The Internet Corporation for Assigned Names and Numbers

Résumé de l'impact de l'extensibilité de la zone racine

Date de publication : octobre 2010

Synthèse

En février 2009, le Conseil d'administration de l'ICANN a demandé qu'une étude soit entreprise pour examiner l'impact de l'introduction d'un nombre de nouvelles technologies et de l'ajout éventuel d'un grand nombre de nouveaux domaines de premier niveau à la racine du DNS. Alors que certaines de ces technologies avaient, jusqu'alors, déjà connu un certain déploiement, des préoccupations étaient exprimées par la communauté quant à la mesure dans laquelle la stabilité du DNS pourrait être menacée si les changements et les ajouts avaient lieu sans précaution. Suite à la demande du Conseil d'administration, deux études ont été réalisées, l'une se concentrant sur l'impact des nouvelles technologies et les ajouts de TLD sur un serveur racine, l'autre examinant, dans une perspective plus vaste, tous les processus liés à la gestion du système racine.

Les nouvelles technologies en question comprenaient l'IPv6 (autant en termes d'adresses IPv6 liées à des noms de domaine de premier niveau et des serveurs racine qu'en termes de soutien des demandes d'IPv6 adressées aux serveurs racine), les noms de domaine internationalisés (IDN) et les améliorations de sécurité pour le DNS (DNSSEC). Cependant, depuis (et dans certains cas, avant même) la résolution du Conseil d'administration de l'ICANN, toutes ces technologies avaient été déployées ou mises en œuvre à la racine ; ainsi, il existe des preuves empiriques qui peuvent être utilisées dans l'effort de compréhension de l'impact de ces technologies.

A ce jour, le déploiement de l'IPv6, des DNSSEC et des IDN dans le système racine n'a pas eu d'impact nuisible sensible. Alors que le déploiement de ces nouvelles technologies peut avoir causé une certaine dégradation de service minime due au manque d'infrastructure IPv6 robuste et/ou à la taille plus importante de la réponse (à cause de l'ajout des enregistrements IPv6 ou de la signature des DNSSEC de la racine) provoquant un largage de réponse résultant en des temporisations et des retransmissions, nul impact n'était assez important pour provoquer l'inquiétude des communautés concernées.

En contemplant l'avenir, et en supposant que les estimations se rapportant à une limite de moins de 1 000 nouveaux gTLD ajoutés par an à la zone racine soient exactes et que les autres paramètres liés à la gestion de la racine DNS ne soient pas considérablement changés, il apparaît que des affectations de ressources et des cycles de mise à niveau opérationnelle normaux suffiront à garantir que l'évolutivité de la racine, autant en termes de nouvelles technologies qu'en

termes de nouveau contenu, n'ait pas d'impact important sur la stabilité du système racine.

Toutefois, sachant que la gestion de la racine du DNS implique de multiples parties et dans l'intérêt des niveaux de précaution les plus élevés concernant la stabilité de la racine du DNS, la surveillance du système de gestion de la racine devrait être améliorée, notamment dans les domaines les plus sensibles à des changements de taux de croissance ou qui nécessitent un délai important pour changer. De plus, une communication plus claire et plus fréquente entre les partenaires de gestion de la racine pertinents et les autres parties prenantes - y compris les communications officielles entre le personnel de l'ICANN et les opérateurs de serveurs racine concernant les nombres de candidatures approuvées prévus, les technologies supplémentaires devant être déployées et dans quels délais, etc. - est susceptible d'améliorer la conviction que les changements du système racine n'auront pas un effet négatif sur la stabilité de ce système.

Introduction

Entre 2004 et 2010, la racine du DNS a fait l'objet de changements importants, aussi bien en termes de contenu qu'en termes d'infrastructure de soutien. De l'ajout des noms de domaine internationalisés (IDN) dans la racine au déploiement de l'IPv6 et des DNSSEC, on peut dire à coup sûr que plus de changements ont eu lieu ces dernières 5 ou 6 années que depuis le déploiement initial du DNS. Tenant compte de l'acceptation imminente de candidatures pour de nouveaux domaines génériques de premier niveau (gTLD), on peut s'attendre à encore plus de changements importants dans la racine du DNS.

Fidèle à la mission de l'ICANN consistant à « assurer le fonctionnement stable et sûr des systèmes d'identificateurs uniques de l'Internet »1 le Conseil d'administration de l'ICANN a demandé qu'une étude soit conjointement réalisée par le comité consultatif sur le système de serveurs racine (RSSAC) de l'ICANN et le comité consultatif pour la sécurité et la stabilité (SSAC) de l'ICANN avec le soutien du personnel principal de l'ICANN afin d'examiner l'impact des modifications proposées sur le système racine du DNS. Cependant, aussi bien avant que pendant la mise en œuvre de cette étude, bon nombre des changements dans le système racine intéressant le Conseil d'administration étaient déjà mis en œuvre sans conséquences négatives notables.

