adresses. Peut-être que le terme adresses n'est pas le plus approprié ici mais vous pouvez voir que ces changements se sont déroulés dans le temps. Et aujourd'hui, parce qu'on a ajouté les adresses IPv6, nous avons 26 adresse IP, donc 13 pour l'IPv4 et 13 pour l'IPv6. Et grâce à Anycast, on peut dire qu'il y a 26 adresses IP, 13 IPv4 et 13 IPv6, qui servent 1 000 instances physiques.

Vous voyez une liste des noms d'hébergement et des adresses IP ainsi que le gestionnaire pour le système de serveurs racine actuel. Tous les noms d'hébergement ont leurs adresses IPv4 IPv6 qui y sons associées.

Cela, c'est une carte qui n'est pas forcément très précise d'un point de vue géographique mais si vous allez sur l'adresse qui figure en bas ici,

root-servers.org, vous pouvez suivre des villes individuelles, d'abord à l'échelle d'un continent, d'un pays et d'une région, pour voir quels sont les serveurs qui opèrent dans cette ville. Cela, c'est au niveau le plus grand. Vous pouvez zoomer pour vous rapprocher et vous pouvez regrouper des informations aussi. Mais ce que cette carte vous montre, c'est qu'il y a des instances dans le monde entier sur tous les continents – d'ailleurs, je ne devrais pas dire cela parce que si cela se trouve, il y a des continents où il n'y en a pas. Mais en tout cas, sur tous les continents à l'exception de l'Arctique, il y a des serveurs. Mais ce sont des informations très intéressantes que vous pouvez retrouver sur root-servers.org pour trouver ce genre d'informations.

Donc là, vous avez la processus de changement à la zone racine, donc le ravitaillement dans les serveurs racine, et comment les serveurs racine vont chercher tout ceci. À gauche, vous avez les opérateurs de TLD. Par exemple, il y a besoin de faire une requête de changement, il contacte l'IANA et il dit : « Écoutez, nos serveurs de noms utilisaient cette adresse IP. On voudrait passer à celle-ci. » Donc ils expliquent ceci à l'IANA, l'IANA a un certain nombre de procédures de vérification pour s'assurer qu'on parle bien à l'opérateur de TLD, qu'il y a une bonne chaîne, que rien ne va se casser. Et une fois que le changement a été approuvé, lorsque l'IANA dit au responsable de la maintenance de la zone racine : « Nous allons donc faire cette mise à jour. », ce responsable de la maintenance signe cryptographiquement et ensuite, il distribue ceci aux opérateurs.

À droite, vous avez toutes ces bulles avec RS. Cela représente les instantes – pour chaque opérateur, il y a beaucoup de ces instances.

Et tout à droite, vous voyez les résolveurs récursifs qui envoient des requêtes et qui reçoivent des réponses.

Donc voilà un petit peu comment se présente le flux d'information. C'est à un très haut niveau, certes, mais c'est le flux d'infrastructure lorsqu'il y a un changement à la zone racine. Davantage d'information sur les opérateurs de zone racine. Je vous ai dit qu'il y en avait 12 et qu'ils se focalisent surtout sur la fiabilité, l'accès, la fiabilité pour les utilisateurs finaux. Ils travaillent ensemble au RSSAC et dans d'autres groupes. Ils se focalisent sur le professionnalisme. Il y a différents types d'organismes. Tous ces organismes ne sont pas des organismes gouvernementaux ou à but non lucratif, donc il y a vraiment une grande diversité technique, organisationnelle, géographique en termes de modèle de financement, etc.

Voilà un petit peu comment tout ceci est coordonné. J'ai parlé des réunions, du secteur, de différentes entités telles que l'ICANN, le RSSAC, l'IETF, les réunions des RIR, les réunions des groupes d'opérateurs. Il y a également différents outils. Ils partagent les données les uns avec les autres et de temps à autre, il y a des activités, des exercices pratiques pour en fait être prêts en cas d'urgence, etc.

Les opérateurs s'occupent de l'évolution du service au niveau opérationnel. Ils évaluent différents protocoles, comme le protocole de DNS. Ils participent à l'IETF pour ceci. Et ils s'assurent qu'il y a toujours une stabilité et un accès qui restent robustes. Ils ne sont pas impliqués dans la mise en place des politiques et pas non plus dans la

modification des données. Ils ne sont pas impliqués dans la définition des données, mais ils les publient.

Cette diapositive vous montre un petit peu quels sont les mythes que j'ai pu observer en comparaison avec la réalité.

Premier mythe : les serveurs racine contrôlent là où va le trafic internet. En fait, ce sont les routers qui contrôlent là où va le trafic internet. Les serveurs racine répondent simplement à des requêtes.

La plupart des requêtes de DNS sont traitées par un serveur racine ; ce n'est pas le cas pour des raisons de cache parce que les serveurs racine se souviennent des informations qu'ils ont reçues, dont ils n'ont pas à reposer la question à chaque fois qu'il y a une requête qui arrive.

