SAN JUAN – Séance quotidienne des boursiers
Lundi 12 mars 2018 – 12h00 à 13h30 AST
ICANN61 | San Juan, Porto Rico

SIRANUSH VARDNYAN: Oui si vous voulez bien récupérer un déjeuner, venez vous assoir, nous avons encore 5 minutes pour commencer.

NON IDENTIFIE : Bonjour ICANN 61, 12 mars, séance des nouveaux venus.

NON IDENTIFIE : Est-ce qu'on peut me promouvoir en tant que présentatrice de la session s'il vous plait ?

SINANUSH VARDANYAN : Vous pouvez donc obtenir un petit déjeuner au fond de la salle et ensuite venir prendre votre place. Rapprochez-vous s'il vous plait, donc les boursiers je veux voir tous vos visages.

Est-ce que nous avons des micros volants pour la salle, merci ?

Encore une fois, est-ce que nous avons des micros volants ? Oui, merci.

NON IDENTIFIE : Voilà les micros qui arrivent.

SIRANUSH VARDANYAN : Nous ne sommes pas enregistrés encore ? Est-ce qu'on nous enregistre ? Nous ne voulons pas être enregistrés, n'est-ce pas ?

Bienvenus à la séance des boursiers journalière, aujourd'hui nous avons une séance spéciale, nous avons nos gourous techniques qui sont là pour vous faire des présentations.

Je voudrais maintenant donc passer la parole à Rachel Reyes pour qu'elle se présente ainsi vous pourrez savoir qui fait la présentation.

Amenez vos boites, petits déjeuners à la table, et préparez-vous car cette séance va être très intéressante.

RACHEL REYES: Bienvenus à tous, bienvenus à la séance sur les fondamentaux du DNS. Nous allons donc passer 15 à 30 minutes ensuite pour que vous puissiez poser des questions.

Je suis Rachel Reyes, je suis soutien technique pour ICANN.ORG. John Crain, qui est là aussi, qui est assis à côté de moi et qui va m'aider avec la portion des questions/réponses.

JOHN CRAIN: Je suis responsable de la sécurité et la stabilité pour ICANN, et je participe à l'opération des serveurs racines. Je travaille sur ce sujet depuis 20 à 30 ans d'ailleurs.

[2]Là-bas, au téléphone à ma droite, c'est monsieur Matt Larson, c'est Monsieur DNS comme on l'appelle, il est dans cette industrie depuis plus longtemps que moi.

Avec ça je vais passer la parole à Rachel.

RACHEL REYES: J'espère que nous allons pouvoir atteindre votre attention pendant votre déjeuner.

Donc les adresses IP sont des machines faciles à utiliser, c'est vrai. Mais il est facile de se rappeler des noms. Mais il est difficile de se rappeler des chiffres. Par exemple, certains d'entre nous ont du mal à se rappeler les numéros de téléphone de nos familles ou de nos amis. C'est la même chose pour le DNS.

Au début de l'internet, les noms étaient très simples, du moins les noms de domaine étaient simples. Il y avait donc une étiquette simple, unique, avec 24 caractères.

La résolution des noms est donc d'organiser les adresses IP et de les transférer en nom.

Au début de l'internet, les noms, les systèmes utilisaient des chiffres, et maintenant nous le faisons à travers des centres d'information réseau, ce que nous appelons NIC, des centres d'information de réseau donc.

Il suffit donc de mettre à jour les documents par courriel, ça se fait une semaine, et cela peut être téléchargé par FTP ; et c'était comme ça que cela fonctionnait au début, dans les premiers jours de l'internet.

Le problème avec ces systèmes c'est que tout était édité, donc corrigé de façon manuelle, donc il y avait beaucoup d'erreurs. Et ce n'était pas très efficace, car il fallait envoyer un courriel avant que la mise à jour soit faite. Donc cela demandait une grande largeur de bande parce qu'il fallait télécharger les documents.

C'est pour cela que les gens avaient donc commencé à discuter dans les années 1990 sur comment ils allaient remplacer le système.

Donc le concept du DNS a commencé et cela a simplifié le routing des courriels. Vous pouvez trouver plus de documents sur les exigences, sur les RFC que vous voyez à l'écran. Donc vous parlez du RFC799, et le RFC819 qui vous donneront plus d'informations sur les exigences de ce nouveau concept du DNS.

En résumé, le DNS, qu'est-ce que c'est ? Nous allons discuter de la terminologie que nous utilisons dans le système DNS, nous avons les données, les résolveurs, les noms de serveurs, les caches et les applications.

Vous voyez, le graphique sur l'écran.

Nous avons les résolveurs, c'est donc ce qu'on appelle les résolveurs stub et nous avons les serveurs de noms. Vous voyez à ma gauche et donc à votre droite Et ces serveurs de nom sont ceux qui envoient des réponses aux demandes qui sont envoyées par les serveurs récursifs. Vous voyez une petite bulle sur l'écran qui dit « cache ». La cache, on l'utilise dans le système DNS pour rendre les choses plus efficaces et plus échelonnables.

Nous n'allons pas rentrer trop en détail, parce que nous le ferons tout à l'heure dans la présentation.

L'espace des noms, ça correspond à la structure des bases de données du DNS. Nous avons une structure descendante, mais dans notre monde DNS, il s'agit d'une structure ascendante.

Par exemple nous ne lisons pas les « .COM.EXEMPLE.WW », nous lisons cela en tant que « WW.EXEMPLE.COM », c'est ce qu'on appelle la qualification des noms de domaine.

Dans notre espace, la première chose c'est la racine, ensuite vous avez les nodes de premier niveau, les nodes de deuxième niveau et les nodes de troisième niveau.

Chacune de ces nodes ont des étiquettes qui consistent au caractère légal que l'on peut utiliser et ceux-ci sont des LDH.

La longueur maximale pour une étiquette est de 63 caractères. Ce n'est pas très sensible au niveau des clefs, vous pouvez écrire .COM comme COM, vous pouvez bien sûr utiliser une majuscule, c'est égale.