[1]Extrait de « l'article 1, section 1. Mission » des règlements de l'ICANN, voir http://www.icann.org/en/general/bylaws.htm

Cet article fournit une récapitulation des changements survenus dans la racine DNS et présente une analyse de ces changements ainsi que des estimations relatives à l'impact prévu des changements futurs, y compris l'ajout de nouveaux noms de domaine de premier niveau.

Contexte

Le 3 février 2009, le Conseil d'administration de l'ICANN a approuvé la résolution 2009-02-03-04 à l'unanimité[2] pour qu'une étude conjointe soit réalisée par le RSSAC et le SSAC afin d'analyser «*l'impact des mises en œuvre proposées [IPv6, TLD IDN, DNSSEC et nouveaux gTLD] sur la sécurité et la stabilité au sein du système de serveurs racine du DNS ».* La résolution précisait que l'étude conjointe devrait :

- « *aborder les implications de la mise en œuvre initiale de ces changements survenant dans une période de temps réduite ».*
- « *aborder la capacité et l'extensibilité du système de serveurs racine face à un éventail stressant de défis techniques et de demandes opérationnelles susceptibles d'émerger dans le cadre de la mise en œuvre des changements proposés ».*
- « *élaborer un cahier des charges pour l'étude et nommer un comité de pilotage qui guiderait les efforts jusqu'au 28 février 2009 ».*
- « *faire directement participer le personnel technique principal de l'ICANN, impliqué dans les mises en œuvre programmées de ces activités et fournir le soutien nécessaire pour mettre en œuvre des aspects de cette étude selon les conditions et avec l'approbation ultime des comités consultatifs ».*
- veiller à ce que *« le processus d'établissement du cahier des charges, de la conception et de la mise en œuvre de l'étude abordent les préoccupations techniques et opérationnelles concernant l'expansion de la zone racine du DNS qui ont été exprimé à ce sujet ».*
- fournir au Conseil d'administration de l'ICANN *« les conclusions et recommandations de l'étude jusqu'au 15 mai 2009 ».*

A la suite de cette résolution, deux efforts furent entrepris, une étude concentrée sur l'impact de l'extensibilité de la racine sur un serveur racine (le serveur racine « L » exploité par l'ICANN) et une étude plus générale visant à modéliser les processus dans le système de gestion de la racine et à analyser les résultats de l'extensibilité du système. Une équipe d'étude ad hoc fut établie et nommée « Equipe sur l'extensibilité des serveurs racine » (RSST). Elle était composée de membres du RSSAC, du SSAC et d'experts indépendants pour réaliser cette seconde étude.

[2] Voir http://www.icann.org/en/minutes/prelim-report-03feb09.htm

L'étude de la racine « L »

L'étude de la racine « L » réalisée par le centre d'opérations, d'analyse et de recherche du DNS (DNS-OARC) dans le cadre d'un contrat avec l'ICANN, s'est spécifiquement concentrée sur l'impact des différentes combinaisons d'ajout d'IPv6, de DNSSEC et de nouveaux TLD dans une simulation en laboratoire du serveur racine « L ». Le rapport final de cette étude, intitulé « augmentation de la zone racine et analyse d'impact » a été publié le 17 septembre 2009 et est consultable à l'adresse http://www.icann.org/en/topics/ssr/root-zone-augementation-analysis-17sep09-en.pdf.

L'étude de la RSST

L'étude de la RSST, qui utilisa l'étude de la racine « L » dans le cadre de ses données d'entrée, externalisa l'élaboration d'une simulation de processus de gestion de la racine, et mena des entretiens avec des opérateurs de serveurs racine, le personnel de l'IANA, VeriSign, la NTIA et d'autres, était beaucoup plus générale, visant à examiner non seulement l'impact sur les serveurs racine mais également les systèmes d'allocation automatique de ressources qui conduisaient en une propagation de la zone racine aux serveurs racine. Le rapport final de cette étude, ayant pour titre « Élargir la racine » et pour sous-titre « Rapport sur l'impact de l'augmentation de la taille et de la volatilité de la zone racine sur le système racine DNS » a été publié le 31 août 2009 et est consultable à l'adresse http://www.icann.org/en/committees/dns-root/root-scaling-study-report-31aug09-en.pdf.

Évènements relatifs à l'extensibilité de la racine

Avant et depuis que le Conseil d'administration de l'ICANN a enjoint au SSAC, au RSSAC et au personnel principal de l'ICANN d'entreprendre l'étude des implications de l'extensibilité de la racine, nombre des sujets de cette étude avaient déjà été mis en œuvre. Les délais liés à l'introduction de nouvelles technologies dans la racine apparaissent dans la *Table 1*.