Autre mythe. L'administration de la zone racine et le service sont la même chose. Encore une fois, il faut faire la différence entre les données et le service des données. L'administration des données, c'est complètement différent de la réponse aux requêtes par rapport aux données.

Autre mythe : certaines des identités de serveur ont une signification spécifique. Et bien non, ce n'est pas le cas. Aucun d'entre eux n'a une signification particulière.

Autre mythe : il n'y a pas que 13 serveurs racine. Non, avec Anycast, il y en a plus de 1 000 mais il n'y a que 13 identités techniques. Les opérateurs de serveurs racine ne fonctionnent pas complètement indépendamment. Ils coopèrent les uns avec les autres. On en a parlé

dans la dernière diapositive. Et les opérateurs de serveurs racine ne reçoivent que la partie TLD d'une requête.

Lorsque j'ai parlé de la résolution, j'avais tout un ensemble de requêtes pour le serveur racine, donc voilà comment cela fonctionne traditionnellement, en tout cas dans plus de 90 % des cas. Donc voilà pourquoi on a marqué le mot « habituellement » en gras.

Nous avons un nouvel organisme sur la protection de la vie privée qui viendra de l'IETF qui a pour objectif de changer ceci, mais ce n'est pas quelque chose déployé de manière très large. Actuellement, la réalité, c'est que les opérateurs de serveurs racine en général reçoivent toute la requête. Très bien.

Donc si vous gérez un réseau, pensez à certaines petites choses par rapport à votre DNS et son interaction avec les serveurs racine. Il vous faut trois à quatre instances proches, cela veut dire topologique, processus de réseau. Ce n'est pas une question de géographie. Donc vous pourrez peut-être travailler avec des collègues si vous avez des problèmes de latence. Il y a plusieurs choses que vous pouvez faire.

Autre chose, mettre en marche la validation DNSSEC dans les résolveurs de manière à ce que vos données soient signées dans la zone racine de manière à ce que vous receviez des données valides entre tous ces différents serveurs. Donc s'assurer que personne ne perturbe les données en transit. Donc vous validez les données dans vos résolveurs locaux et cela est vraiment utile.

Si cela vous intéresse, vous pouvez également participer au caucus du RSSAC et apporter votre contribution. On vous en parlera tout à l'heure, mon collègue le fera. Et si vous êtes opérateurs de réseau et que vous souhaitez héberger une instance Anycast, parlez à un membre RSSAC après la présentation ou alors vous pouvez poser une question tout à l'heure. Vous pouvez envoyer un courriel à cette adresse : ask-rssac@icann.org.

Je vais maintenant passer la parole à mon collègue Ozan Sahin qui va vous parler de la partie organisation.

OZAN SAHIN : Merci Andrew. Bonjour à tous, je m'appelle Ozan, je fais partie d'ICANN Org et je travaille avec le RSSAC, donc le comité consultatif des serveurs racine.

Nous allons commencer par le rôle du RSSAC. Son rôle est assez limité finalement. Le rôle de ce comité consultatif des serveurs racine, c'est de fournir des avis à la communauté de l'ICANN et au Conseil d'Administration de l'ICANN sur toutes les questions d'opérations, d'administration, de sécurité, d'intégrité du système de serveurs racine de l'ICANN.

Vous voyez sur la diapositive qu'il y a des notes sur ce que fait le RSSAC et sur ce qu'il ne fait pas. Il s'agit d'un comité qui produit des avis principalement au Conseil d'Administration de l'ICANN mais également à d'autres entités de l'ICANN et à d'autres organismes qui sont impliqués dans tout ce qui est relatif au DNS. Les opérateurs de

serveurs racine sont représentés au sein du RSSAC mais le RSSAC ne s'immisce pas dans tout ce qui est opérationnel.

En termes d'organisation, le RSSAC est composé de représentants nommés des opérateurs de serveurs racine. Il y a des suppléants à ces représentants et il y a des liaisons. Il y a également une autre entité qu'on appelle le caucus RSSAC, c'est en fait un ensemble de volontaires qui sont des experts dans leur sujet. Et les membres sont confirmés par le RSSAC sur la base d'une manifestation d'intérêt. Donc si vous voulez devenir membre du caucus RSSAC, vous devez envoyer, comme le collègue Andrew qui vient de parler vous l'a dit, votre manifestation d'intérêt et ensuite, le RSSAC confirmera que vous êtes devenu membre.

Nous avons deux coprésidents, ils sont là dans la salle, Brad Verd et Fred Baker. J'aimerais également mentionner que le RSSAC est en phase de transition ; nous allons utiliser le modèle président/vice-président. Donc d'ici la fin de l'année, nous aurons eu des élections pour le vice-président et le leadership du RSSAC suivra la modèle président et vice-président.