Toutes les nodes ont donc un nom de domaine dans notre exemple, nous allons utiliser cet arbre, ce graphique. L'étiquette qui est soulignée, c'est le WWW.EXEMPLE.COM. Tout cela est séparé par des points.

Comme je l'ai dit tout à l'heure, les DN qualifiés sont FQDN et cela termine avec un point. Lorsque nous essayons de trouver un nom de domaine, nous n'utilisons pas toujours un point à la fin, mais nous tapons exemple.com, etc.

Un domaine est node, et tout ce que cela comprend. Dans notre exemple, .COM est le node principal de notre domaine. En dessous, vous avez les territoires de .COM ou les territoires qui correspondent au domaine .COM.

Les zones correspondent à tout ce qui est administratif. Chaque zone est basée sur les frontières qui correspondent aux autorités différentes et cela est délégué à une entité, une zone peut avoir un domaine ou plusieurs domaines ou des sous-domaines.

La délégation donc crée des zones, la zone déléguée s'appelle un parent, et donc l'autre c'est ce que l'on appelle un enfant.

Donc la zone racine, le parent, délègue des informations à l'enfant, .COM, UK, par exemple UK, CAFE ; Vous voyez l'exemple à l'écran.

Donc les serveurs de noms, comme je l'ai dit tout à l'heure, sont ceux qui répondent aux demandes qui sont envoyées par le serveur récursif.

L'autorité pour la zone connait bien la zone. Donc quand vous envoyez une demande, si c'est un serveur qui est vide, cela ira directement sur la zone parce que c'est là où il faut que vous alliez pour recevoir la réponse définitive à votre demande. Les zones ont donc des serveurs authoritatifs qui sont multiples pour l'efficacité.

Comment est-ce que vous gardez, vous conservez les données à travers tous ces serveurs ? Nous avons des protocoles internet qui font la duplication des zones. On utilise donc les serveurs primaires et secondaires. Le serveur primaire a donc les

données, et si vous voulez faire un changement dans la zone, vous devez le faire sur le serveur primaire. De l'autre côté, le serveur secondaire, ce qu'on appelle le serveur esclave, c'est celui-là qui va obtenir les données d'un autre serveur. Nous appelons ça le transfert de zone. C'est la communication entre un serveur DNS et un autre serveur d'autorité.

Un autre serveur dont nous devons parler, c'est le serveur principal, le master, c'est là d'où vient le document de la zone. Le serveur master ne doit pas être votre serveur primaire. Votre serveur secondaire peut avoir les mêmes fonctions.

Le transfert est donc initié par votre serveur secondaire et vous pouvez ainsi trouver à travers donc le RFC, le RFC 1996, vous pouvez donc trouver les détails sur ce processus.

Maintenant, nous passons à tout ce qui est document de ressources DNS, c'est ce qu'on appelle les RR. Si vous vous rappelez, comme je l'ai déjà dit tout à l'heure, tous les nœuds ont des noms de domaine. Les noms de domaine ont des tas de données qui sont associées, donc les noms de domaine sont stockés dans les RR. Nous avons des RR différents, mais nous allons seulement débourser certains d'entre eux.

Donc nous allons passer au format que nous utilisons. Les records, donc les RR ont 5 domaines. Le propriétaire, dons le TTL, la classe, le type et le RDATA. Le propriétaire est donc le

nom de domaine avec lequel les informations sont associées. Pour ce qu'on appelle le TTT c'est le temps qui est accordé à chaque donnée, la classe c'est un mécanisme pour l'extension qui n'est vraiment pas tellement utilisé. Le type, c'est le type de données qui sont stockées, et le RDATA correspond aux données qui sont comprises dans le RR.

Quand vous regardez cette nouvelle diapo, vous allez mieux comprendre, je vais vous montrer dans quelques secondes.

Donc voilà l'information que nous appelons les rapports de ressources pour ceux qui connaissent un peu ce qu'on appelle le netwrking, le réseau, vous allez un peu mieux comprendre ce dont je parlais tout à l'heure.

Alors les extensions sont toujours un parent, et cela est nécessaire.

Voilà les ressources qui sont utilisées le plus souvent, donc c'est le A data, les données A pour les adresses IPv4, les 4 A sont là pour les adresses IPv6, et NS, il s'agit du nom de serveur d'autorité, et cela apparait toujours à l'apex de la zone. Comme vous avez vu notre exemple, vous avez vu que vous pouvez trouver les informations au SOA. CNAME, c'est le nom des alias, et MX c'est pour le serveur d'échange de courriels, et PTR, c'est utilisé pour faire du mapping à l'envers.

Il y a beaucoup d'autres types d'informations, depuis décembre 2017 il y en a 84, vous pouvez aller sur ce site web comme vous le voyez à l'écran pour trouver des informations sur ces ressources. Si vous allez sur cette page, voilà ce que vous allez voir.

Alors, nous allons voir ce qui correspond au A et au AAAA. Comme je vous l'ai dit, voilà de quoi ça a l'air, ça va vous donner l'adresse IPv4, et puis les AAAA vous donneront des adresses IPv6.

Le Name Serveur, donc le NS spécifique est un nom de serveur autoritaire pour une zone. Vous pouvez le trouver dans plusieurs endroits, donc ce qu'on appelle les zones parents, les zones enfants. Lorsque vous voyez cet exemple à gauche c'est le nom de la zone et à droite vous avez le nom du serveur, pas l'adresse IP.

Voilà donc comment les records de nom de serveurs sont délégués, nous passons du parent à l'enfant. Donc le .COM a 13 serveurs différents. Voilà donc notre zone racine, donc nos 13 zones racine. Voilà vous les voyez ici. Ca vient de la racine et ça va jusqu'au .COM.

