

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

Résumé des commentaires et analyse

L'ICANN a conduit une période de commentaires publics sur le Résumé de l'impact de l'extensibilité de la zone racine, du 6 octobre 2010 au 5 novembre 2010. Deux commentaires ont été reçus sur le forum.

Résumé des commentaires

L'ICANN a reçu les commentaires de deux individus, dont l'un a noté de manière explicite que les commentaires étaient envoyés d'une manière individuelle. L'analyse de ces commentaires est disponible ci-dessous. On peut consulter le forum des commentaires à l'adresse <http://forum.icann.org/lists/root-zone-scaling-impact/>.

Analyse détaillée

Commentaires des actionnaires

Les commentaires de cette catégorie comprennent l'apport d'Eric Brunner-Williams et de « k claffy », les deux envoyés via le forum de commentaires de l'ICANN.

Eric Brunner-Williams

Brunner-Williams note que le sentiment que « plus de changement est intervenu [dans le DNS] ces 5 ou 6 dernières années que depuis que le DNS a été déployé », n'est peut-être pas universellement partagé. Ce commentaire dans le Résumé de l'impact de l'extensibilité de la zone racine vient de plusieurs sources ; par exemple, l'Annonce de renseignements DNSSEC entreprise par le Département américain du commerce, NTIA déclarait : « une zone racine DNSSEC signée représenterait l'un des changements à l'infrastructure du DNS les plus significatifs depuis sa création¹. » Comme tel, l'association du déploiement de DNSSEC, des IDN, d'Ipv6 et des nouveaux gTLD représenterait une combinaison de changements sans précédent dans le déploiement du DNS. Cependant, il est généralement admis qu'une telle évaluation n'a pas de métrique définie, et peut donc être vue comme étant subjective.

Brunner-Williams s'élève contre l'usage du terme de « personnel ICANN senior ». Ce terme est utilisé 3 fois dans le document « Résumé de l'impact de l'extensibilité de la zone racine » et est issu de la terminologie utilisée dans la Résolution du conseil de l'ICANN, qui établit explicitement :

¹ <http://www.ntia.doc.gov/dns/DNSSECNOI.doc>

« ... implique la participation directe du personnel technique senior de l'ICANN... »

Brunner-Williams note qu'une adjonction maximum de « moins de 1000 nouveaux gTLD par an » est une estimation de l'encours maximum de l'ensemble du système de traitement, y compris le traitement administratif tel que le nombre de contrat ICANN que le conseil a estimé pouvoir traiter, et pas seulement le processus de gestion du changement de la zone racine IANA. Il a le sentiment que l'estimation devrait être mieux explicitée.

Brunner-Williams observe que le projet de Guide de Candidature fait de l'Ipv6 l'assistance obligatoire pour les nouveaux gTLD, bien que le Résumé de l'impact de l'extensibilité de la zone racine note que l'infrastructure de l'Ipv6 ne correspond pas (encore) à l'infrastructure de l'Ipv4 et suggère que l'assistance de l'Ipv6 dans les enregistrements du nouveau gTLD soit rendue optionnelle.

Brunner-Williams pense que la discussion sur l'impact des IDN sur l'IANA et le système d'opérateur de registre n'a pas vocation à apparaître dans un rapport sur l'extensibilité. La section en question résume les impacts que les changements récents au DNS ont eus sur les différents systèmes, et il est donc probable qu'un résumé qui ne comprend pas les impacts sur l'IANA et aux systèmes d'opérateur de registre résultant du déploiement des IDN puisse paraître incomplet.

Brunner-Williams s'élève contre la comparaison entre le traitement des enregistrements AAAA par l'IANA et VeriSign, car il pense que l'ICANN « fait de la comptabilité et des requêtes », tandis que VeriSign « rend opérationnel chaque changement demandé, génère les zones signées, et publie les zones signées ». Bien que cette observation soit juste, cela peut réduire les processus de communication souvent consommateurs de temps et de travail, que le personnel de l'IANA doit entreprendre pour que les administrateurs de TLD reconnaissent que les requêtes sont valides et adéquates, même en surestimant potentiellement l'impact de processus largement automatisés effectués par VeriSign. En termes de temps de traitement (tel que mesuré à partir du point où la requête initiale est reçue par le personnel de l'IANA, jusqu'au point où la requête est transmise au Département américain du commerce, NTIA), c'est généralement beaucoup plus que la quantité de temps passée par VeriSign à implémenter la requête dans la zone racine.

Brunner-Williams pense que deux aspects du Résumé de l'impact de l'extensibilité de la zone racine ne sont pas envisagés :

1. L'impact des conséquences décisives du temps lorsqu'un changement incorrect est publié
2. Comment la coordination de tous les administrateurs de TLD sera mise en œuvre, comme cela s'est avéré utile dans la réponse au variant « C » du worm Conficker.

