Groupe de travail Réseau
Request for Comments : 2870
RFC rendue obsolète : 2010
BCP : 40
Catégorie : Bonne pratiques actuelles
Traduction Claude Brière de L'Isle

R. Bush, Verio
D. Karrenberg, RIPE NCC
M. Kosters, Network Solutions
R. Plzak, SAIC
juin 2000

Exigences pour le fonctionnement du serveur de noms racine

Résumé
Comme l'Internet devient de plus en plus critique pour l'infrastructure économique et sociale du monde, l'attention s'est à juste titre concentrée sur le fonctionnement correct, sûr, et fiable de l'infrastructure Internet elle-même. Les serveurs de noms de domaine racine sont perçus comme une partie cruciale de cette infrastructure technique. Le présent document se concentre principalement sur la fourniture de lignes directrices pour le fonctionnement des serveur de nom de la racine. Les autres opérateurs majeurs de serveur de zone (les gTLD, ccTLD, les zones majeures) peuvent aussi le trouver utile. Ces lignes directrices sont destinées à satisfaire les besoins sociétaux ressentis sans trop prescrire de détails techniques.

1. Fondements

La résolution des noms de domaines sur l'Internet dépend de façon critique du fonctionnement approprié, sûr, et sécurisé des serveurs de noms du domaine racine. Actuellement, ces serveurs au nombre d'environ une douzaine sont fournis et entretenus par un groupe de volontaires très compétents et de confiance. Le présent document ne propose pas de changer cela, mais simplement de fournir des lignes directrices formelles afin que cette communauté comprenne comment et pourquoi cela est fait.

1.1 La corporation pour l'allocation des noms et numéros de l'Internet (ICANN, *Internet Corporation for Assigned Names and Numbers*) a été chargée du fonctionnement des serveurs racines. L'ICANN a chargé un comité consultatif du système de serveurs racines (RSSAC, *Root Server System Advisory Committee*) de donner un avis technique et opérationnel au bureau de l'ICANN. L'ICANN et le RSSAC comptent sur l'IETF pour fournir les normes d'ingénierie.

1.2 Les serveurs racine servent la racine, autrement dit la zone ".". Bien qu'aujourd'hui certains des serveurs racines servent aussi certains TLD (domaines de niveau supérieur) comme les gTLD (COM, NET, ORG, etc.) des TLD d'infrastructure tels que INT et IN-ADDR.ARPA, et certains ccTLD (TLD de code de pays, par exemple FR pour la Francen) cela va vraisemblablement changer (voir en 2.5).

1.3 Les serveurs racines ne sont pas impliqués ni dépendants des données de 'whois'.

1.4 Le système de noms de domaines s'est révélé suffisamment robuste pour qu'on puisse avoir confiance que la perte, temporaire, de la plupart des serveurs racines ne devrait pas affecter significativement le fonctionnement de l'Internet.

1.5 L'expérience a montré que l'Internet est assez vulnérable aux données incorrectes dans la zone ou les TLD racines. L'authentification, la validation, et la sécurité de ces données est donc d'une grande importance.

2. Les serveurs eux-mêmes

Les exigences suivantes s'appliquent aux détails techniques des serveurs racines eux-mêmes :

2.1 Il ne convient pas que le présent document spécifie un matériel, des systèmes d'exploitation ou des logiciels de service de noms particuliers. La variété dans ces domaines est en fait un gage de robustesse globale.

2.2 Chaque serveur DOIT faire fonctionner un logiciel qui mette correctement en œuvre les normes de l'IETF pour le DNS, actuellement, les [RFC1035] et [RFC2181]. Bien qu'il n'y ait pas de suites d'essais formelles pour la conformité aux normes, ceux qui entretiennent le logiciel utilisé sur les serveurs racine sont supposés prendre toutes les actions raisonnables pour se conformer aux attentes actuellement documentées de l'IETF.