Durant la délégation, nous incluons aussi ce qu'on appelle un record glue. C'est soit un IPv4 ou un IPv6. C'est inclus dans les records des parents, au niveau de la délégation. C'est pour ça

qu'on en a besoin, parce que si, disons on cherche l'adresse IP de WWW.EXEMPLE.COM vous allez aller directement dans la zone racine et la racine vous donnera l'adresse IP d'un nom de serveur et ensuite vous allez demander au nom de serveur quelle est l'adresse de WWW.EXEMPLE .COM, et là vous allez continuer jusqu'à ce que vous puissiez obtenir votre réponse, parce qu'ils n'ont pas encore l'adresse IP. C'est pour ça que nous devons avoir ce qu'on appelle des records glue.

Alors état d'autorité. Donc les SOA. Vous pouvez les trouver à l'apex, donc à l'apex de la zone. Voilà donc un exemple, de quoi a l'air SOA. Il y a donc votre domaine, le nom de votre serveur, il y a l'administrateur qui héberge la zone, et ensuite vous avez le numéro de série qui est la version courante du dossier.

Vous avez donc toutes les mises à jour qui sont faites par le serveur secondaire. Il y a aussi le nombre de secondes de délai pour ce fameux transfert de zones. Il y a aussi le nombre maximum de secondes pour que le serveur secondaire puisse utiliser les données avant qu'il y ait une mise à jour. Le minimum c'est le TTL.

CNAME, donc encore une fois, les records ont été créés pour passer d'un nom de domaine à un autre. Donc à ma droite et à votre gauche, vous allez trouver les noms C, le CNAME et… Oui,

à droite vous allez trouver les noms canoniques et donc la cible de l'alias.

Attention, n'utilisez pas trop ce système-là, ne créez pas une chaine parce que ce n'est pas bon pour vos données.

Alors l'échange de courriel, MX. C'est donc un serveur de courriel et ça vous donne une préférence pour la destination du courriel, par exemple sur notre exemple ici donc sur l'écran, vous avez EXEMPLE.COM MX le nombre correspondant de 10 ou 20 comme vous voyez sur l'exemple, correspond à la priorité. Le chiffre le plus petit est plus intéressant.

Alors le mapping à l'envers, la plupart du temps nous cherchons des adresses IP d'un nom de domaine, mais il y a des fois où nous essayons de trouver un espace de nom pas une adresse IP. C'est là que les PTR peuvent être très, très utiles. Nous n'utilisons pas toujours cela, mais du côté réseautage, vous savez que cela se trouve toujours dans les données.

Voilà donc de quoi ça a l'air. Donc le…

Excusez-moi, encore une fois. Je vais demander à John Crain pourquoi avons-nous IN-ADDR.ARPA.

JOHN CRAIN: Oui, c'est l'adresse mise à l'envers parce que certains protocoles vérifient cela pour s'assurer que les chiffres et les nombres puissent se lire dans les deux sens.

RACHEL REYES: Voilà donc sur l'écran d'autres ressources que nous avons. Mais je ne les vois pas souvent, sauf pour le CDS et CDNSKEY.

Voilà donc un exemple, encore sur l'écran, d'un dossier zone pour exemple.com. Vous voyez le SOA, le nom du serveur, l'IPv4, l'IPv6, et les dossiers MX. Vous avez aussi ce qu'on appelle les glue records, les informations glue, il s'agit des adresses IP comme je vous l'ai dit tout à l'heure.

Maintenant nous allons passer au processus de résolution. Comme je l'ai dit tout à l'heure, nous avons des résolveurs qu'on appelle stub, et ces serveurs coopèrent pour chercher les données DNS dans l'espace des noms. Vous pouvez le faire sur votre téléphone, sur votre ordinateur. Les serveurs vont envoyer des demandes aux serveurs de nom et ceux-ci vont envoyer des réponses aux demandes.

Une demande utilise toujours des demandes non incursives ou itératives. Nous avons des résolveurs, ce qu'on appelle type stub, qui envoient encore une fois des demandes non incursives

ou itératives, ce qu'on appelle des références. On en parlera plus tard.

Voilà, je dois en parler de celle-ci puisque si vous commencez un processus de résolution où le serveur récursif est vide, vous n'avez pas d'autres options que d'aller au serveur de nom de racine parce que les dossiers se trouvent là.

Comment est-ce que ce serveur trouve le serveur de nom ? Il faut faire une configuration et cela doit être fait par l'administrateur.

Voilà, maintenant la liste des serveurs de nom racine et les dossiers de racine.

Alors les serveurs de nom, les IPv4, les adresses IPv4, les AAAA des IPv6.

Alors l'administration de la zone racine est très compliquée, donc on ne va peut-être pas en parler. Nous devrions garder les choses un peu plus simples. Si vous voulez en savoir plus, peut-être pouvez-vous demander à Matt Larson de M&M Peanuts qui aura certainement plus de temps pour vous en parler. Mais nous n'allons pas en parler ici ;

Il y a deux organisations qui coopèrent pour administrer le contenu de la zone. Donc à la base c'est ICANN et puis Verisign.

Il y a aussi 12 organisations qui opèrent les serveurs de nom autoritatifs pour la zone racine.

En fait, vous vous demandez pourquoi 12 puisque nous avons 13 serveurs de racine. Verisign en a 2, le A et le J. Pourquoi en ont-ils deux ? Encore une fois, John et Matt auront des réponses pour vous. Mais ils ne vont pas en parler ici, à moins que John ait du temps pour nous raconter son histoire.

JOHN CRAIN: Non, c'est un facteur historique. La dernière fois que les noms de serveur ont été distribués, dans les années 90 quand les nouveaux noms ont été rajoutés, pas tous ces noms ont été nouvellement organisés.

Un est allé à la côte IS, donc à Verisign, et les autres sont restés en SSI, donc la lettre L et quand l'ICANN est née, cela donc est rentré dans l'ICANN. Et J est resté avec verisign.

C'est juste un petit peu d'historique sur la distribution.