Comme je vous l'ai dit, nous avons des liaisons au RSSAC. Quatre de ces liaisons sont des liaisons qui sont nouvelles. Il y en a quatre qui ont terminé leur mandat. Il y a une liaison pour l'opérateur de fonctions IANA, il y en a une pour le responsable de la maintenance de la zone racine, il y a une liaison pour le comité de l'architecture de l'internet et une liaison pour le comité consultatif sur la stabilité et la sécurité.

Il y a quatre liaisons sortantes, une auprès du Conseil d'Administration de l'ICANN, une auprès du comité de nomination de l'ICANN, une autre comité de clients permanents et une autre comité de révision de l'évolution de la zone racine.

Le caucus RSSAC a plus de 100 membres qui sont des experts techniques dans le DNS. Comme je l'ai dit, toute personne qui est intéressée peut se porter candidate en envoyant une manifestation d'intérêt publique et puis également être créditée pour son travail individuel. Donc le travail du RSSAC, vous pouvez y être impliqués en faisant partie du caucus RSSAC. Comme je l'ai dit, c'est ces experts techniques qui amènent leur expertise à nos publications.

Il y a deux groupes de travail actifs actuellement au sein du RSSAC. Premièrement, en matière d'analyse des comportements modernes des résolveurs, ils voient un petit peu quel est le comportement des logiciels déployés qui existent et des résolveurs récursifs. Autre thème, les attentes du système des serveurs racine et moyens de mesure connexes. L'idée, c'est de définir des outils de mesure vérifiables à l'externe et couvrant l'ensemble du système qui démontrent que le RSS dans son ensemble est en ligne et au service de l'utilisateur final.

Il y a deux mécanismes qui contribuent à la transparence du RSSAC et des RSO. Je vais vous en mentionner quelques uns. Vous avez rssac.icann.org qui est une page web où vous pouvez trouver tous les noms des membres du RSSAC, du caucus du RSSAC, vous pouvez avoir accès à tout ce qui a été publié. Vous pouvez également y trouver les procès verbaux de nos réunions. Il y a des réunions publiques du

RSSAC donc si cela vous intéresse, vous pouvez participer aux réunions.

Le RSSAC a également des réunions avec d'autres groupes de l'ICANN pendant les réunions publiques de l'ICANN. Par exemple pendant cette réunion, les coprésidents du RSSAC ont fait un point auprès du comité consultatif gouvernemental. Le Conseil d'Administration va également rencontrer le RSSAC et le RSSAC aura une réunion privée avec le SSAC. Donc nous sommes en communication avec les autres groupes.

Le RSSAC publie le RSSAC000 avec toutes les procédures opérationnelles qui sont décrites, ce qui permet de travailler de manière transparente.

Les RSO également ont des informations qui sont publiques. Vous avez donc la page root-servers.org. Andrew vous a montré qu'il y a des instances dans le monde entier, on peut les trouver sur cette page. Les opérateurs de serveurs racine, les RSO, ont donc leur propre page aussi avec des rapports collaboratifs qui sont publiés sur les manifestations majeures. Et comme Andrew l'a dit, vous pouvez si vous avez des questions les envoyer à ask-rssac@icann.org pour obtenir des réponses.

Pendant cette deuxième partie de la présentation, je vais parler du travail qui est en cours sur l'évolution du système de serveurs racine. Commençons par regarder le calendrier du travail.

Il y a un peu plus d'un an, le RSSAC037 et le RSSAC038 ont été publiés. Ils proposaient un nouveau modèle de gouvernance du système de serveurs racine. Le Conseil d'Administration de l'ICANN a demandé à ICANN Org de consulter ces documents et d'y travailler. Ensuite en avril 2019, l'ICANN a publié un document de concept. Et en août 2019, il y a eu une période de commentaires publics par rapport à ce document qui s'est terminée, donc la consultation a été reçue des différents groupes. Et c'est en consultant ces différents commentaires que nous sommes passés à l'étape suivante en janvier 2020. Donc en janvier 2020, il y aura un groupe de travail sur la gouvernance qui sera formé et qui travaillera sur l'élaboration d'un modèle pour 2020-2021. Et d'ici 2022, le nouveau modèle sera mis en œuvre.

Voyons un petit peu de quoi il s'agissait dans ce RSSAC037. Il définit les 11 principes de fonctionnement et d'évolution du système de serveurs racine. Il propose un modèle initial de gouvernance pour le système de serveurs racine et ses opérateurs. Et il démontre également comment le modèle RSSAC037 fonctionne en utilisant un ensemble de scénarios sur la désignation et le retrait d'opérateurs.

Sur cette diapositive, vous voyez trois recommandations qui sont en complément au RSSAC037 : premièrement, lancer un processus pour produire une version définitive du modèle basée sur le RSSAC037 ; deuxièmement, faire une estimation des coûts du système de serveurs racine et mettre au point le modèle, donc les efforts initiaux doivent se focaliser sur la mise au point du calendrier ; et enfin, mettre en œuvre la version définitive du modèle sur la base des principes de responsabilité, de transparence, de durabilité et d'intégrité du service.