2.3 À tout moment, chaque serveur DOIT être capable de traiter une charge de demandes de données racines qui est trois fois la pointe mesurée de ces demandes sur le plus chargé des serveurs dans leurs conditions normales courantes. C'est habituellement exprimé en demandes par seconde. Ceci est destiné à assurer un fonctionnement continu des services racines si deux tiers des serveurs étaient hors service, que ce soit intentionnel, par accident, ou malveillance.

2.4 Chaque serveur racine devrait avoir une connexité suffisante à l'Internet pour prendre en charge la bande passante nécessaire pour l'exigence précédente. La connexité à l'Internet DEVRAIT être aussi diverse que possible. Les serveurs racines DEVRAIENT avoir des mécanismes en place pour accepter la connexité IP au serveur racine à partir de tout fournisseur Internet qui fournit la connexité à ses propres frais.

2.5 Les serveurs DOIVENT ne fournir des réponses d'autorité que pour les zones qu'ils desservent. Les serveurs DOIVENT désactiver les recherches récurrentes, la transmission, ou toute autre fonction qui puisse leur permettre de fournir des réponses tirées d'antémémoires. Ils NE DOIVENT PAS non plus fournir de service secondaire pour une zone autre que la racine et les zones root-servers.net. Ces restrictions aident à empêcher une charge indue sur les serveurs racines et réduit les chances qu'ils mettent en antémémoire des données incorrectes.

2.6 Les serveurs racines DOIVENT répondre aux interrogations provenant de tout hôte Internet, c'est-à-dire qu'il ne peuvent bloquer en aucune façon la résolution de nom racine provenant de toute adresse IP valide, sauf dans le cas d'interrogations qui causent des problèmes de fonctionnement, auquel cas le blocage DEVRAIT ne durer qu'autant que le problème, et être aussi spécifique que raisonnablement possible.

2.7 Les serveurs racines NE DEVRAIENT PAS répondre aux AXFR, ou autre transfert de zone, aux interrogations provenant de clients autres que d'autres serveurs racines. Cette restriction est destinée à, entre autres choses, empêcher une charge inutile sur les serveurs racines car il y a eu des avis tels que "pour éviter d'avoir une antémémoire corruptible, faites de votre serveur une copie furtive de la zone racine". Les serveurs racines PEUVENT activer la zone racine pour ftp ou un autre accès sur un ou plusieurs serveurs moins critiques.

2.8 Les serveurs DOIVENT générer des sommes de contrôle lorsque ils envoient des datagrammes UDP et DOIVENT vérifier les sommes de contrôle lorsque ils reçoivent des datagrammes UDP qui contiennent une somme de contrôle non zéro.

3. Considérations pour la sécurité

Les serveurs ont besoin de sécurité à la fois physique et de protocole ainsi que d'une authentification non ambiguë de leurs réponses.

3.1 La sécurité physique DOIT être assurée de la façon attendue de centres de données critiques pour une entreprise majeure.

3.1.1 Que le site global sur lequel est localisé le serveur racine ait ou non un contrôle d'accès, la zone spécifique dans laquelle est situé le serveur racine DOIT avoir un contrôle d'accès positif, c'est-à-dire que le nombre d'individus qui ont accès à la zone DOIT être limité, contrôlé, et enregistré. Au minimum, des mesures de contrôle DEVRAIENT être des verrous mécaniques ou électroniques. La sécurité physique PEUT être améliorée par l'utilisation d'instruments de détection d'intrusion et de capteurs de mouvement, plusieurs séries de points d'accès, du personnel de sécurité, etc.