RACHEL REYES: Si vous voulez en connaitre un peu plus en ce qu'il s'agit de la géographie des serveurs racine, vous pouvez aller sur ce site web qui est root-serveur.org. Je vais vous le montrer d'ailleurs.

Disons que vous cherchez la disponibilité des serveurs racine, donc par exemple à Puerto Rico, voilà, le L et le J sont donc disponibles à Puerto Rico en ce moment. Donc vous pouvez aller sur ces sites web si vous voulez en savoir plus.

Nous avons aussi des exemples de serveurs racine qui vous permettront de chercher le DNS ou le serveur racine le plus proche de vous. Ça aide quand on fait une recherche puisque c'est plus efficace.

Nous allons parler maintenant du processus changement de zone racine. Comme je vous l'ai montré sur l'écran, c'est un processus qui a été simplifié, mais il y a beaucoup d'autres processus qui sont inclus.

Donc à la base, vous avez un directeur de TLD qui soumet un changement à l'IANA et l'IANA va mettre en application cette demande à travers la base de données de la zone racine et va créer un dossier et le publier à travers tous les serveurs racine.

Nous avons donc le processus de résolution. Voilà ce qu'il se passe si vous faites une demande, que ce soit sur votre téléphone, ou votre ordinateur ou un autre instrument. Donc si vous… Il y a toujours un résolveur qui est local par rapport au client. Votre client, la question va être celle-ci : quelle est l'adresse IP de exEMPLE.COM. Cette question va passer par votre serveur récursif, avec une adresse comme celle-ci : 4 .2.2, et cela

va poser la question comme ça : quelle est l'adresse IP de WWW.EXEMPLE.COM, et votre serveur récursif va répondre comme cela : je ne sais pas, mais certainement le serveur racine a cette information.

Pourquoi est-ce que votre serveur récursif n'a pas cette information encore ? C'est simple, c'est un nouveau serveur récursif. Comme je l'ai dit, il est soit nouveau ou vide, donc il n'a pas toutes les informations cache encore. Donc cela ira directement vers le serveur racine pour qu'il puisse obtenir l'adresse IP, parce que votre serveur racine a le dossier de la zone racine. Votre serveur racine va donc envoyer la recommandation, l'information, il va vous dire je n'ai pas l'adresse mais j'ai l'adresse de .COM ; le serveur récursif va donc aller vers le serveur .Com et demander l'adresse IP de WWW.EXEMPLE.COM

Votre serveur COM va dire : je ne sais pas, mais je sais que l'adresse IP du serveur de nom est celle-ci. Donc votre serveur récursif va aller vers le serveur de nom exemple.com et ce serveur va donner l'adresse IP ou va retourner vers vous avec une réponse définitive et votre serveur récursif va donc retourner l'adresse IP vers votre résolveur.

Cela fonctionne en quelques secondes, pas en quelques minutes. C'est la même chose si vous lancez une application à

partir de votre téléphone, de votre ordinateur, il arrive que ça prenne un peu plus de temps pour que cette application s'ouvre, mais si vous essayer de re-télécharger une fois de plus, ça va plus vite Pourquoi ? Parce que l'information est déjà envoyée dans le cache de votre client.

Donc, on recommence, le système de cache accélère le processus. Si le cache connait déjà le nom et l'adresse IP de votre zone racine et de votre nom de serveur. Donc si vous essayez d'avoir accès ou si vous essayez de faire une demande sur l'adresse FTP exemple.com, maintenant vous allez pouvoir demander quelle est l'adresse de FTP exemple.com.

Donc votre safari ou votre résolveur va aller vers le serveur récursif une fois de plus et cette fois-ci, cela ne va pas revenir vers la zone racine, ou le serveur de nom, donc encore une fois, il va aller directement vers le serveur de nom, parce que l'information est déjà dans le cache.

Donc utiliser le cache permet au processus d'être plus efficace.

Voilà, le processus est également plus rapide, voici comment le processus fonctionne.

Alors nous avons une diapositive sur le DNSSEC, si vous souhaitez parler en plus de détail du DNSSEC, il y a quelques séances qui seront organisées. Je crois que c'est cette semaine,

n'est-ce pas ? Il me semble. Les gens peuvent participer à un atelier DNSSEC.

JOHN CRAIN: Je vais voir. Nous avons une séance DNSSEC, je crois que c'est le mercredi, je vais vérifier avant la fin de la séance.

NON IDENTIFIE: Il y avait également un tutoriel hier.

RACHEL REYES: Très bien, donc c'est juste les bases là du DNSSEC. Je vais donc vous lire. Donc les données DNS peuvent être signées numériquement pour être authentifiées. Chaque zone a une clef publique ou privée qui fonctionne avec le DNSSEC. Plusieurs enregistrements existent, donc DNSKEY, RRSIG, c'est-à-dire la signature numérique, NSEC, NSEC3, c'est un pointeur vers le nom suivant dans la zone, et DS signature de délégation.

Donc si vous souhaitez en savoir davantage sur le DNSSEC, vous pouvez participer aux séances DNSSEC que nous avons donc mercredi.

L'écosystème du nom de domaine ressemble à ça. Vous avez donc l'opérateur de registre qui détient la base de données pour les titulaires de noms de domaine, ensuite il y a le bureau

d'enregistrement qui est l'agent entre le registre et le titulaire de nom de domaine et le titulaire de nom de domaine qui détient le nom ou le domaine.

Voilà comment le processus de nom de domaine fonctionne, nous n'allons pas parler de tout le processus, mais ce que je suis en train de vous dire c'est que ce dont on a parlé en fait partie de l'enregistrement général des noms de domaine.

Nous avons parlé des serveurs faisant autorité, nous avons parlé des serveurs récursifs et des utilisateurs de l'internet, tout ceci est intégré à ce processus.

Voilà, c'est tout ce que j'avais à vous dire pour la séance d'aujourd'hui.

Si vous avez des questions, n'hésitez pas.