Date	Technologie	Évènement
Juillet 2004	IPv6	Premières adresses IPv6 ajoutées à la zone racine pour les domaines de premier niveau (KR et JP).
novembre 2005	DNSSEC	Signature du premier domaine de premier niveau (.SE).
Juin 2007	DNSSEC	Mise à disponibilité du premier champ d'essai de signature de DNSSEC de la racine par l'IANA.
Août 2007	IDN	Noms de domaine de premier niveau IDN expérimentaux ajoutés à la racine.
Février 2008	IPv6, gTLD	Premières adresses IPv6 ajoutées pour les serveurs racine (A, F, J, K, L et M). Une limite d'un maximum de moins de 1 000 nouveaux gTLD par an est dérivée des estimations de temps de traitement des gTLD.
Janvier 2010	DNSSEC	Publication de la zone racine volontairement non validable (DURZ) sur le premier serveur racine (« L »).
Mai 2010	IDN, DNSSEC	Premiers IDN de production, ajoutés à la racine (pour l'Égypte, l'Arabie saoudite et les Émirats arabes unis). Déploiement de la DURZ sur l'ensemble des 13 serveurs racine.
Juin 2010	DNSSEC	Les premiers enregistrements DS sont publiés dans la zone racine (pour .UK et .BR).
Juillet 2010	DNSSEC	La racine est signée DNSSEC et l'ancre de confiance de la racine est publiée.

Table 1 - Évènements relatifs à l'extensibilité de la racine

Impacts

Au cours de la période s'étendant de juillet 2004, quand les premières adresses IPv6 ont été ajoutées à la racine pour des serveurs de noms TLD, jusqu'à juillet 2010, avec la signature DNSSEC de la racine et l'insertion des enregistrements DS dans la racine, il n'y avait toujours pas de signalement ou d'observation publique de dégradation de service liée à ces évènements et concernant le service racine DNS. Cette section examine l'impact de chacun des divers changements portant sur la racine du DNS.

IPv6

L'inclusion d'IPv6 dans la racine du DNS a deux composantes : l'ajout de 'glue records' (duplication d'informations) IPv6[3] dans la zone racine pour les serveurs de noms de TLD faisant autorité et l'ajout d'enregistrements 'glue' IPv6 aux serveurs racine. Chacun de ces impacts sera examiné à tour de rôle.

Domaines de premier niveau

En juillet 2004, les domaines .JP et .KR ont été les premiers TLD à ajouter des enregistrements 'glue' IPv6. A compter de septembre 2010, il existe 283 enregistrements 'glue' IPv6 dans la zone racine, couvrant 203 TLD. Un impact de l'utilisation élevée d'enregistrements 'glue' IPv6 a été l'augmentation du nombre de résolutions qui utilisent le transport IPv6. A compter de septembre 2010, au moins un serveur racine (le serveur racine « L ») voit environ 1,3% des requêtes sur IPv6 du DNS[4]. Compte tenu de l'infrastructure de réseau moins robuste de l'IPv6 dans l'Internet aujourd'hui, des requêtes et/ou réponses IPv6 sont susceptibles d'être plus fréquemment perdues qu'avec IPv4. Ceci résulte en plus de délais d'attente et de retransmissions que s'il n'y avait pas de soutien IPv6 dans les TLD. Cependant, cet impact a des conséquences négatives minimes et des améliorations sont à attendre à mesure que le déploiement d'IPv6 progresse.

Serveurs racine

Lorsque certains des opérateurs de serveurs racine ont ajouté des adresses IPv6 pour leurs enregistrements de noms de serveurs racine, la taille de la requête initiale des résolveurs (priming) a sensiblement augmenté. Tel que discuté dans le rapport SAC018 produit conjointement par le RSSAC et le SSAC et intitulé « Adaptation des enregistrements de ressources d'adresses Ipv6 à la racine du système de noms de domaine » [5], il y avait des soucis dus au fait qu'il était prévu que la requête initiale croitrait au-delà de la réponse DNS « classique » maximale non tronquée de 512 multiplets. Si le résolveur requérant la réponse initiale ne fournissait pas une taille de mémoire tampon de réponse plus grande via l'extension EDNS0[6] , on craignait que les serveurs racine puissent indiquer une réponse tronquée qui conduirait le résolveur requérant à retransmettre la requête sur TCP. Puisque les requêtes du DNS basées sur TCP sont sensiblement plus intensives en ressources que les requêtes basées sur UDP

---

[3] Les 'glue records' sont des enregistrements de ressources IPv4 (« A ») et IPv6 (« AAAA ») associés aux serveurs de noms qui sont dans la zone en question. Voir la RFC 1034 (http://www.ietf.org/rfc/rfc1034.txt) pour la définition des 'glue records'.

[4] Communication privée avec les opérateurs du serveur racine « L ». D'autres serveurs racine devraient voir un pourcentage similaire de requêtes.