En ce qui concerne le premier aspect, il semble probable que tout changement incorrect qui serait publié aurait pour résultat une diminution dans l'encours du système de gestion de la racine dans l'ensemble, comme plusieurs systèmes de gestion de la racine (IANA, NTIA et VeriSign) sont préemptés pour procéder à des

corrections, et donc réduire le nombre potentiel de nouveaux entrants dans la racine. Une autre manière de voir ce problème serait de généraliser cela avec un taux d'erreur constant, la hausse dans le nombre de TLD aurait pour résultat une hausse dans le nombre de corrections nécessaires à traiter d'une manière urgente. L'impact des erreurs fait l'objet d'une discussion dans une certaine mesure dans la section 2.2 du rapport sur « l'Extensibilité de la racine », avec une réponse temporelle estimée entre 5 minutes et 36 heures, bien que ce ne soit pas mentionné dans le . Résumé de l'impact de l'extensibilité de la zone racine.

Le second aspect, le fait que la coordination des administrateurs TLD pour la réponse à des événements tels qu'un Conficker n'est, de fait, pas pris en compte dans aucun des rapports sur l'extensibilité de la racine, et n'est pas non plus traité dans la section sur les impacts du rapport « Résumé des impacts de l'extensibilité de la zone racine », puisque la situation dans laquelle les coordinateurs auraient été nécessaires pour un nombre de TLD croissant significatif ne s'est pas présentée. Une analyse séparée et une proposition de mécanismes par lesquels la coordination du TLD peut être assurée pourrait être justifiée.

k claffy

Claffy soutient que le rapport « Résumé de l'impact de l'extensibilité de la zone racine » avance un certain nombre d'affirmations concernant la preuve empirique et n'apporte pourtant pas de citations à l'appui d'estimations fondées ou d'affirmations fondées sur des données. Dans plusieurs cas, les données ont été issues d'expériences sur le serveur racine « L » (puisque le serveur racine « L » qui surveille les données est publiquement disponible à l'adresse <http://stats.l.root-servers.org>) et extrapolées aux autres serveurs racine, en supposant que tous les serveurs racine reçoivent la même distribution (quoique non numérique) de requêtes. Dans d'autres cas, l'analyse de l'impact est fondé sur le manque de conséquences observé sur le déploiement de nouvelles technologies par le personnel de l'ICANN, soit dans les rapports imprimés, les sources d'informations d'Internet, comme les blogs ou Twitter, ou dans les forums d'opérations de réseaux, tels que les listes de diffusion d'opérations de réseau. Ainsi, l'utilisation de termes conditionnels, tels que « pourrait » et « pas significatif (le cas échéant) », a été nécessaire en raison du manque de mécanismes de traitement d'ensemble pour le DNS. Le rapport « Résumé de l'impact de l'extensibilité de la zone racine » note de manière explicite que le traitement des systèmes de gestion de la racine devrait être amélioré.

Claffy pose une série de questions :

- « comment l'ICANN ou d'autres améliorent-ils la surveillance pour être capable de répondre à ces questions de manière plus définitive ? » Proposer des améliorations de la surveillance des systèmes de gestion de la racine a été déclaré hors du champ de compétences d'un document censé résumer l'impact des changements récents apportés au système de racine.
- « l'ICANN peut-il présenter des documents d'aide de reporting, par exemple, combien d'adresses IPv6 ont été ajoutées en 2010, et comment il compare cela à

ce qui est attendu dans 5, 10, 15 ans ? » Le personnel de l'IANA présente² les données historiques suivantes :

Fin d'année	Adresses IPv6
2007	107
2008	161
2009	226
2010	292

Une meilleur ajustement linéaire de ces données aboutit à l'équation $y = 62x + 41.5$ avec un R^2 de 0,9979. En extrapolant ce meilleur ajustement linéaire, on obtient les projections suivantes d'adresses IPv6 associées à des TLD existants :

Fin d'année	Adresses IPv6
2011	352
2012	414
2013	476
2014	538
2015	600
2016	662
2017	724
2018	786
2019	848
2020	910
2021	972
2022	1034
2023	1096
2024	1158
2025	1220
2026	1282

Puisque tous les nouveaux gTLD doivent appuyer l'IPv6, le nombre total d'adresses IPv6 dans la zone racine dépendra du nombre de nouveaux TLD et du nombre d'adresses IPv6 associées à chaque nom de serveur pour les TLD entrés dans la zone racine.

- « à quel rythme une réponse signée était-elle demandée ? quelle fraction des requêtes cela représentait-il ? » Les données sur le serveur racine « L »³ indiquent qu'entre 60 % et 80 % des requêtes avaient autorisé « DNSSEC OK ».
- « quelle fraction (octet) du trafic y avait-il, et dans quelles directions ? » Ces données ne sont pas accessibles au public, cependant, dans la perspective

² Email privé avec Kim Davies, Manager des Services de zone racine à l'ICANN.

