Groupe de travail Réseau
Request for Comments : 5001
Catégorie : Sur la voie de la normalisation

R. Austein, ISC
août 2007
Traduction Claude Brière de L'Isle

Option Identifiant de serveur de noms (NSID) du DNS

Résumé
Avec l'utilisation accrue de l'envoi à la cantonade du DNS, l'équilibrage de charge, et les autres mécanismes qui permettent que plus d'un serveur de noms du DNS partagent une seule adresse IP, il est parfois difficile de dire lequel des serveurs de noms d'un groupe a répondu à une interrogation particulière. Bien que les mécanismes ad hoc existants permettent à un opérateur d'envoyer des interrogations de suivi quand il est nécessaire de déboguer une telle configuration, la seule façon complètement fiable d'obtenir l'identité du serveur de noms qui a répondu est de faire que le serveur de noms inclue cette information dans la réponse elle-même. La présente note définit une extension du protocole pour prendre en charge cette fonctionnalité.

Table des matières

1. Introduction

Avec l'utilisation accrue de l'envoi à la cantonade du DNS, l'équilibrage de charge, et les autres mécanismes qui permettent à plus d'un serveur de noms du DNS de partager une seule adresse IP, il est parfois difficile de dire quel serveur de noms dans un groupement a répondu à une interrogation particulière.

Les mécanismes ad hoc extistants permettent à un opérateur d'envoyer des interrogations de suivi quand il est nécessaire de déboguer une telle configuration, mais il y a des situations dans lesquelles ceci n'est pas une solution totalement satisfaisante, car l'acheminement à la cantonade peut avoir changé, ou le groupement de serveurs en question peut être

derrière un matériel d'équilibrage de charge extrêmement dynamique. Donc, bien que ces mécanismes ad hoc soient certainement mieux que rien (et aient l'avantage d'être déjà déployés) une meilleure solution semble souhaitable.

Étant donné qu'une interrogation au DNS est une opération idempotente sans état conservé, il semblerait que la seule façon vraiment fiable d'obtenir l'identité du serveur de noms qui a répondu à une interrogation particulière est de faire que ce serveur de noms incluse des informations d'identification dans la réponse elle-même. La présente note définit une amélioration du protocole pour ce faire.

1.1 Mots réservés

Les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT", et "FACULTATIF" en majuscules dans ce document sont à interpréter comme décrit dans le BCP 14, [RFC2119].

2. Protocole

La présente note utilise une option EDNS [RFC2671] pour signaler le désir du résolveur d'obtenir des informations d'identification du serveur de noms et de conserver la réponse du serveur de noms, s'il en est une.

2.1 Comportement du résolveur

Un résolveur signale son désir d'avoir des informations identifiant un serveur de noms par l'envoi d'une option NSID vide (paragraphe 2.3) dans un pseudo RR EDNS OPT dans le message d'interrogation.

Le resolveur NE DOIT PAS inclure de données de charge utile NSID dans le message d'interrogation.

La sémantique d'une demande NSID n'est pas transitive. C'est-à-dire que la présence d'une option NSID dans une interrogation est une demande que le serveur de noms qui reçoit l'interrogation identifie lui-même. Si le côté serveur de noms d'un serveur de noms récurrent reçoit une demande de NSID, le client demande au serveur de noms récurrent de s'identifier ; si le côté résolveur du serveur de noms récurrent souhaite recevoir des informations d'identification, il est libre d'ajouter des demandes NSID dans ses propres interrogations, mais c'est une autre question.

2.2. Comportement du serveur de noms

Un serveur de noms qui comprend l'option NSID et choisit d'honorer une demande NSID particulière répond en incluant les informations d'identification dans une option NSID (paragraphe 2.3) dans un pseudo RR EDNS OPT dans le message de réponse.

Le serveur de noms DOIT ignorer toutes les données de charge utile NSID qui pourraient être présentes dans le message d'interrogation.

L'option NSID n'est pas transitive. Un serveur de noms NE DOIT PAS renvoyer une option NSID à un résolveur qui ne l'a pas demandée. En particulier, alors qu'un serveur de noms récurrent peut choisir d'ajouter une option NSID quand il envoie une interrogation, cela n'a pas d'effet sur la présence ou l'absence de l'option NSID dans la réponse du serveur de noms récurrent au client original.

Comme indiqué au paragraphe 2.1, ce mécanisme n'est pas restreint aux serveurs de noms d'autorité ; sa sémantique est destinée à être également applicable aux serveurs de noms récurrents.

2.3 Option NSID

Le code d'option pour l'option NSID est 3.

Les données d'option pour l'option NSID sont une chaîne d'octets opaque, dont la sémantique est délibérément laissée en dehors du protocole. Voir la discussion du paragraphe 3.1.

2.4 Format de présentation

Les interfaces d'utilisateur DOIVENT lire et écrire le contenu de l'option NSID comme une séquence de chiffres hexadécimaux, deux chiffres par octet de charge utile.