3.1.2 Sauf si il existe une expérience documentable d'une fiabilité du réseau d'énergie électrique local supérieure à celle du MTBF d'un UPS (c'est-à-dire, cinq à dix ans) la continuité de l'alimentation électrique pendant au moins 48 heures DOIT être assurée, que ce soit par des batteries sur site, une génération d'électricité sur site, ou une combinaison des deux. Cela DOIT fournir le serveur lui-même, ainsi que l'infrastructure nécessaire pour connecter le serveur à l'Internet. Il DOIT y avoir des procédures qui assurent que les mécanismes et fournitures de secours sont vérifiés pas moins fréquemment que l'exigent les spécifications et recommandations du fabricant.

3.1.3 La détection et/ou des dispositifs de retard d'incendie DOIVENT être fournis.

3.1.4 Des dispositions DOIVENT être prises pour un retour en fonctionnement rapide après une panne du système. Cela

DEVRAIT impliquer une sauvegarde des logiciels et de la configuration des systèmes. Mais cela DEVRAIT aussi impliquer un matériel de sauvegarde qui soit préconfiguré et prêt à prendre la suite du fonctionnement, qui PEUT exiger des procédures manuelles.

3.2 La sécurité du réseau devrait être au niveau fourni pour les infrastructures critiques d'une entreprise commerciale majeure.

3.2.1 Les serveurs racines eux-mêmes NE DOIVENT PAS fournir de services autres que le service de noms de la racine, par exemple, des protocoles Internet distants tels que http, telnet, rlogin, ftp, etc. Les seuls comptes de connexion permis devraient être pour le ou les administrateurs du serveur. L'accès "racine" ou "usager privilégié" NE DOIT PAS être permis sauf à travers un compte d'utilisateur intermédiaire.

Les serveurs DOIVENT avoir un mécanisme sûr pour l'accès administratif et la maintenance à distance. Lorsque surviennent des défaillances, étant donnée l'exigence (selon le point 4.5) d'une disponibilité 24 heures sur 24 et 7 jours sur 7, il y aura des moments où les choses tourneront assez mal pour que des réparateurs très avertis aient à se connecter à distance. La connexion à distance DOIT être protégée par des moyens sûrs qui sont fortement authentifiés et chiffrés, et les sites à partir desquels la connexion distante est permise DOIVENT être protégés et renforcés.

3.2.2 Les serveurs de noms racines NE DEVRAIENT PAS faire confiance aux autres hôtes, sauf les serveurs secondaires qui peuvent faire confiance au serveur principal pour les questions d'authentification, de clés de chiffrement, ou autres informations d'accès ou de sécurité. Si un opérateur racine utilise l'authentification kerberos pour gérer l'accès au serveur racine, le serveur de clés kerberos associé DOIT être protégé avec la même prudence que le serveur racine lui-même. Cela s'applique à tous les services connexes qui sont d'une certaine manière de confiance.

3.2.3 Le ou les segments de LAN sur lesquels est hébergé un serveur racine NE DOIVENT PAS héberger des hôtes vulnérables. C'est-à-dire que les segments de LAN devraient être commutés ou acheminés de telle sorte qu'une usurpation d'identité soit impossible. Certains commutateurs de LAN ne conviennent pas aux exigences de sécurité ; des attaques contre leur filtrage ont été publiées. Bien que celles-ci puissent souvent être empêchées par une configuration soigneuse, une extrême prudence est recommandée. Le mieux est que le segment de LAN n'ait tout simplement pas d'autre hôte.

3.2.4 Le ou les segments de LAN sur lesquels est hébergé un serveur racine DEVRAIENT être protégés par des pare-feu séparés ou un filtrage de paquets séparé pour décourager l'accès réseau sur tout accès autre que ceux nécessaires pour le service de noms.

3.2.5 Les serveurs racines DEVRAIENT avoir leurs horloges synchronisées via NTP [RFC1305] [RFC2030] ou des mécanismes similaires, d'une manière aussi sûre que possible. À cette fin, les serveurs et leurs pare-feu associés DEVRAIENT permettre aux serveurs racines d'être des clients NTP. Les serveurs racines NE DOIVENT PAS agir comme des homologues ou serveurs NTP.