³ http://stats.l.root-servers.org/cgi-bin/dsc-grapher.pl?binsize=60&window=604800&plot=do_bit&server=L-root&yaxis=percent

d'étendre l'infrastructure de la zone racine, ce qui importe est la taille de la réponse (puisque les réponses sont invariablement plus longues que les requêtes), que la réponse soit signée DNSSEC ou non. Comme on peut le voir sur les graphiques de tailles de réponse sur le serveur racine « L »⁴, la distribution est multi-modale, avec aucune réponse dépassant 2,5 % de toutes les requêtes, avec une grande majorité de réponses inférieures à 800 octets.

- « quels serveurs racine n'ont pas été signalés [pour des requêtes autorisées EDNS0] ? » Le serveur racine a été utilisé comme représentant de tous les serveurs racine.

Claffy note que les études de données DITL montrent que la plupart des requêtes compétentes-EDNS peuvent être considérées comme de la pollution, et qu'au niveau du client, la transmission de la pollution a diminué avec le temps. Néanmoins, les mesures sur le serveur racine « L » indiquent un pourcentage relativement constant de 70 % de requêtes avec « DNSSEC OK » autorisé. Le fait qu'un serveur racine doive en réalité n'avoir reçu que 30 % de requêtes de ce type est hors de propos, puisque le serveur racine doit répondre, et que la réponse consommera des ressources du serveur racine. Si la pollution des requêtes est réduite, cela reviendra à un échappement croissant dans l'infrastructure du serveur racine.

Claffy demande « quels serveurs sont visés », quand le rapport sur le « Résumé de l'impact de l'extensibilité de la zone racine » déclare « quand la racine signée a été servie de tous les serveurs racine, ces serveurs commencent immédiatement à renvoyer un ensemble d'au moins 50 000 enregistrements de ressource liés au DNSSEC par seconde. » La note de bas de page associée à cette phrase dans le rapport dit :

« En supposant une estimation de retour à l'enveloppe moyen de 8000 requêtes par seconde par ensemble de serveurs racine plus de 13 ensembles de serveurs racine et avec la mention « DNSSEC OK » sur la moitié des requêtes. »

L'intention était de tirer un nombre prudent sans accès à toutes les données (puisque les données ne sont pas systématiquement mise à disposition du public par tous les opérateurs de serveurs racine) pour démontrer que l'infrastructure racine complète était sujette à un nombre non-insignifiant de requêtes autorisées DNSSEC bien qu'aucune indication de problèmes n'ait été reçue par l'ICANN (ou autres associés signant la zone racine). Le « 8000 requêtes par seconde » a été choisi comme estimation de la limite inférieure de la moyenne globale des requêtes par seconde dans tous les groupes de serveurs racine, en tenant compte du fait que les serveurs les plus chargés (A, F, J) recevraient des quantités significativement plus élevées que cela (ex. : plus de 20 000 requêtes/seconde), et les serveurs les moins chargés (D, G, H) recevraient significativement moins (ex. : moins de 2000 requêtes/seconde). Comme on l'a dit, l'estimation du nombre de requêtes avec « OK

⁴ ex. : http://stats.l.root-servers.org/cgi-bin/dsc-grapher.pl?binsize=60&window=604800&plot=rcline_vs_repylen&server=L-root&yaxis=percent

DNSSEC » était de 50 %, ce qui représentait la limite inférieure de ce type de requêtes reçues par le serveur racine « L », puisque l'enregistrement avec le nouveau système de surveillance implémenté dans le « L » remonte à 2007. Ainsi, la dérivation de l'estimation « minimum » est $13 * 8000 * .5 = 52000$, ce qui peut être arrondi à 50 000. La moyenne réelle de requêtes par seconde avec « DNSSEC OK » est, avec certitude, significativement plus élevé que l'estimation utilisée dans le calcul « retour de l'enveloppe », même si des chiffres plus élevés signifieraient plus de chances que quelque chose tourne mal, dont quelqu'un informerait les partenaires de la zone racine.

Claffy note que « 200 n'est pas un taux », dans la phrase « ... le personnel de l'ICANN estime que le taux attendu de nouveaux TLD intégrant la racine sera de l'ordre de 200 ou 300... » L'idée était de dire que le taux attendu de nouveaux TLD serait de 200 à 300 TLD *par an*.