JOHN CRAIN: Avant de passer aux questions, je vais vous donner les dates du DNSSEC, donc c'est mercredi de 9 h à 15 h donc toute la journée sur le DNSSEC. Je pense qu'on n'a même pas besoin de tout ça.

SIRANUSH VARDANYAN: Nous allons passer aux questions. Allez-y.

NICOLAS FIUMARELLI: Bonjour Nicolas Fiumarelli de l'Uruguay, vous avez mentionné que le DNS en fait peu importe les lettres majuscules ou minuscules. Mais qu'est-ce qui se passe en ce qui concerne les noms de domaine internationalisés ?

RACHEL REYES: Matt va répondre.

MATT LARSON: Alors le DNS en lui-même peu importe si vous utilisez les majuscules ou minuscules, les IDN sont une couche en plus.

Alors, Rachel est-ce que vous pouvez revenir en arrière, à la diapositive du début, sur l'espace des noms.

Très bien.

Alors si vous regardez cette diapositive, en fait la lettre en haut à droite, vous avez XN--, donc pour les IDN ce que nous avons fait, c'est que nous les avons ajoutés comme couche supérieure, en plus.

Donc du point de vue de l'utilisateur, si une application est activée IDN, l'application convertit l'alphabet internationalisé avec ce format, donc avec les tirets. Donc du point de vue du DNS, on dirait que c'est simplement des étiquettes normales.

Donc vous voyez XN—c'est un code qui veut dire que le r'este de l'étiquette c'est un nom chiffré IDN. Et il y a le Punycode qui est en fait un petit peut comme l'Unicode qui est un autre nom qui permet de concevoir des caractères justement pour les IDN.

MATT LARSON: Pour vous donner un petit peu plus d'historiques il y a des personnes qui disaient lorsqu'on faisait ceci : mais pourquoi est-ce qu'on a besoin de cette couche en plus du DNS ? Pourquoi est-ce qu'on ne pourrait pas simplement utiliser UTF-8 dans le DNS, avoir des étiquettes UTF-8 dans le DNS.

En fait les gens s'inquiétaient parce que le système DNS ne s'attendrait pas à ceci, il n'était pas conçu pour agir de la sorte. Donc il a fallu ajuster l'infrastructure et il aurait fallu également mettre à jour tous les clients.

Donc voilà pourquoi nous avons procédé de cette manière avec les IDN. Bien sûr qu'il faut mettre à jour les clients, mais au moins on ne touche pas le reste de l'infrastructure du DNS.

Donc la question c'était de savoir est-ce qu'on veut tout changer, les applications et l'infrastructure de DNS ou juste les applications.

SIRANUSH VARDANYAN: Nous avons une question là. Allez-y monsieur.

ABDULKARIM OLOYEDE; Merci, Adbulkarim. Je voudrais poser une question de suivi, vous avez parlé d'une couche qui est sur le DNS. Je comprends, mais si j'ai bien compris, cela veut dire que si vous envoyez une requête au serveur DNS, vous envoyez tout ça au serveur DNS. Donc comment ça se fait qu'il y a cette couche ? C'est un suivi en fait par rapport à ça.

MATT LARSON: Alors la couche sur le DNS, voilà ce que ça veut dire. C'est un concept en fait. Mais c'est à l'intérieur des applications qui comprennent les IDN.

Donc par exemple, lorsqu'on a un navigateur moderne qui comprend les IDN, vous tapez des caractères qui ne sont pas des caractères de l'alphabet latin et vous convertissez le XN--, donc XN--.etc donc c'est pour chaque étiquette qu'il y a internationalisation. Et donc le navigateur envoie la requête au résolveur local, le résolveur local envoie la requête au serveur suivant et donc les tirets sont dans l'étiquette. Donc quand je parle de couches sur le DNS, c'est quelque chose qui arrive au niveau de l'application, pas dans les résolveurs et les serveurs.

ABDULKARIM OLOYEDE: J'ai encore une autre question. Vous avez fait une présentation et j'ai peut-être raté quelque chose quand je mangeais ou alors vous êtes allé trop vite, mais par rapport au serveur de zone, vous avez dit que c'était compliqué. Donc ce n'était pas très clair pour moi ça, qu'est-ce que vous voulez dire par là ? Serveur de zone ?

Vous parlez surtout de serveur de zone primaire, secondaire et vous avez expliqué qu'il y a des esclaves et des maitres donc je n'ai pas bien compris ça.

L'autre partie de ma question, c'est le 4.2.2.2, est-ce que c'est par exemple lorsqu'on envoie une requête de défaut ? Le serveur récursif de défaut pour toutes les requêtes ?

JOHN CRAIN: Alors si vous parlez d'autres types de serveurs de nom, donc serveurs de zone, vous avez parlé de serveurs de zone mais c'est peut-être le serveur de nom…

On va revenir en arrière.

Donc à la base, il y a trois types de serveurs. Il y a le premier, le serveur local, c'est en fait votre ordinateur, ou votre téléphone. Il est dans le système d'exploitation ou dans l'exploitation, dans votre navigateur par exemple. Ça c'est uniquement un serveur qui répond aux questions ;

Ensuite vous avez les serveurs récursifs qui sont soit avec le FSI, et ce sont eux qui vont faire passer la question aux serveurs faisant autorité. Et ces serveurs faisant autorité ont les réponses. Voilà pourquoi on les appelle faisant autorité, parce qu'ils ont l'autorité, ils peuvent répondre.

Sur les récursifs, vous avez en fait un moteur qui pose des questions, qui envoie les requêtes et les seules données qui existent dans ce serveur c'est uniquement les données qui sont dans le cache.

Le résolveur local peut lui aussi avoir un cache avec des données.

Donc vous avez un cheminement de votre dispositif et donc qui remonte jusqu'en haut.

Alors il y avait un commentaire par rapport à la complexité par rapport à [l'avitaillement] de la zone racine, c'est à ça que vous faites référence ? Je ne sais pas.