Ce que vous voyez là, c'est un diagramme qui reflète la proposition. Il y a trois différents domaines : il y a la gouvernance, il y a les opérations de racine et il y a l'intégration et le départ des opérateurs de serveurs racine. Dans la partie gouvernance, vous voyez trois parties prenantes : la communauté de l'ICANN, l'IETF et le comité de l'architecture et les opérateurs de serveurs racine.

Cette diapositive vous donne également les cinq fonctions qui ont été proposées dans le modèle, c'est-à-dire la fonction de performance de surveillance et de mesure. Il y a la fonction de retrait, il y a la fonction financière, il y a la stratégie, l'architecture et les politiques et il y a la fonction secrétariat. Ces cinq fonctions ont été proposées dans le cadre du modèle. Ensuite, vous notez au bas de cette diapositive qu'il y a certaines unités de mesure de performance qui vont être utilisées pour ce qui est de l'intégration et du retrait des opérateurs de serveurs racine.

Je viens de vous parler des fonctions. Donc pour revenir à ce modèle de concept, ce modèle prévoit la structure suivante en fonction du modèle 037. L'un, c'est le conseil de gouvernance du système des serveurs racine, l'autre c'est le comité permanent du système des serveurs racine, le panel de révision des opérateurs de serveurs racine et pour ce qui est des dernières fonctions, les finances et le secrétariat, ICANN Org.

Ce document de réflexion souligne un processus qui est conduit par la communauté pour finaliser un nouveau modèle de coopération et de gouvernance conformément à la recommandation un du RSSAC038.

Dans la phase un, l'organisation ICANN fait une révision et une évaluation du RSSAC037. C'est d'ores et déjà fait.

Dans la deuxième phase, le RSSAC037, le document de réflexion et le groupe de travail sur la gouvernance et les documents pertinents sont disponibles pour commentaires publics. Dans la troisième phase, nous développons un nouveau modèle de coopération et de gouvernance pour RSS avec deux pistes de travail, l'une structurelle, l'autre administrative.

Pour ce qui est de la piste structurelle, le groupe de travail sur la gouvernance développe un modèle tandis que pour la piste administrative, il s'agit de mettre en œuvre un modèle du groupe de travail sur la gouvernance qui est géré et conduit par l'organisation ICANN.

Qu'est-ce que ce groupe de travail sur la gouvernance et comment est-il constitué ? Il est constitué de représentants du RSSAC, des organisations de soutien aux ccTLD, donc la ccNSO, l'IAB, le groupe des parties prenantes des opérateurs de registre et du SSAC. Il y a également des liaisons auprès du Conseil d'Administration de l'ICANN, de l'IANA et des responsables de maintenance de la zone racine. Ils sont chargés de peaufiner les détails de ce modèle. Et le document de réflexion met en exergue également certaines lignes directrices sur lesquelles doivent travailler les membres du groupe de travail sur le gouvernance, travailler de manière ouverte et transparente, trouver des contributions éclairées si nécessaire et respecter les principes

décrits dans le RSSAC037 et faire référence au RSSAC037, au document de réflexion et aux commentaires publics reçus à la suite.

Nous allons maintenant passer à la séance questions et réponses avec la salle. Nous avons des représentants des opérateurs de serveurs racine, des membres du RSSAC, donc je vais leur suggérer de venir nous rejoindre sur l'estrade pour voir s'il y a des questions dans le public. Sachez qu'il va y avoir des micros volants dans la salle donc si vous avez une question, levez la main, quelqu'un viendra vous voir avec un micro pour que vous puissiez poser votre question.

STEVE CONTE : Je vois qu'il y a une question ici pendant que les intervenants prennent place au panel. Alors, première question ici dans la salle.

ORATEUR NON-IDENTIFIÉ : Bonjour. Je ne suis pas technicien et je me demande comment déterminez-vous quand et à quel moment vous avez besoin d'une nouvelle instance du serveur racine ? Ensuite, quelle est la différence entre les serveurs de noms, serveurs récursifs ? Quelle est la différence exactement ?

FRED BAKER : En fait, il y a tout un processus que l'on suit qui commence par une évaluation des besoins et voir pourquoi on a besoin d'un nouveau serveur et pourquoi on a besoin d'un nouveau RSO, opérateur de serveurs racine. S'il y a un besoin valable, il y a toute une série de

principes qui nous permettent d'identifier une compagnie ou une organisation, une entreprise qui puisse le faire et qui veuille le faire. D'ailleurs, je vous suggère vivement de lire le RSSAC037 puisqu'il couvre tout cela.

WES HARDAKER : En fait, je pense qu'il parlait plus des instances de serveurs racine et non pas des opérateurs de serveurs racine.