Claffy attire l'attention sur le fait que le RSSAC et le NTIA ne se sont pas engagés (sans doute publiquement) à « ajuster leurs ressources pour satisfaire la demande [d'extensibilité de la racine] ». Compte tenu que le RSSAC est un comité consultatif sans moyen d'imposer des conduites, il n'est pas évident qu'un engagement de sa part impliquerait quoi que ce soit d'utile concernant l'extensibilité du système de racine. Pour ce qui est du NTIA, le SSAC a recommandé⁵ que les partenaires de gestion de la racine (y compris le NTIA) déclarent (individuellement ou conjointement) qu'ils « sont matériellement préparés pour les changements proposés ». Jusqu'à présent, on ne sait pas si cette recommandation a été transmise par l'ICANN de façon formelle aux parties concernées pour qu'elles prennent les mesures adéquates.

Claffy demande « quelles activités sont entreprises pour traiter » la question en suspens de la détection des chargements croissants dans le système de gestion de la racine avant que ces chargements ne deviennent un problème. Il soutient que le verbe « détecter » est impropre à propos de quelque chose qui n'est pas encore arrivé, et suggère que si l'intention était d'utiliser le verbe « prévoir », l'ICANN aurait besoin d'avoir un modèle prédictif ou un « 'seuil d'inquiétude' prudent qui fasse l'unanimité (ouvertement justifié) qui pourrait déclencher une nouvelle enquête ».

Comme le « Résumé de l'impact de l'extensibilité de la zone racine » avait pour but de faire des observations sur des événements advenus depuis que le Conseil de l'ICANN a demandé une analyse de l'impact des activités d'extensibilité de la racine, il a été déclaré hors sujet de détailler les actions qui devraient être entreprises pour traiter les problèmes en suspens. Néanmoins, puisque la gestion de la racine est une opération en cours avec des mesures opérationnelles, dont certaines sont exposées à <https://charts.icann.org/public/index-iana-main.html>, la détection de la charge croissante pourrait être fondée sur des fluctuations significatives du comportement passé (autrement dit, le modèle de prévision est que demain sera similaire à hier). Puisque les fluctuations du comportement passé se produisent avec une certaine

⁵ <http://www.icann.org/en/committees/security/sac046.pdf>

fréquence, la définition d'un « seuil d'inquiétude » est justifiée ; cependant la manière dont le « seuil d'inquiétude » est défini n'entre pas dans les compétences du rapport « Résumé de l'impact de l'extensibilité de la zone racine ».

Claffy demande : « Le chiffre de 1000 TLD annuels est-il considéré unanimement comme prudent par la majorité de la communauté ? » Le rapport sur les « Scénarios de taux de délégation pour les nouveaux gTLD » a été publié pour faire l'objet de commentaires publics du 6 octobre 2010 au 5 novembre 2010. Pendant cette période, un total de 17 commentaires a été reçu. Bien que (à ce jour) l'ICANN n'ait pas encore publié d'analyse/résumé des commentaires, il apparaît que seul un commentaire a traité de manière substantielle les estimations projetées et que ce commentaire exprime le sentiment que les estimations fournies par le rapport sont « entre 20 % et 40 % supérieures à ce qui sera vérifié dans la pratique ».

Claffy demande : « Quelqu'un d'autre a-t-il été consulté au sujet de problèmes possibles avec le manque généralisé de mise en cache négative si le dictionnaire au plus haut niveau du DNS s'enrichit chaque année ? » Le personnel de l'ICANN n'est pas au courant des études sur ce sujet, cependant étant donné que des zones existent, qui sont d'un ordre de grandeur supérieur à la zone racine, et qu'aucun effet indésirable n'a été signalé concernant le manque de mise en cache négative dans ces zones, il est difficile de savoir pourquoi la zone racine serait particulière à cet égard.

Commentaires des Opérateurs de registre, Associations TLD et Organisations Internet

Aucun commentaire reçu.

Commentaires de la Communauté d'affaires

Aucun commentaire reçu.

Étapes suivantes

L'ICANN doit examiner et mettre en œuvre comme il se doit les recommandations du SSAC, comme développé dans le SAC046.

Les commentaires apportés ont soulevé plusieurs points pour lesquels des éclaircissements ou un développement du « Résumé de l'impact de l'extensibilité de la zone racine » seraient utiles. Quatre domaines particuliers pour lesquels une étude complémentaire pourrait être justifiée ont été identifiés :

- Comment la coordination d'un grand nombre d'administrateurs de TLD sera-t-elle effectuée pour obtenir des réponses similaires à celle faite au variant « C » du worm Conficker ?
- Comment la surveillance des systèmes de gestion de la racine peut-elle être améliorée ?
- Comment un « seuil d'inquiétude » peut-il être déterminé ?
- Quels sont les impacts potentiels de la croissance de la zone racine quant à la mise en cache négative dans les résolveurs ?

Commentaires reçus

<i>Individu</i>	<i>URL du commentaire</i>
Eric Brunner-Williams	http://forum.icann.org/lists/root-zone-scaling-impact/msg00000.html
k claffy	http://forum.icann.org/lists/root-zone-scaling-impact/msg00001.html