[5] Voir http://www.icann.org/en/committees/security/sac018.pdf

[6] L'EDNS0 est défini dans la RFC 2671 (voir http://www.ietf.org/rfc/rfc2671.txt).

normales, il y avait une certaine inquiétude quant au fait que les serveurs racine pourraient être surchargés, ce qui résulterait en une dégradation de service à l'égard de tous les utilisateurs qui adressaient des requêtes aux serveurs racine. De plus, il y avait une certaine inquiétude quant au fait que la réponse plus grande de la part des serveurs racine soit susceptible d'être bloquée ou filtrée par les barrières de sécurité, les NAT (les traductions d'adresses de réseaux) et autres dispositifs 'intermédiaires' qui 'savaient' (incorrectement) qu'une réponse DNS ne pouvait jamais dépasser les 512 multiplets. Dans de tels cas, il y a un risque que les requérants ne reçoivent jamais de réponse et soient ainsi incapables d'obtenir des adresses des serveurs racine.

Suite à un examen approfondi et à une mise à l'essai de cette question, les adresses IPv6 ont été ajoutées à la zone racine en février 2008. En pratique, les mises en œuvre de serveurs DNS opérant sur la racine écartaient les informations non essentielles (« section supplémentaire ») pour éviter de tronquer des réponses à des requêtes qui ne spécifiaient pas un tampon suffisamment grand via l'EDNS0 (ou n'avaient pas utilisé l'EDNS0). Ceci a pu résulter en une augmentation légère du nombre de requêtes adressées aux serveurs racine puisque les résolveurs étaient tenus d'émettre des requêtes supplémentaires pour des données précédemment fournies dans la section supplémentaire. Toutefois, si c'est le cas, l'augmentation n'était pas notable.

Pour les requérants qui fournissaient une taille de tampon plus grande via l'extension EDNS0, il a pu y avoir une augmentation du nombre de paquets de données fragmentés qui auraient pu résulter en un non envoi de réponses soit dû à la perte d'un fragment soit parce que les dispositifs intermédiaires étaient configurés de sorte à ignorer les fragments. De plus, certaines politiques de sécurité ont suggéré (à tort) que les requêtes DNS basées sur le protocole TCP devaient être bloquées Dans ces cas, une requête initiale sans l'option d'extension EDNS0 (ou dans laquelle le tampon offert est plus petit que la taille de la réponse) pourrait résulter en une réponse bloquée. Cependant, au cours de la période de plus de deux ans et demi depuis que les premiers enregistrements 'glue' IPv6 pour les serveurs racine ont été installés dans la racine, il n'y a pas eu de signalements importants (le cas échéant) de conséquences négatives.

En examinant le côté traitement du système de gestion de la racine, les processus et le système de gestion de la racine de l'ICANN ainsi que les processus et systèmes de VeriSign ont nécessité une certaine modification afin de traiter les enregistrements de ressource « AAAA » IPv6 et vérifier l'accessibilité d'IPv6 dans le cadre de « contrôles techniques » effectués par les deux parties. Les impacts autant sur l'ICANN que sur VeriSign étaient toutefois minimes et ces processus et systèmes continuent à fonctionner aujourd'hui sans incident.

Les noms de domaine internationalisés (IDN)

Du point de vue du DNS, mis à part une longueur moyenne de label légèrement plus longue, les noms de domaine internationalisés sont pratiquement impossibles à distinguer des autres noms de domaine. L'ajout d'IDN à la racine ne représentait ainsi,

pour le DNS, aucune différence avec l'ajout à la racine de tout autre TLD non IDN. En tant que tel, nul impact ne fut observé au niveau du DNS.

Il y eut, toutefois, un certain impact sur les processus et systèmes de gestion de la racine de l'ICANN. Afin d'afficher les informations IDN de manière utile, le personnel de l'IANA a dû réviser les processus de requête de labels U en plus des labels A et a dû modifier des systèmes de l'IANA tels que le serveur Whois pour soutenir l'affichage de labels A et de labels U. D'une manière plus générale, le soutien des IDN dans les systèmes dorsaux de traitement, notamment en matière d'affichage des données des titulaires de noms de domaine, continue à être un sujet de discussion permanente au sein des forums de l'ICANN (et d'autres forums liés à la sécurité, par ex.). On peut s'attendre à ce que l'affichage correct des informations IDN représente à l'avenir un impact non insignifiant pour les bureaux d'enregistrement (au moins).

DNSSEC

L'ajout de DNSSEC à la racine a eu un impact considérable, autant en termes de taille de la zone racine, de taille des réponses aux requêtes de la racine, qu'en termes d'implications du déploiement des DNSSEC pour l'ICANN, VeriSign, et la NTIA, les parties impliquées dans la gestion de zones racine. En termes de taille de zone racine, à compter du 6 septembre 2010, la zone racine signée (tel que transmis sur fil dans un transfert de zone complet) était de 222 246 multiplets. Lorsque tous les enregistrements liés à des DNSSEC, à savoir les enregistrements de ressources DNSKEY, NSEC, DS et RRSIG, étaient ôtés de cette zone, la taille de zone restante était de 122 657 multiplets. Cependant, en se basant sur les données de l'étude de la racine « L », on s'attendait à ce que la charge supplémentaire de données imposée par les DNSSEC sur tout serveur de nom raisonnablement configuré, serait sans importance. En pratique : il n'y a pas eu de signalements de difficultés rencontrées par n'importe lequel des opérateurs de serveurs racine chargeant et desservant la zone signée DNSSEC au cours du déploiement de la « zone racine volontairement non validable (DURZ) », correspondant au déploiement étagé des DNSSEC dans la racine avant la publication de l'ancre de confiance de la racine.