La charge utile de NSID est de données binaires. Toute comparaison entre des charges utiles NSID DOIT être une comparaison des données binaires brutes. Les opérations de copie NE DOIVENT PAS supposer que la charge utile brute de NSID est terminée par des caractères nuls. Toute ressemblance entre des données brutes de charge utile NSID et une forme quelconque de texte serait une pure coïncidence, et ne changerait pas la nature sous-jacente des données de charge utile. Voir la discussion au paragraphe 3.3.

3. Discussion

Cette Section discute certains aspects du protocole et explique les considérations qui ont conduit à ces choix.

3.1 Charge utile NSID

La syntaxe et la sémantique du contenu de l'option NSID sont délibérément laissé en dehors du champ d'application de la présente spécification.

Le choix du contenu du NSID est une prérogative de l'administrateur du serveur. L'administrateur du serveur pourrait choisir de coder le contenu du NSID d'une façon telle que l'opérateur du serveur (ou les clients autorisés par l'opérateur du serveur) puisse décoder le contenu du NSID pour obtenir plus d'informations que ne le peuvent les autres clients. Autrement, l'opérateur du serveur pourrait choisir un contenu de NSID non codé qui soit égalemnt significatif pour tous les clients.

Cette Section décrit certains des types de données que les administrateurs de serveur pourraient choisir de fournir comme contenu de l'option NSID, et explique les raisons de spécifier une simple chaîne d'octets opaque dans le paragraphe 2.3.

Il y a plusieurs possibilités pour la charge utile de l'option NSID :

- Elle pourrait être le nom "réel" du serveur de noms spécifque au sein du groupe de serveurs de noms.

- Elle pourrait être l'adresse IP "réelle" (IPv4 ou IPv6) du serveur de noms au sein du groupe de serveurs de noms.

- Elle pourrait être une sorte de numéro pseudo aléatoire généré de façon quelque peu prévisible en utilisant l'adresse IP ou le nom du serveur comme valeur de germe.

- Elle pourrait être une sorte d'identifiant probabilistiquement unique initialement déduit par une sorte de générateur de nombres aléatoires puis préservé dans les réamorçages du serveur de noms.

- Elle pourrait être une sorte d'identifiant généré de façon dynamique afin que seul l'opérateur du serveur de noms puisse dire si deux interrogations ont ou non reçu une réponse du même serveur.

- Elle pourrait être un ensemble de données signées, avec une clé correspondante qui pourrait (ou non) être disponible via des recherches dans le DNS.

- Elle pourrait être un ensemble de données chiffrées, dont la clé pourrait être restreinte aux parties qui ont besoin de la connaître (du point de vue de l'opérateur du serveur).

- Elle pourrait être une chaîne arbitraire d'octets choisis à la discrétion de l'opérateur du serveur de noms.

Chacune de ces options a des avantages et des inconvénients :

- Utiliser le nom "réel" est simple, mais le serveur de noms peut n'avoir pas de nom "réel".

- Utiliser l'adresse "réelle" est aussi simple, et le serveur de noms a très certainement bien au moins une adresse IP non en envoi à la cantonade pour les opérations de maintenance, mais l'opérateur du serveur de noms peut ne pas vouloir divulguer son adresse non en envoi à la cantonade.

- Étant donné qu'une raison courante pour utiliser les techniques du DNS en envoi à la cantonade est une tentative pour endurcir un serveur de noms critique contre les attaques de déni de service, certains opérateurs de serveurs de noms veulent probablement un identifiant autre que le nom "réel" ou l'adresse "réelle" de l'instance de serveur de noms.

- Utiliser un hachage ou un nombre pseudo aléatoire peut fournir une valeur de longueur fixée que le résolveur peut utiliser pour sortir deux serveurs de noms sans nécessairement être capable de dire qui est "réellement" l'un d'eux, mais rend le débogage plus difficile si l'un d'eux se trouve être dans un environnement ouvert. De plus, le hachage pourrait ne pas apporter grand chose, car un hachage fondé sur une adresse IPv4 n'implique que 32 bits d'espace de recherche, et les noms du DNS utilisés pour les serveurs que les opérateurs pourraient avoir à déboguer à 4 heures du matin tendent à n'être pas très aléatoires.

- Les identifiants probabilistiquement uniques ont des propriétés similaires aux identifiants hachés, mais (avec un générateur de nombres aléatoires suffisamment bon) sont immunisés conte les problèmes d'espace de recherche. Cependant, la force de cette approche est aussi sa faiblesse : il n'y a pas de transformation algorithmique par laquelle même l'opérateur de serveur puisse associer des instances de serveur de noms à des identifiants lors du débogage, ce qui pourrait être ennuyeux. Cette approche exige aussi que l'instance de serveur de noms préserve l'identifiant probabilistiquement unique à travers les réamorçages, mais cela ne paraît pas être une restriction sérieuse, parce que les serveurs de noms d'autorité ont presque toujours une forme de mémorisation non volatile. Dans les rares cas d'un serveur de noms qui n'aurait aucun moyen de mémoriser un tel identifiant, rien de terrible n'arrivera si le serveur de noms génère un nouvel identifiant chaque fois qu'ils se réamorce.