Mais ça c'est quelque chose d'autre, c'est un système d'avitaillement du système de serveur de nom. Je vais demander à Matt d'en parler parce qu'il a déjà parlé de ce type de chose, il a déjà travaillé sur ce type de chose.

En ce qui concerne les serveurs récursifs et savoir lequel on utilise, cela est défini lorsque vous installez votre ordinateur sur

votre réseau. Lorsque vous vous connectez à un réseau, ici par exemple, vous utilisez le protocole DHCP.

C'est ce qui vous envoie votre adresse IP que vous utilisez, mais c'est également ce qui définit quel va être serveur faisant autorité.

Vous pouvez en avoir 1, 2, 4. Toutes vos requêtes passeront par ces serveurs qui auront été configurés.

SIRANUSH VARDANYAN: Il y a une question d'un participant à distance. Ah attendez pardon, vous n'aviez pas fini.

MATT LARSON: Vous avez posé la question du 4.2.2.2, c'est un serveur qui est opéré par des communications de niveau 3 par un FSI, c'est en fait un serveur récursif ouvert. Lorsqu'on a beaucoup de clients, donc en fait c'est dans n'importe quel réseau, si vous avez un FSI pour un client de large bande ou là dans le réseau ICANN, donc vous avez le premier niveau donc le résolveur local, vous devez avoir ensuite un serveur récursif. Et donc le fournisseur de réseau s'occupe de faire la connexion et il se configure.

Mais vous n'êtes pas obligé d'utiliser le serveur récursif, vous pouvez en utiliser un autre. Et il y a des serveurs récursifs

ouverts qui acceptent les requêtes de n'importe qui. Ce sont des serveurs de parties tiers, ce sont des serveurs publics, et c'est une adresse très simple.

Et par exemple celui de Google est facile à utiliser parce que l'adresse est très facile à mémoriser. Donc vous pouvez l'installer sur votre téléphone, c'est le 8.8.8.8, c'est très facile donc c'est très plébiscité.

Et il avait des gens qui avaient dit : il faut avoir des résolveurs récursifs en dehors de votre réseau. Donc Verisign en a, PCH a le Qaud9 ; 9.9.9.9, donc il y en a plusieurs qui sont publics. Et le 4.2.2.2 c'est un résolveur de niveau 3 qui existe depuis très longtemps.

SIRANUSH VARDANYAN; Merci, il y a une question d'un participant à distance qui est africain.

L'Afrique est en phase de développement graduel et il faut absolument augmenter les capacités en Afrique. En dehors du programme des boursiers qui comble les lacunes du développement des pays en développement, qu'est-ce qui est fait au niveau du DNSSEC pour améliorer les compétences et qu'est-ce qui existe en Afrique en matière de politique ?

JOHN CRAIN: Alors le renforcement des capacités, on a parlé du DNS, donc je vais parler des capacités relatives au DNS dans ce cas.

En général, on travaille avec la communauté. Donc mon groupe en particulier, nous faisons beaucoup de formations, de renforcement de capacités. Mais en ce qui concerne l'Afrique, c'est souvent des organismes tels qu'AfriNIC ou alors si vous allez à AFNOG à AfTLD, donc domaine de premier niveau pour l'Afrique, c'est ce type d'organisme qui vont fournir ces formations. Et nous travaillons avec eux, avec ces organismes.

Il y a également le NetWork, le centre de ressources du réseau qui a également fait beaucoup de choses en Afrique pour parler du DNS et du DNSSEC.

Alors en ce qui concerne les DNSSEC en particulier, il y a des formations qui sont faites en Afrique avec AFNOG et avec tout ce qui est AF, tous les organismes AF qui existent.

Je ne sais pas quand est la prochaine formation, mais il me semble qu'il y a quelques formations sur le DNSSEC pour l'Afrique en mai ou en juin.

Donc nous sommes très présents sur place. Mais nous nous appuyons sur l'expertise locale. Former le monde, c'est énorme. Ce n'est pas le travail de l'ICANN.

L'ICANN est une organisation relativement petite, les gens pensent que c'est trop gros, mais en fait c'est une organisation qui est petite.

Donc nous utilisons les compétences de la communauté technique, nous les aidons en leur fournissant des supports, en améliorant leurs supports et c'est beaucoup plus facile de cette manière.

Et pour beaucoup d'entre nous, nous avons des plateformes d'apprentissages en ligne, ce qui nous permet de fournir des formations en ligne.

Il y a également la possibilité de traduction dans différentes langues. Donc même si on n'est pas là pour former le monde entier, on passe quand même un certain temps à former.

Dans mon titre, il y a les mots sécurité, stabilité et résilience, dans l'écosystème, et une des choses qui me permet de faire avancer ces projets, c'est justement d'assurer que les gens sont au courant.

SIRANUSH VARDANYAN: Lendon, vous avez la parole.

LENDON TELESFORD: Lendon, de Grenade. Je ne sais pas si c'est une question sur le DNS en lui-même ou si ce n'est pas plutôt par rapport au fonctionnement général du système. Mais enfin, je vais la poser quand même.

Dans la présentation, il a été souligné qu'il existe différentes instances, il existe Anycast, différents serveurs, et donc ma question c'est par rapport au serveur client et au serveur Anycast. Quels sont les mécanismes qui existent pour se protéger contre les attaques des DDos en matière de proximité pour que les clients ne soient pas perdus, pour savoir où aller, quel serveur utiliser.

JOHN CRAIN: Je réfléchis là un instant.

MATT LARSON: Je ne vois pas ce que vous voulez dire par là. Les clients qui sont perdus et qui ne savent pas quel serveur utiliser. Je vais encore une fois répondre en utilisant le concept de la couche.

En fait, Anycast, c'est une couche en dessous du DNS, ça fait partie du système de routage. Donc en prenant un système de serveur de DNS, et je crois que toutes les adresses IP sont maintenant dans Anycast. Donc imaginons que nous avons un serveur récursif qui envoie une requête à la racine L, donc du

point de vue de la couche DNS, tout ce qu'il se passe c'est que j'envoie la requête à cette adresse IP.