Potentiellement plus importante, la taille de la majorité des réponses des serveurs racine augmenta sensiblement, à savoir, une requête adressée aux serveurs de noms racine passait de 492 multiplets à 829 multiplets lorsqu'une réponse signée DNSSEC était requise. Contrairement à la taille des données de zone, un doublement de la taille d'une réponse du DNS était préoccupant compte tenu de la limite de 512 multiplets discutée précédemment dans le contexte de l'IPv6. Les spécifications des DNSSEC ont traité cette limite en requérant l'utilisation de l'EDNS0 pour signaler que le résolveur était équipé pour gérer des réponses qui comportaient des enregistrements de ressources liés à des DNSSEC. Cependant, il apparaît que la majorité des résolveurs sur Internet, du moins ceux adressant des requêtes aux serveurs racine, utilisent l'EDNS0 par défaut et mettent un bit dans les requêtes DNS (le bit « DNSSEC OK ») pour indiquer

que le résolveur comprend des réponses qui comportent des enregistrements de ressources liés à des DNSSEC (indépendamment du fait que le résolveur utilise ou non ces enregistrements de ressources). Suite à ce qui précède, entre 50% et 80% des requêtes atteignant le serveur racine avant la signature de la racine, comportaient l'indication « DNSSEC OK » et ainsi, lorsque la racine signée était servie par tous les serveurs racine, ces serveurs ont immédiatement commencé à renvoyer un total d'au moins 50 000 enregistrements de ressources liés aux DNSSEC par seconde[7].

Avant la signature de la racine, il existait de sérieuses inquiétudes concernant l'impact du renvoi des réponses signées DNSSEC plus grandes à des clients qui pouvaient ne pas s'y attendre. En particulier, on s'inquiétait que les dispositifs intermédiaires ignoreraient, comme dans le cas de l'IPv6 mentionné précédemment, les réponses dépassant les 512 multiplets. Prenant ceci en compte, l'ICANN, VeriSign et la NTIA se mirent d'accord sur un déploiement étagé de la zone racine signée (la « DURZ ») qui comportait aussi un appareillage appréciable de serveurs racine pour observer tout changement dans les schémas de requêtes. Pourtant, après le déploiement de la zone racine signée sur l'ensemble des 13 serveurs racine en une période de 6 mois, nul signalement de conséquences négatives n'a été reçu par l'une quelconque des parties impliquées dans la signature de la racine.

En termes de changements de processus, le déploiement des DNSSEC à la racine résultant en la création de nouveaux processus avec de nouvelles installations physiques nécessaires pour gérer de manière sûre la clé de signature de clé de la racine par l'ICANN et la clé de signature de zone racine par VeriSign. De nouveaux processus furent également mis en place pour permettre aux gestionnaires de TLD d'offrir en toute sécurité des informations DS (« signataire de délégation ») à l'ICANN (et pour permettre à l'ICANN de soumettre à VeriSign des informations DS à inclure dans la zone racine) et faciliter la création d'une « chaîne de confiance » de la racine aux zones enfants signées. A ce jour, ces nouveaux processus ont fonctionné sans incident.

Résumé

Pour résumer les impacts à ce jour de l'ajout de l'IPv6 au système racine, des noms de domaines de premier niveau IDN et du déploiement des DNSSEC, nuls effets nuisibles importants n'ont été observés par l'ICANN ou signalés à l'ICANN.

Toutefois, ceci étant dit, un point soulevé dans le cadre des discussions relatives à l'extensibilité de la racine est le besoin de communications améliorées entre les parties prenantes impliquées dans la gestion du système racine. Dans certains cas, l'introduction de nouvelles technologies pourrait probablement avoir été améliorée par des exigences plus formelles concernant la communication entre toutes les parties susceptibles d'être touchées, par la discussion de ces exigences et impacts, par des

[7] En supposant que l'estimation approximative d'une moyenne de 8 000 requêtes par seconde par grappe de serveurs racine sur 13 grappes de serveurs racine avec l'indication « DNSSEC OK » dans la moitié des requêtes.

plans documentés comportant des délais, etc. A cet égard, les communications, la documentation et les discussions entourant le déploiement de la racine signée ont été suggérées comme un exemple de mouvement dans la bonne direction.

Prévisions

Le système racine continue à faire l'objet de changements, quoique ces changements portent maintenant plus sur des déploiements poursuivis de technologies existantes que sur des changements structurels tels que l'introduction de nouvelles technologies. Cette section examine certaines prévisions de changements probables, adoptant l'hypothèse que des paramètres tels que les temps de rafraîchissement de zone, les valeurs TTL (durée de vie) des enregistrements DNS, les taux de changements de zone racine, et la longueur et complexité des processus administratifs ne varient pas extrêmement ou de manière inattendue par rapport aux valeurs historiques.