FRED BAKER : Pour ce qui est des instances de serveurs racine, il faut vous adresser à nous, à l'un des opérateurs de serveurs racine. Par exemple mon entreprise, si vous allez sur notre site web isc.org, vous allez trouver sur le site « Cliquez ici si vous voulez un nouveau serveur racine et une nouvelle instance de serveur racine ». Donc on parlera avec vous de vos besoins et on a certaines attentes pour ce qui concerne les connectivités IPv4 et IPv6 au système. Il faut qu'il y ait une bonne connexion, une bonne connexion électrique, etc. Ensuite si tout se passe bien, nous allons signer un protocole d'accord et nous allons opérer le serveur à distance. Et si vous en voulez un, il vous suffit de demander et on entame un dialogue.

WES HARDAKER : J'aimerais ajouter. En fait, on a des requêtes de différentes parties. On a des requêtes de gens qui nous disent : « Oui, on se lance là-dedans, on est disposés à aider. » Mais ensuite, on a des requêtes ou des conditions internes. Moi par exemple, j'essaie de déployer dans des

régions où on ne déploie pas forcément énormément. Donc il y a des gens qui pensent que dans leur zone ou dans leur région, ce n'est pas suffisamment bien déployé ; donc voilà, moi, je m'occupe de cela.

BRAD VERD : Ce que vous entendez ici, ce sont différentes approches parce que chacun des opérateurs de serveurs racine a son propre point de vue et prend ses propres décisions en fonction d'un besoin, en fonction d'un besoin de trafic, en fonction d'un besoin qui justifierait telle ou telle instance.

Mais je pense que la deuxième partie de votre question par rapport aux résolveurs récursifs, nous, nous nous occupons des résolveurs récursifs pour la racine et le résolveur récursif, c'est ce à quoi vous vous adressez, c'est votre intermédiaire finalement entre tous les résolveurs faisant autorité, .us, etc. Donc vous ne parlez probablement pas à vos résolveurs récursifs. C'est le résolveur récursif qui ensuite nous parler à nous si la réponse est en cache.

Est-ce que j'ai bien répondu à votre question ?

OZAN SAHIN : Autre question ici dans la salle.

ORATEUR NON-IDENTIFIÉ : Merci. En fait, je ne sais pas si ma question s'adresse à la bonne personne ou pas. Mais par rapport au DNS sur HTTPS, ma question est de savoir si Firefox et Chrome d'ici quelques mois ou quelques

semaines, ce qui représente 95 % du trafic internet, va être chiffré ou pas. C'est ma question. Quel va être l'impact ? Est-ce que cela va changer ou est-ce que cela va être la même chose mais caché ? Parce que je ne vois aucun panel là-dessus sur tout le calendrier de l'ICANN et c'est une question important. Donc si vous ne pouvez pas me répondre, peut-être que vous pouvez m'indiquer qui peut répondre à cette question.

WES HARDAKER : Moi, je siège à l'IAB qui participe avec l'IETF pour faire avancer ce travail en termes de processus de normalisation. Donc par rapport au déploiement de Firefox et de Chrome, ils font deux déploiements très différents d'ailleurs donc ne vous trompez pas là-dessus, entre le navigateur, internet et le résolveur. Et Firefox prend un résolveur par défaut sur Cloudflare et ils le choisissent par défaut aux États-Unis ce mois-ci. Et dans les autres pays, ils cherchent un autre résolveur. Pour les autres résolveurs, cela n'inclut pas les serveurs racine mais les ccTLD .com, etc.

Chroma à l'inverse fait quelque chose de différent. Ils essaient de voir si les résolveurs de fournisseurs de service internet peuvent le faire et si c'est le cas, ils vont le faire avec le fournisseur de service internet. Là, ce sont deux déploiements totalement différents. Malheureusement, il y a beaucoup de confusion autour de cela parce que l'information change tellement rapidement, même Firefox a pris une décision très récente aux États-Unis par rapport à Cloudflare. Mais dans deux semaines, on va en parler à la réunion de l'IETF à

Singapour. Mais dans quelques mois, cela va changer parce que les choses changent très rapidement.

BRAD VERD : Une fois encore, j'aimerais redire que cela, c'est entre le client et le résolveur, savoir si le chiffrement a lieu ou pas. Je dirais qu'on en a parlé à l'ICANN, c'était une question qui a suscité beaucoup d'intérêt à Marrakech donc je vous renvoie à l'agenda de Marrakech. Il y a eu une grande présentation qui a été faite par le RSSAC et la ccNSO me semble-t-il. Il y a eu un panel qui a parlé de cela et il continue à en parler. Je sais que le RSSAC continue d'y travailler et il y a un travail en cours. Donc cela attire beaucoup d'Attention.

FRED BAKER : J'aimerais poser une question sur le DNSSEC. Les navigateurs ne peuvent pas forcément déployer le DNSSEC. Donc lorsque le navigateur va sur DoH, est-ce que le DNS est vérifié ?