Mais lorsqu'on arrive à la couche du routage, le réseau doit transporter le paquet. Les routeurs du réseau vont voir qu'il y a plusieurs instances, plusieurs endroits dans le réseau où cette adresse IP est disponible.

Alors, en matière de BGP, on dirait que différents réseaux annoncent.

Donc vous avez plusieurs réseaux sur internet qui disent : oui, je peux aller jusqu'à la racine, et les routeurs utilisent les différentes informations du BGP et ils se disent alors, de mon point de vue, quel est le meilleur moyen d'accéder à la racine L. Et tous les routeurs fonctionnent de cette manière.

Donc par rapport à là où on est dans le réseau finalement ce qu'il se passe c'est que les gens vont à l'instance la plus proche. Ce n'est pas une question de géographie, il y a différents facteurs qui ont un impact sur la politique de routage de BGP.

Alors je ne sais pas… Je ne pense pas qu'il y ait de confusion en fait.

Alors en cas d'attaque par contre, ou de surcharge, les opérateurs configurent des serveurs de nom selon la configuration Anycast. Lorsqu'un serveur est live, simplement,

on saura qu'il est possible de l'utiliser. Mais s'il y a congestion, surcharge, le réseau dira : je ne fonctionne pas, je ne suis pas en live, je ne peux pas accepter la requête. Et le réseau à ce moment-là envoie la requête autre part.

LENDON TELESFORD: Donc du point de vue du routeur la décision de savoir où aller est prise par rapport à des informations BGP pré-acquises.

MATT LARSON: En fait non, parce que ça évolue à chaque fois. Chaque système autonome, c'est un réseau du point de vue du BGP, chaque système autonome est un réseau qui a un ensemble de routes, d'adresses IP.

J'ai ces adresses IP, j'ai un certain nombre d'informations. Donc voilà les informations que je connais et les autres routeurs sont là et ils décident en temps réel, sur l'instant où aller.

C'est une version très simplifiée du système, mais le BGP, en fait c'est quelque chose qui se passe en temps réel.

JOHN CRAIN: Et ça, ce n'est pas quelque chose qui est causé par Anycast, ça existait avant Anycast, parce qu'il y a différents chemins.

Donc si par exemple quelqu'un fait la publicité d'un site web et que je suis très loin, moi je ne vois qu'un chemin, mais si je suis proche il y aura sans doute plusieurs chemins. Et ça, ça existait avant. Donc en fait c'est une petite astuce routage qui a été reconnue et qui a permis d'ajouter davantage de serveurs.

Il n'y a pas eu de changements technologiques pour Anycast, par Anycast, c'est simplement une astuce de routage.

LENDON TELESFORD: J'aimerais savoir si on peut justement en fait piéger le routage.

JOHN CRAIN: Je ne pense pas. Le routage a ses propres problèmes de routage, mais ce ne sont pas des problèmes liés à Anycast. Il y a des problèmes de sécurité, ou de manque de sécurité, certes, dans le cadre du routage. Mais ce ne sont pas des problèmes qui sont spécifiques à Anyscast.

SIRANSUH VARDANYAN: Oui, merci. Allez-y.

SHABNIL ANAL SAMI: Shabnil de Fidji. Si un pays souhaite héberger un serveur racine, quelles sont les meilleures pratiques pour décider de savoir

lequel héberger ? Est-ce que c'est basé sur les régions, est-ce que n'importe qui peut héberger un serveur ?

JOHN CRAIN: Ça dépend à qui vous parlez. La première chose que je dirais c'est que ce n'est pas un pays, c'est un réseau ou un opérateur de réseau qui héberge une instance. Et donc il peut se rendre sur la liste des opérateurs.

Nous, nous sommes opérateurs par exemple, nous faisons partie de la liste, je crois qu'il y en a à Fidji, il y a d'autres personnes qui s'en occupent. Donc vous pouvez simplement vous adresser à ces opérateurs et leur demander quelles sont les conditions. Et les opérateurs sont chacun un petit peu différents.

Mais ce n'est pas compliqué. Il y a 990 instances, 990 lieux actuellement. Donc en ajouter d'autres, ce n'est pas problématique, c'est simplement s'adresser au contact, vous allez sur le site et vous aurez une liste des opérateurs avec les documents pour les contacter. On peut d'ailleurs en parler si vous souhaitez, à la fin de la réunion.

SHABNIL ANAL SAMI: Ce que je voulais savoir c'est lequel héberger ? L ou autre. Parce que j'ai vu qu'à Puerto Rico, le L est hébergé. Donc ce qui n'est pas clair pour moi, c'est la question de la région.

JOHN CRAIN: En fait ce n'est pas régional, c'est souvent une question de relation. Donc la raison pour laquelle Fidji a le L comme Puerto Rico, c'est en fait simplement que nous avons quelqu'un qui travaille à Fidji qui fait partie du personnel.

Donc très souvent ça dépend des relations qu'on a avec les gens. Et puis il y a également d'autres critères, les critères financiers, qui diffèrent d'un système à l'autre. À l'ICANN nous avons une solution selon laquelle on paye pour le serveur, on le met en ligne, et c'est nous qui faisons le reste du travail. Plutôt qu'ils vous envoient le serveur. Donc le modèle est différent.

Donc c'est à vous de voir ce qui vous convient. Tous les serveurs racines du point de vue du DNS sont les mêmes. Ils vous donnent les mêmes réponses, ils fonctionnent tous du point de vue de la requête de la même manière, donc après ce sont des questions commerciales, des questions de relations et la question de savoir qui vous connaissez.

SIRANUSH VARDANYAN: D'autres questions ? Pardon, allez-y.

NON IDENTIFIE: Alors, comment s'assurer de la publication des données, comment faire pour ne pas publier des données qui ne sont pas justes ?