3.2.6 Toutes les tentatives d'intrusion ou autres compromissions DEVRAIENT être enregistrées et tous ces enregistrements sur tous les serveurs racines DEVRAIENT être analysés par une équipe coopérative de sécurité communiquant avec tous les opérateurs de serveurs pour rechercher les schémas, les tentatives sérieuses, etc. Les serveurs DEVRAIENT enregistrer en GMT pour faciliter la comparaison des enregistrements.

3.2.7 Le serveur d'enregistrement DEVRAIT être sur un hôte distinct qui DEVRAIT être protégé de façon similaire à celles des serveurs racines eux-mêmes.

3.2.8 Le serveur DEVRAIT être protégé contre les attaques fondées sur l'acheminement de source. Le serveur NE DOIT PAS s'appuyer sur l'authentification fondée sur l'adresse ou le nom.

3.2.9 Le réseau sur lequel le serveur est hébergé DEVRAIT avoir un service in-addr.arpa.

3.3 L'authentification et la sécurité du protocole doivent s'assurer que les données présentées par les serveurs racines sont celles créées par ceux qui sont autorisés à entretenir les données de la zone racine.

3.3.1 La zone racine DOIT être signée par l'autorité d'allocation des numéros de l'Internet (IANA, *Internet Assigned Numbers Authority*) conformément au DNSSEC, voir la [RFC2535] ou ce qui la remplace. Il est entendu que le DNSSEC n'est pas encore déployé sur certaines plateformes courantes, mais sera déployé lorsque pris en charge.

3.3.2 Les serveurs racines DOIVENT avoir la capacité DNSSEC afin que les interrogations puissent être authentifiées par les clients qui ont des soucis de sécurité et d'authentification. Il est entendu que le DNSSEC n'est pas encore

déployé sur certaines plateformes courantes, mais sera déployé lorsque pris en charge.

3.3.3 Le transfert de la zone racine entre les serveurs racines DOIT être authentifié et être aussi sûr que raisonnablement possible. La validation de sécurité hors bande des mises à jour DOIT être prise en charge. Les serveurs DOIVENT utiliser DNSSEC pour authentifier les zones racines reçues d'autres serveurs. Il est entendu que le DNSSEC n'est pas encore déployé sur certaines plateformes courantes, mais sera déployé lorsque pris en charge.

3.3.4 Un serveur 'principal caché', qui ne permet l'accès qu'aux serveurs racines secondaires autorisés, PEUT être utilisé.

3.3.5 Les mises à jour de zone racine DEVRAIENT ne progresser qu'après qu'un certain nombre de vérifications heuristiques conçues pour détecter les mises à jour erronées aient été effectuées. Dans le cas où la mise à jour échoue à passer les vérifications, une intervention humaine DOIT être demandée.

3.3.6 Les mises à jour de zone racine DEVRAIENT normalement être effectives pas plus de 6 heures après la notification de l'opérateur du serveur racine.

3.3.7 Une procédure spéciales pour les mises à jour urgentes DEVRAIT être définie. Les mises à jour initiées par la procédure d'urgence DEVRAIENT être effectuées pas plus tard que 12 heures après la notification.

3.3.8 Dans l'éventualité d'une défaillance critique du réseau, chaque serveur racine DOIT avoir une méthode pour mettre à jour les données de la zone racine via un support qui sera livré par un chemin de remplacement, en dehors du réseau.

3.3.9 Chaque racine DOIT tenir des statistiques globales sur la quantité et les types d'interrogations reçues/répondues quotidiennement. Ces statistiques doivent être tenues à la disposition des chercheurs accrédités par le RSSAC et le RSSAC pour aider à déterminer comment déployer plus efficacement ces machines à travers l'Internet. Chaque racine PEUT collecter des photographies des données pour aider à déterminer des points de données tels que des tempêtes d'interrogation au DNS, des bogues de mise en œuvre significatives, etc.