WES HARDAKER : Excellente question, Fred.

Il y a deux aspects à la sécurité en général : le chiffrement et la protection des données et ensuite, savoir si les données sont authentiques, s'il s'agit de données correctes. Elles peuvent être chiffrées mais mauvaise. Vous pouvez avoir un fichier de données erronées.

Le DNSSEC protège de l'origine, c'est-à-dire l'endroit où la donnée a été créée, dans ce cas-là c'est l'IANA, responsable de la maintenance des données et de la plupart des TLD et tout ce qui suit. Vous pouvez me le cacher sur un bout de papier et je peux trouver la signature, où cela a été créé, depuis l'IANA jusqu'en bas.

Donc pour revenir à votre question, DoH fait aussi l'intégrité mais c'est uniquement entre deux points. Donc si cette entité au-dessus du résolveur à laquelle vous parlez sait où se cache cette information, certains résolveurs DoH font de la validation DNS. Donc si vous parlez à un résolveur DoH sur une chaîne de résolveurs particulière, Cloudflare me semble-t-il fait une validation par défaut. Je ne sais pas pour ce qui est du reste.

BRAD VERD : Ce serait à creuser.

STEVE CONTE : Vous vouliez intervenir de nouveau ?

ORATEUR NON-IDENTIFIÉ : Les données ne sont pas visibles pour un fournisseur de service internet ? Ils ne peuvent plus voir les erreurs et tout ce qu'il y a mais vous, vous pouvez le voir ? Donc qui va encore pouvoir avoir une visibilité sur les requêtes DNS et qui ne va plus avoir de visibilité là-dessus ?

WES HARDAKER : Comme je vous disais, je peux vous donner la réponse aujourd'hui mais demain, ce sera différent. Cela, c'est vrai pour les gens qui utilisent Firefox mais le fournisseur DoH comme Cloudflare va pouvoir le voir. Et à partir de là, cela dépend.

Si vous posez une question à un moment donné, vous dites : « Il faut que je vous pose la question. » Vous pouvez poser la question « Où est le site web ? » Il y a toujours une personne qui va pouvoir répondre à votre question. Mais pour Chrome, de l'autre côté, étant donné qu'ils vont faire DoH par le fournisseur de service internet, cela ne va pas changer la visibilité du fournisseur de service internet. Cela dépend de la situation. Et Chrome et Firefox font deux choses différentes pour ce qui est de DoH. Donc c'est difficile de répondre à votre question par oui ou pas non ; cela dépend.

FRED BAKER : Peut-être que c'est le bon moment de parler d'un projet sur lequel on travaille à l'IETF qui concerne la minimisation, l'idée de donner aussi peu d'information que possible mais qu'elle soit aussi correcte que possible. Par exemple www.exemple.com, je vais demander à mon résolveurs récursif. Mon résolveur récursif va dire : « Je ne sais pas où est .com. » Et plutôt que d'envoyer le nom en entier à un serveur racine, ce qu'il fait maintenant, il va envoyer com au serveur racine. Le serveur racine va savoir quel est le nom et il va demander www.exemple.com. Donc ainsi, les serveurs récursifs auront eux-seuls accès à ces informations.

ORATEUR NON-IDENTIFIÉ : L'autre partie, c'est l'agrégation. Si vous avez des milliers de personnes qui vont vers le même résolveur récursif, alors ce résolveur récursif sait que vous avez fait cette requête et a obtenu des milliers de requêtes mais cela ne peut pas forcément être attribué à un individu mais une personne qui utilise ce résolveur récursif.

OZAN SAHIN : Merci. Question suivante s'il vous plaît.

ORATEUR NON-IDENTIFIÉ : Bonjour. Je voudrais savoir si les DSO retiennent des logs. Et qu'en est-il de la confidentialité ?

BRAD VERD : On a entendu DSO. Vous parlez de DSO ou RSO ?

Je n'ai pas entendu la première partie de la question mais pour répondre à la deuxième partie de la question, c'est très simple. Je dirais que maintenant, c'est un mandat non financé. Donc à mesure que l'internet a cru de manière exponentielle et qu'il y a un certain nombre de choses qui ont été ajoutées, depuis 1998, il n'y a pas eu de nouveau résolveur récursif. Je crois que c'est en 1991 qu'Anycast a été introduit. Donc on est passé de 13 identificateurs, 13 serveurs à plus de 1 000 résolveurs mais avec 13 identificateurs toujours. Mais c'est autofinancé par chaque organisation.

Pour répondre à la première partie de votre question, est-ce que vous pourriez la répéter s'il vous plaît ?

ORATEUR NON-IDENTIFIÉ : J'aimerais savoir si vous avez des listes de requêtes et je voudrais comprendre quelles sont les règles en matière de protection de la vie privée.