Alors ensuite les copies de la racine, dans les pays hôtes, est-ce que ça fait partie de différentes zones dans le monde ou est-ce que ça fait partie des zones… Par exemple la racine L, est-ce que ça fait partie des autres zones ou est-ce que tous les enregistrements y sont ?

MATT LARSON: Tous les serveurs racines ont les mêmes informations, il n'y a qu'une zone racine avec ces informations et tous les serveurs ont les mêmes informations.

Alors est-ce que vous pouvez répéter votre première question ?

SIRANUSH VARDANYAN: Il y a traduction, vous pouvez le faire dans votre langue si vous le souhaitez, donc n'hésitez pas.

NON IDENTIFIE: Alors, lorsque les registres de chaque pays font un registre de zone, disons un ccTLD ou quelque chose comme ça et ensuite ils le publient dans toute la zone, comment est-ce qu'on s'assure que ces publications sont justes et qu'il n'y ait pas d'erreur dans

ces publications ou dans la distribution ? Parce que j'ai compris que cela s'est passé déjà auparavant.

JOHN CRAIN: Il y a donc un mélange de technologie et de mots, de terminologie. Quand il s'agit des ccTLD ou des gTLD, vous savez quand ils publient la zone, cette zone est faite de données qui viennent de bases de données et ils sont ainsi responsables de s'assurer de l'exactitude de ces données.

Lorsque c'est publié, si votre DNSSEC signe la zone, et que vous authentifiez ces requêtes de DNS, vous vous assurez ainsi de ce qui est publié.

Voilà donc le point final, c'est le côté de publication du DNS. De l'autre côté, il faut considérer la sécurité des bases de données, l'intégrité de vos données, de la sécurité. Il y a eu des problèmes dans le passé, il y a eu du piratage au niveau des ccTLD, je pense que c'est de ça dont vous parlez.

Il n'y a rien, il n'y a pas de réseau vraiment sécurisé. Il y a une susceptibilité à ce problème. Ce que nous faisons à l'ICANN et avec nos amis dans ces registres, surtout mon groupe, mon groupe de sécurité, lorsque nous avons eu des problèmes, ils viennent nous voir et nous les aidons et nous essayons de

trouver des experts qui puissent les aider à refaire à reconcevoir leur système.

Je pense que je sais de qui vous parlez, mais je ne vais pas en donner le nom. Nous avons eu des cas où il y a eu des attaques d'injection qui sont spécifiques au système, et cela a permis aux personnes malveillantes de changer les dossiers ou les données pour une organisation assez importante et pointer cet internet, la diriger ailleurs. Je pense que c'est de cela dont il parle.

Donc de l'extérieur, on a l'impression que ce serveur web a été piraté, mais en fait c'est le système de registre. Donc nous avons passé beaucoup de travail avec les opérateurs de registre, et ils ont maintenant un système en place qui est complètement neuf et qui leur permet d'auditer tous ces problèmes. Ils ont appris de leurs erreurs et ils sont allés de l'avant. Donc ils savent maintenant ce qu'il faut faire quand vous êtes compromis, vous devez savoir comment régler votre système, et vous apprenez à faire de nouveaux processus.

Ça ne veut pas dire que d'autres ccTLD ou d'autres gTLD ne seront pas piratés dans l'avenir, ce n'est pas la réalité, parce que nous voyons des corporations très importantes des corporations de millions de dollars qui sont attaquées.

NON IDENTIFIE: Merci beaucoup.

SIRANUSH VARADANYAN; Oui, quelqu'un d'autre veut prendre la parole ?

JASON HYNDS: Je suis Jason Hynds, je viens de la Barbade. John, j'ai une question pour vous. Y a-t-il des publications que vous avez publiées pour aider les opérateurs de registre pour qu'ils puissent prévenir ces problèmes, avant qu'ils aient lieu ?

JOHN CRAIN: Oui, j'ai parlé du travail que nous avons fait avec ces partenaires, nous avons fait du renforcement de capacité et des heures de formation avec les opérateurs pour qu'ils sachent comment sécuriser leur réseau, comment ils peuvent surveiller leur réseau.

Donc bien sûr, la communauté que vous voyez ici, tous ces opérateurs donc, ont leur propre groupe ou rassemblement et partagent les meilleures pratiques. Et ils ont de l'aide au niveau de l'ingénierie aussi

Donc par exemple, en Jamaïque, la région LAC, il y a une organisation qui s'appelle LACTLD qui inclue tous les opérateurs de registres, du moins la plupart d'entre eux, ceux de la région.

Ils ont des réunions souvent et ils ont des séances plus techniques et il faut donc les aider.

Et ce n'est pas un problème auquel ils font face seuls. Ils ont de l'aide, il y a de la formation, il y a de l'entraide. Donc il se passe beaucoup de choses dans ce sens-là.

SIRANUSH VARDANYAN: Y a-t-il des questions ? Il n'y a plus de question.

Je voudrais donc vous encourager à participer mercredi durant l'atelier de travail du DNSSEC qui aura lieu entre 9 h et midi, pardon de 9 h à 15h. Nous aurons une pause déjeuner au milieu parce que nous avons une séance boursier.

Venez nous rejoindre dans cet atelier travail car il est très important.

Quelques derniers mots de la part de nos présentateurs ?

RACHEL REYES: Oui, merci d'être restés avec nous et j'apprécie vraiment votre participation et je remercie Matt et John pour m'avoir aidé à répondre aux questions.

SIRANUSH VARDANYAN: Je voudrais remercier les interprètes et notre équipe technique, John, Matt et Rachel nous apprécions vraiment votre participation. Je sais que vous êtes très occupés durant cette réunion, je vous remercie d'être venus et d'avoir fait votre présentation devant les boursiers.

On applaudit nos présentateurs.

Avec ça, notre réunion est donc terminée. Merci.

[FIN DE LA TRANSCRIPTION]