IPv6

Il est très probable qu'à l'avenir, des domaines de premier niveau supplémentaires ajoutent des enregistrements d'adresses IPv6 pour leurs serveurs de noms. A compter du 6 septembre 2010, la zone racine contient 283 enregistrements 'glue' IPv6 correspondant à 203 des 294 domaines de premier niveau ayant au moins un enregistrement d'adresse IPv6 pour leurs serveurs de noms. A mesure que l'IPv6 se développe pleinement, on peut raisonnablement penser que plus de TLD ajouteront un soutien IPv6, pour couvrir finalement tous les TLD, et que le nombre moyen de serveurs de noms avec soutien IPv6 pour ces TLD augmentera. Jusqu'à ce que l'infrastructure IPv6 se soit améliorée pour égaler la structure IPv4, les utilisateurs finaux pourraient faire l'expérience de quelques conséquences négatives sous forme de retards résultant de la temporisation de requêtes envoyées aux serveurs de noms IPv6.

Dans le cas de la racine, le rapport SAC018 décrit que la taille de la réponse à la requête initiale lorsque tous les serveurs racine auront déployé l'IPv6 devrait être de 811 multiplets. Alors que les opérateurs de serveurs racine qui n'ont pas encore déployé l'IPv6 n'ont pas avancé de dates auxquelles ils prévoient une activation de l'IPv6 sur leurs serveurs racine, ils ont tous indiqué qu'ils avaient l'intention de le faire[8]. Cependant, puisque des réponses dépassant les 512 multiplets ont déjà été rencontrées, il est peu probable que les 100+ multiplets supplémentaires dans une réponse à une requête initiale aient un impact notable.

DNSSEC

A compter du 15 juillet 2010, la zone racine a été signée et est en cours de distribution à toutes les instances de l'ensemble des 13 serveurs racine. De ce fait, un impact supplémentaire sur la zone racine compte tenu des DNSSEC sera probablement limité à l'ajout, la modification et la suppression des enregistrements de ressources DS

[8] Communications privées avec le co-président du RSSAC et l'opérateur du serveur racine « L ».

(signataire de délégation), à un potentiel de changements des algorithmes de clé, des longueurs de clés ou du nombre de clés et des évènements de frappe coulée.

Comme les enregistrements de ressources DS peuvent varier du point de vue taille selon l'algorithme de hachage utilisé, l'augmentation exacte de taille que l'ajout d'enregistrements DS présentera à l'avenir est difficile à prévoir avec précision. Cependant, la structure des enregistrements de ressources DS étant donnée, on pourrait dire qu'une estimation pessimiste de la taille d'enregistrements DS serait de 64 multiplets. A compter du 6 septembre 2010, il y a 49 enregistrements DS pour 29 TLD (y compris les 11 TLD IDN d'essai encore dans la racine). En supposant, comme le fait l'étude de la racine « L », que le déploiement complet d'enregistrements DS par les TLD résultera en un total de 1440 enregistrements de ressources DS pour 1 000 zones, le nombre total de multiplets que les enregistrements DS ajouteraient serait moins de 100 kilo-octets. Le nombre réel sera probablement nettement inférieur vu qu'il est lié au nombre de TLD et, comme discuté dans la section suivante, on s'attend à ce que ce nombre soit nettement inférieur aux 1 000 nouveaux TLD présumés dans l'étude de la racine « L ».

Concernant les changements relatifs aux algorithmes de clés, aux longueurs de clés et au nombre de clés, il est possible que le changement le plus important soit de passer à la cryptographie à courbe elliptique, ce qui résulterait en des clés sensiblement plus petites de même puissance cryptographique.

Enfin, bien qu'il s'agisse plus d'une question opérationnelle que d'une question d'extensibilité de la racine, les évènements de frappe coulée surviennent assez régulièrement avec toutes les zones signées DNSSEC. Normalement, les défilements de clés de signature de clé nécessiteront que des enregistrements DS actualisés soient fournis à l'administrateur de la zone parent. Dans le cas de la zone racine, faire défiler la clé de signature de clé racine nécessitera une actualisation de l'ancre de confiance de la racine dans tous les résolveurs configurés pour la validation. On espère que les mécanismes basés sur la RFC 5011 permettront qu'un grand nombre de frappes de coulée de clé de signature de clé racine soit automatisé, mais on peut s'attendre à une certaine perturbation lorsque la clé de signature de clé racine est changée et ainsi, faire défiler la clé de signature de clé racine devrait avoir lieu avec une certaine précaution.