BRAD VERD : La seule chose que je pourrais vous dire de regarder, c'est que tous les ans, vous avez une collecte numérique. C'est en fait un jour dans la vie, un Diddle comme on le dit en anglais. Donc c'est un détail, une collection de 24h qui rassemble toutes les données de ce que fait l'internet dans une journée. Donc tous les opérateurs de serveurs racine peuvent apporter leur contribution, de même que les TLD, les ccTLD, les grands opérateurs de DNS, les grandes organisations. Donc c'est un effort communautaire. Et ces données sont stockées dans la base de données. Et pour avoir accès à la base de données, vous devez devenir membre et signer un contrat relatif à la confidentialité, etc.

WES HARDAKER : Un autre point. Beaucoup d'opérateurs anonymisent les données avant de les donner à l'organisation. Donc cela veut dire que l'adresse IP est anonymisée mais au départ, c'est de toute façon un résolveur. Donc ce n'est pas lié à une machine, c'est lié à un résolveur. Et surtout avec ce qui est plus récent, avec le RGPD, il faut aller parler à chacun. Je ne sais pas quel est le statut exact, la situation exacte en termes d'anonymisation.

OZAN SAHIN : Autre question dans la salle.

ORATEUR NON-IDENTIFIÉ : D'abord, je souhaite m'excuser parce que je pense que la question sera difficile.

Tout à l'heure, au début dans les diapositives, je me suis rendu compte que la plupart des organismes qui détiennent les adresses IP pour les serveurs racine sont des organismes américains, donc je me demandais la chose suivante. Dans un monde où le gouvernement américain ne va pas vraiment faire de commentaire sur la question de la neutralité, y a-t-il des mécanismes qui permettent de s'assurer que les serveurs racine, donc la colonne vertébrale de l'internet, restent neutres ?

FRED BAKER : Je vais y répondre mais il y a probablement plus d'une réponse à cela. En tout cas, ce que fait le RSSAC actuellement, c'est de travailler sur la question de la mesure du système. Et une des choses qui nous préoccupe en fait, c'est de savoir si le RSO qui est mesuré – et on les mesure tous, on les évalue tous mais parlons d'un exemple, d'un RSO – de s'assurer qu'il est bien au service du système qui vient de l'IANA.

Donc si la zone racine que vous recevez d'un serveur spécifique est différente, ceci est en infraction de manière assez importante. Donc cela, c'est considéré comme négatif.

Donc ce que nous faisons, c'est que nous téléchargeons littéralement toutes les quelques minutes. On télécharge les informations de l'IANA et on vérifie et ensuite, on retélécharge. Donc en fait, on fait passer ce que l'IANA nous a donné.

Alors, que nous a donné l'IANA ? Les TLD, les ccTLD, les gTLD. Moi, j'ai les noms. Ils ont des enregistrements relatifs à l'IANA puisque c'était la partie neutre dans tout ceci qui gérait le système. Donc en fait, ce de quoi on est dépendant en termes de neutralité, c'est de l'étique, de la déontologie de l'IANA et des RSO. Est-ce que cela répond à votre question ?

WES HARDAKER : Attendez, j'aimerais ajouter quelque chose à cette réponse. Je vous recommande de lire le document 23 du RSSAC qui correspond à l'historique de la mise en place du système de serveurs racine. On en parlait justement tout à l'heure lors de notre réunion du RSSAC. Vous pouvez d'ailleurs y assister et écouter ce dont on parle. Mais cela nous explique comment est-ce qu'on en est arrivé à ce point-là avec les organismes qui existent. Tout ceci est basé sur un historique et pendant 20 ans, rien n'a changé. Le RSSAC27 avait pour objectif de voir comment est-ce qu'on pouvait évoluer par rapport à ce système justement.

Je parlais tout à l'heure du DNSSEC. Lorsque vous faites une validation du DNSSEC et si votre domaine est validé de haut en bas, vous savez qu'il n'y a pas eu de modification. Quel que soit le pays par lequel vous êtes passé, c'est complètement indépendant parce que du

point de vue technique, il serait impossible de fausser ces données. Donc je pense que c'est vraiment votre réponse, d'avoir un résolveur validé par le DNSSEC.

BRAD VERD : J'aimerais encore ajouter quelque chose à cette réponse. Le RSSAC037, qui a été publié et qui est donc à disposition de tous, vous donne un petit peu les principes directeurs définis par les opérateurs de serveurs. Et un de ces principes directeurs est justement de rester neutre. Donc le point de vue est vraiment apolitique. Il n'y a pas de politique impliquée. Nous desservons la zone racine telle qu'elle nous a été livrée par l'IANA.

En ce qui concerne le commentaire sur le fait que ce soit basé aux États-Unis, cela, c'est un résultat de la croissance organique. L'internet a commencé aux États-Unis, il a grandi aux États-Unis, il avait besoin d'opérateurs de serveurs racine et voilà pourquoi on en est là. C'était simplement une question de croissance organique.