4. Communications

Les communications et la coordination entre les opérateurs de serveur racine et entre les opérateurs et l'IANA et l'ICANN sont nécessaires.

4.1 Les interruptions de fonctionnement planifiées et autres temps d'arrêt DEVRAIENT être coordonnés entre les opérateurs de serveur racine pour s'assurer qu'un nombre significatif des serveurs racines ne sont pas arrêtés en même temps. Des annonces préalables des interruptions de fonctionnement planifiées préservent les autres opérateurs des pertes de temps qui résultent des interrogations sur toute anomalie.

4.2 Les opérateurs de serveur racine DEVRAIENT coordonner les prévissions de sauvegarde afin que de nombreux serveurs ne soient pas hors ligne au même moment. Les sauvegardes DEVRAIENT être fréquemment transférées hors site.

4.3 Les opérateurs de serveur racine DEVRAIENT échanger les fichiers de journalisation, en particulier lorsque ils se rapportent à des événements de sécurité, de chargement ,et autres événements significatifs. Cela PEUT se faire par un point de coordination d'enregistrement central, ou PEUT être informel.

4.4 Les statistiques lorsque elles concernent les taux d'usage, la charge, et l'utilisation des ressource, DEVRAIENT être échangées entre les opérateurs, et elles DOIVENT faire l'objet d'un rapport à l'IANA pour les besoins de planification et de rapport.

4.5 Le personnel administratif du serveur de noms racine DOIT être disponible pour assurer le service 24 heures sur 24, 7 jours sur 7. Un appel personnel PEUT être utilisé pour assurer ce service en dehors des heures de service normales.

5. Remerciements

Les auteurs tiennent à remercier Scott Bradner, Robert Elz, Chris Fletcher, John Klensin, Steve Bellovin, et Vern Paxson de leurs commentaires constructifs.

6. Références

[RFC1035] P. Mockapetris, "Noms de domaines – Mise en œuvre et spécification", STD 13, novembre 1987. (*MàJ par la* RFC6604)

[RFC1305] D. Mills, "Protocole de l'heure du réseau, version 3, spécification, mise en œuvre et analyse", STD 12, mars 1992. *(Remplacée par* RFC5905)

[RFC2030] D. Mills, "Protocole simple de l'heure du réseau (SNTP) version 4 pour IPv4, IPv6 et OSI", RFC 2030, octobre 1996. *(Rendue obsolète par la* RFC 4330*)*

[RFC2181] R. Elz et R. Bush, "Clarifications pour la spécification du DNS", juillet 1997. *(Information)*

[RFC2535] D. Eastlake, 3rd, "Extensions de sécurité du système des noms de domaines", mars 1999. (*Obsolète, voir* RFC4033, RFC4034, RFC4035) *(P.S.)*

7. Adresse des auteurs

Randy Bush
Verio, Inc.
5147 Crystal Springs
Bainbridge Island, WA US-98110
téléphone : +1 206 780 0431
mél : randy@psg.com

Daniel Karrenberg
RIPE Network Coordination Centre (NCC)
Singel 258
NL-1016 AB Amsterdam
Netherlands
téléphone : +31 20 535 4444
mél : daniel.karrenberg@ripe.net

Mark Kosters
Network Solutions
505 Huntmar Park Drive
Herndon, VA 22070-5100
téléphone : +1 703 742 0400
mél : markk@netsol.com

Raymond Plzak
SAIC
1710 Goodridge Drive
McLean, Virginia 22102
+1 703 821 6535
mél : plzakr@saic.com

8. Spécification des exigences

Dans le présent document, les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMETE", "PEUT", et "FACULTATIF" sont à interpréter comme décrit dans le BCP 14, [RFC2119].

9. Déclaration complète de droits de reproduction

Remerciement
Le financement de la fonction d'éditeur des RFC est actuellement fourni par la Internet Society.