Domaines de premier niveau

Dans l'analyse faite dans le document préliminaire « Scénarios de taux de délégation pour les nouveaux gTLD »[9], le personnel de l'ICANN estime que le taux prévu de nouveaux TLD introduits dans la racine sera de l'ordre de 200 à 300, même avec des taux de candidatures plus élevés que prévu. Le même document déduit qu'indépendamment du nombre de candidatures, il y aura une limite imposée par le

[9] Voir http://www.icann.org/en/topics/new-gtlds/anticipated-delegation-rate-model-25feb10-en.pdf

processus concernant un ajout de nouveaux TLD inférieur à un maximum de 1 000 nouveaux gTLD par an[10]. Pour les besoins de cette analyse, on supposera un nombre fixe de 1 000 nouveaux TLD supplémentaires par an.

Sur la base du travail fait dans l'étude de la racine « L », la taille prévue de la zone racine signée DNSSEC avec l'IPv6, un plein déploiement DS et 1 000 nouveaux noms de domaine de premier niveau, est de 624 791 multiplets. Sur la base des informations reçues de la part des opérateurs de serveurs racine, il est peu probable que ce montant de données de zone représente une pression quelconque pour les serveurs racine. De plus, cette zone racine doit être distribuée à chaque instance de l'ensemble des 13 serveurs racine. Pour les besoins de cette analyse, en supposant que la largeur de bande minimum effective (prenant en considération les parasites, les communications interrompues, etc.) vers l'instance la plus mal connectée de tous les serveurs racine est de 300 bits par seconde, il faudrait environ 4 heures et demie pour transférer la zone entière, donc on reste bien dans les limites de la période actuelle de 12 heures pour la régénération de zone racine [11].

En considérant la situation dans 10 ans et en prenant toujours pour hypothèse un maximum de 1 000 nouveaux TLD par an, l'étude de la racine « L » prévoit que la zone racine aura atteint les 7 471 784 multiplets. De nouveau, sur la base des informations reçues de la part des opérateurs de serveurs racine, il est peu probable que ce montant de données de zone représente une pression quelconque pour les serveurs racine. Concernant la largeur de bande, la largeur de bande minimum nécessaire pour transférer la zone de cette taille dans la fenêtre de 12 heures serait d'environ 1 400 bits par seconde.

Un autre impact potentiel futur de l'ajout des nouveaux TLD est lié à 'l'évasement' de la requête racine. C'est à dire que la dispersion de requêtes à travers un nombre élevé de TLD pourrait avoir un certain impact sur le fonctionnement de serveurs antémémoire individuels. Alors qu'il n'est pas certain qu'un nombre élevé de TLD résulterait en un nombre élevé de requêtes ou que les schémas de requête changeront radicalement, en prenant le cas extrême où un résolveur envoie une requête à chaque TLD dans la racine, la mémoire cache de ce résolveur finira par détenir les enregistrements NS de chaque TLD (avec les enregistrements 'glue' IPv6 et IPv4 et les enregistrements liés aux DNSSEC s'ils existent) pendant toute la TTL de ces enregistrements. Comparé au nombre limité de TLD aujourd'hui, ceci augmenterait la quantité de mémoire consommée par le serveur de nom antémémoire et, selon les techniques de gestion de mémoire du serveur de nom antémémoire, ceci pourrait augmenter la probabilité de saturation de mémoire du serveur de nom antémémoire. Cependant, les serveurs de noms

[10] 924 nouveaux TLD par an pour être spécifique.

[11] Les 300 bits par seconde représentent bien sûr un chiffre invraisemblablement bas. Toutefois, un chiffre plus réaliste permettrait que la zone soit transférée plus rapidement et ainsi l'utilisation de 300 bits par seconde pourrait être considérée comme la pire éventualité.

antémémoire ont déjà à faire à ces sortes de défis de gestion de mémoire puisqu'il existe déjà assez de noms de domaine qui peuvent faire l'objet de requêtes (à tous les niveaux) pour bien inonder toute configuration de mémoire si les requêtes sont adressées assez rapidement (c'est-à-dire dans les TTL des enregistrements de sorte que les nouveaux enregistrements ajoutés soient plus nombreux que les enregistrements ayant expiré). De la sorte, on ne s'attend pas à ce que l'impact lié à un degré plus élevé d'évasement dans la zone racine résulte en un impact considérable sur les serveurs antémémoire.

Comme discuté dans le rapport RSST, l'ajout de nouveaux domaines de premier niveau est susceptible d'avoir des impacts liés aux processus et systèmes dorsaux de traitement utilisés par l'ICANN (dans l'exécution de la fonction IANA), VeriSign et la NTIA. Par exemple, il est probable que les quantités de données maintenues dans la base de données utilisée pour conserver les coordonnées de contact des gestionnaires de TLD augmenteront sensiblement et que les processus utilisés pour passer en revue les requêtes dans chacune des organisations impliquées dans la gestion de la racine aient besoin d'être changés pour faire face à la charge accrue liée aux modifications courantes de zone racine. Toutefois, toutes les organisations impliquées dans la gestion de la racine ont indiqué qu'elles ajusteront leurs ressources pour satisfaire la demande. Ainsi, la considération primordiale est de détecter les charges accrues avant qu'elles ne deviennent pas problématiques et de faciliter l'ajustement des ressources. De ce fait, la surveillance des systèmes de gestion de la racine aux points de ces systèmes où des étranglements pourraient survenir, ainsi que la définition de seuils qui signaleraient les domaines de préoccupation, constituent un champ nécessitant des efforts supplémentaires.