FRED BAKER : Et nous avons des opérateurs de serveurs racine qui sont en dehors des États-Unis ; il y en en Suède, un au Pays-Bas et un au Japon.

STEVE CONTE : Nous avons une question ici dans l'ombre à votre droite.

ORATEUR NON-IDENTIFIÉ : Vous savez que les attaques deviennent de plus en plus virulentes et les attaques de déni de service se poursuivent. Alors que peut-on faire pour continuer de protéger les serveurs racine ? Est-ce que le RSSAC a des réunions avec le SSAC pour s'assurer que les serveurs racine sont bien protégés par rapport à ces attaques et comment est-ce que cela fonctionne ?

BRAD VERD : Je peux vous envoyer à la publication d'un document qui justement répond à votre question directement. C'est un document sur les menaces au système de serveurs racine. Donc ils expliquent ce qu'ils ont fait pour répondre à ces menaces générales.

Par rapport au RSSAC maintenant, les RSSAC est en conversation constante avec le Conseil d'Administration, avec le SSAC sur toutes les menaces éventuelles du système. On a parlé de DoH et de DoT, on a parlé des répercussions sur l'infrastructure lorsque quelque chose de ce type se produit. Donc ces conversations ont lieu constamment. Mais la question opérationnelle a lieu entre les RSO et au niveau des RSO lorsqu'il y a un DDoS ou un partage d'informations, donc lorsqu'il y a atténuation.

WES HARDAKER : Où peut-on trouver ce document ?

BRAD VERD : Pardon. Le document n'est pas un document RSSAC. C'est un document qui se trouve sur la page web des serveurs racine, donc root.servers.org. Je crois que c'est en haut de la page.

ORATEUR NON-IDENTIFIÉ : Parfait, merci beaucoup.

Est-ce que je peux poser une dernière question ? Je sais que sur les serveurs, lorsque le DNSSEC n'est pas bien configuré, il y a le potentiel d'attaques d'amplification. Donc j'aimerais savoir dans le cadre du déploiement du DNSSEC s'il y a moyen d'essayer de pousser un petit peu pour un DNSSEC durci pour les serveurs configurés, donc avoir des méthodes un petit peu différentes. En 2013, on avait beaucoup travaillé sur le durcissement du DNSSEC.

WES HARDAKER : Est-ce que vous pouvez ajuster votre question ? Vous parlez d'une mauvaise configuration et du DNSSEC, je ne sais pas si c'est trop large ou trop précis.

ORATEUR NON-IDENTIFIÉ : Oui, si par exemple le n'a pas été bien configuré, vous avez donc ce serveur puis vous avez une attaque avec usurpation d'adresses IP. Donc cela pose problème et finalement, l'attaque d'amplification est plus importante.

WES HARDAKER : Donc en fait, ce qui vous inquiète, c'est une attaque de réflexion. Les DNSSEC ajoute des données donc les signatures deviennent très larges, les clés sont très larges. Et vous avez raison, par le passé, le DNSSEC était utilisé comme attaque de réflexion parce qu'on envoyait les attaques là où il y avait beaucoup de trafic.

Donc de nos jours, la plupart des serveurs et je ne parle pas seulement des serveurs racine, mais la plupart des serveurs ont des technologies qui utilisent ce qu'on appelle un limiteur de taux de réponse. Donc le serveur ne pose pas beaucoup de questions. Il vient un moment où je ne veux plus te parler. Tu peux me parler mais il faut que tu m'envoies une communication beaucoup plus difficile à usurper. Donc c'est complètement différent. Avant, la plupart des gens ne mettaient pas ceci en marche, donc il y avait un trafic très important et puis au bout d'un moment, les gens se sont rendus compte que ce n'était pas un moyen viable. Donc on ne voit plus maintenant ces attaques de réflexion avec le DNSSEC.

STEVE CONTE : Merci beaucoup. D'autres questions ? Il n'y a pas de question en ligne. Y a-t-il des questions dans la salle ?

WES HARDAKER : Ce sont d'excellentes questions bien techniques. Merci.

STEVE CONTE : J'aimerais remercier Andrew et Ozan pour leurs excellentes présentations. Je voudrais également remercier les opérateurs de serveurs racine d'avoir répondu à ces questions.

Et je vais faire une petite page pub. Je sais que la journée est pratiquement terminée mais nous avons une séance toute nouvelle qui commence à 17:00 dans la salle 512G. Et Erin va nous parler des registres internet régionaux, de ce qu'ils font et de certaines notions de base là-dessus. Donc encore une séance à 17:00, 512G, une séance sur les registres internet régionaux.

Ceci étant, merci à vous tous, merci Ozan, merci Andrew et merci à ceux qui étaient dans la salle.

WES HARDAKER : Il y a également une autre page pub. Il y a également une présentation sur le DNSSEC pour les débutants et c'est également à 17:00. Donc venez à celle-ci plutôt.

STEVE CONTE : Merci à tous.

[FIN DE LA TRANSCRIPTION]