Résumé

Il est vrai que prévoir l'avenir représente un défi. Toutefois, dans le cas de la prévision de l'impact de l'extensibilité de la racine, il semble probable que si nous supposons que les schémas historiques ne changeront pas de manière inattendue, on puisse dire que la croissance à laquelle on s'attend s'encadre bien dans la capacité du système à s'ajuster à cette croissance.

Dans le cas de l'IPv6, près de 70% des domaines de premier niveau ont déjà déployé l'IPv6. Ceci est aussi valable pour 8 des 13 serveurs racine. Il est peu probable qu'un passage à 100% des TLD et des serveurs racine ait des conséquences négatives (des retards modulos éventuels pour les utilisateurs finaux résultant des temporisations vu que l'infrastructure IPv6 n'égale pas encore l'infrastructure IPv4).

Avec les DNSSEC, alors qu'il y aura des ajouts de nouveaux enregistrements DS à mesure que les TLD signeront leurs zones, il est peu probable que ceci cause des changements discernables dans la racine, mis à part le fait que la zone racine grandira à un rythme qui sera (au plus) lié au nombre de nouveaux TLD.

Enfin, l'ajout de nouveaux TLD comporte, en puissance, le plus grand impact, mais étant donné la limite prévue de moins de 1 000 nouveaux TLD par an, il est peu probable que

l'impact de cette croissance cause des perturbations dans la mesure où les systèmes et les processus sont ajustés dans le cadre de mises à niveau opérationnelles normales.

Conclusion

A mesure que le DNS continue à croître et à évoluer pour satisfaire de nouvelles exigences, veiller à ce que ces changements n'aient pas d'impact négatif sur la stabilité du DNS est de la plus haute importance. Suite à la résolution 2009-02-03-04 du Conseil d'administration de l'ICANN, deux études ont été entreprises pour analyser l'impact de l'ajout de l'IPv6, des DNSSEX, des IDN et des nouveaux gTLD à la racine du DNS. Dans l'étude de la racine « L », il a été montré qu'un serveur racine au moins pouvait facilement gérer autant le déploiement des nouvelles technologies que les divers ordres de grandeur quant au nombre de nouveaux TLD, pour que l'ICANN puisse les traiter dans un avenir prévisible. L'étude RSST a suggéré que les nombres absolus n'étaient pas particulièrement pertinents. Dans l'étude, il est suggéré que ce qui est important est plutôt le taux de changement et la manière selon laquelle les divers processus de gestion de la racine et les systèmes dorsaux de traitement étaient modifiés pour gérer les changements.

Cependant, au cours de la période qui s'est écoulée depuis la publication de la résolution 2009-02-03-04, le déploiement de nouvelles technologies s'est poursuivi. Ainsi, des données empiriques peuvent être utilisées pour valider les observations des deux études. Le déploiement de l'IPv6 dans la racine, qui a commencé en 2004, n'a causé aucun effet nuisible important. De même, l'insertion des IDN dans la racine en 2007 s'est effectuée sans heurts du point de vue stabilité du DNS, et le déploiement des DNSSEC dans la racine à partir de janvier 2010 n'a résulté en aucune conséquence négative discernable ou signalée.

En contemplant l'avenir, il est peu probable que les ajouts supplémentaires d'IPv6, de DNSSEC et d'IDN aient un impact négatif sur la stabilité du DNS, quoique le défilement de la clé de signature de clé racine doive être soigneusement géré pour s'assurer que les résolveurs de validation ont la nouvelle ancre de confiance de la racine configurée avant que l'ancienne ancre de confiance ne devienne caduque. Le seul élément imprévisible restant a rapport avec le nombre de nouveaux TLD introduits dans la racine.

Une observation claire des études effectuées en réponse à la résolution 2009-02-03-04 du Conseil d'administration de l'ICANN et des discussions liées à ces études était la nécessité d'améliorer autant la surveillance des systèmes de gestion de la racine que les communications entre les diverses parties prenantes impliquées dans la gestion de la racine. Alors que les modifications apportées à la racine n'ont, à ce jour, résulté en aucun impact négatif discernable, on peut dire que sans surveillance supplémentaire et communications améliorées, l'élargissement de la racine pourrait dépasser un seuil critique sans que l'on s'en aperçoive, ce qui résulterait en des problèmes d'extensibilité qui pourraient affecter la stabilité du DNS dans son ensemble. En supposant que moins de 1 000 nouveaux TLD seront ajoutés par an et que la surveillance et les communications entre les parties prenantes pertinentes seront améliorées, il apparaît

clair que le système racine devrait demeurer stable tout en changeant pour satisfaire les nouvelles demandes.