- Utiliser une chaîne d'octets arbitraire donne aux opérateurs de serveur de noms un autre réglage à configurer, ou mal configurer, ou oublier de configurer. Avoir tous les nœuds dans une constellation de serveur de noms en envoi à la cantonade qui s'identifient comme "Mon serveur de noms" ne serait pas particulièrement utile.

- Un ensemble signé n'est pas particulièrement utile comme charge utile de NSID sauf si les données signées sont dynamiques et incluent une forme de protection contre la répétition, comme un horodatage ou une forme de données identifant le demandeur. Les ensembles signés qui satisfont à ces critères pourraient être utiles dans certaines situations mais cela demanderait une analyse de sécurité détaillée qui sort du domaine d'application du présent document.

- Un ensemble chiffré statique ne serait pas particulièrement utile, car il serait soumis à des attaques en répétition et serait, en fait, juste un nombre aléatoire pour toute partie qui ne possède pas la clé de déchiffrement. Les ensembles chiffrés dynamiques pourraient être utiles dans certaines situations mais, comme avec les ensembles signés, les ensembles signés dynamiques demanderaient une analyse de sécurité détaillée qui sort du domaine d'application du présent document.

Étant donnés tous les problèmes mentionnés ci-dessus, il ne paraît pas qu'il y ait une seule solution qui satisfasse tous les besoins. Le paragraphe 2.3 définit donc la charge utile de NSID comme étant une chaîne d'octets opaque et laisse le choix du contenu de la charge utile à la mise en œuvre et à l'opérateur de serveur de noms.

Les lignes directrices suivantes peuvent être utiles aux mises en œuvre et opérateurs de serveurs :

- Les opérateurs pour lesquels la divulgation de l'adresse d'envoi individuel est un problème pourraient utiliser la représentation binaire brute d'un numéro aléatoire probabilistiquement unique. Ce devrait probablement être le comportement de mise en œuvre par défaut.

- Les opérateurs pour lesquels la divulgation de l'adresse d'envoi individuel n'est pas un problème pourraient juste utiliser la représentation binaire brute d'une adresse d'envoi individuel pour sa simplicité. Cela ne devrait être fait que via un choix explicite de configuration par l'opérateur.

- Les opérateurs qui ont réellement besoin ou veulent la capacité de régler la charge utile de NSID à une valeur arbitraire pourraient le faire, mais cela ne devrait être fait que via un choix explicite de configuration par l'opérateur.

Cette approche paraît fournir assez d'informations pour un débogage utile sans laisser involontairement fuir les adresses de maintenance des serveurs de noms d'envoi à la cantonade à des mauvaises personnes, tout en permettant aussi aux opérateurs de serveur de noms qui ne se sentent pas menacés par de telles fuites de fournir plus d'informations à leur discrétion.

3.2 Le NSID n'est pas transitif

Comme spécifié aux paragraphes 2.1 et 2.2, l'option NSID n'est pas transitive. C'est un mécanisme strictement bond par bond.

La plus grande partie de la discussion sur l'identification des serveurs de noms se concentre aujourd'hui sur l'identification des serveurs de noms d'autorité, car les cas les mieux connus de serveurs de noms en envoi à la cantonade sont un sous ensemble des serveurs de noms pour la zone racine. Cependant, étant donné que les techniques du DNS en envoi à la cantonade sont aussi applicables aux serveurs de noms récurrents, le mécanisme peut aussi être utile avec les serveurs de noms récurrents. La sémantique du bond par bond prend cela en charge.

Bien qu'il puisse y avoir une certaine utilité à disposer d'une variante transitive de ce mécanisme (afin, par exemple, qu'un résolveur d'extrémité puisse demander à un serveur récurrent de lui dire quel serveur de noms d'autorité a fourni une certaine réponse au serveur de noms récurrent) la sémantique d'une telle variante serait plus compliquée, et fera l'objet de travaux futurs.

3.3 Questions d'interface d'utilisateur

Étant donnée la gamme de contenus de charge utile possibles décrite au paragraphe 3.1, il n'est pas possible de définir un seul format de présentation pour la charge utile de NSID qui soit efficace, pratique, sans ambiguïté, et esthétiquement satisfaisant. En particulier, bien qu'il soit tentant d'utiliser un format de présentation qui utilise une forme de chaînes textuelles, essayer de le prendre en charge compliquerait significativement ce qui est conçu comme un très simple mécanisme de débogage.

Dans certains cas, le contenu de la charge utile de NSID peut être des données binaires qui n'ont de signification que pour l'opérateur du serveur de noms, et peut n'avoir pas de signification pour l'utilisateur ou l'application, mais l'utilisateur ou l'application doit de toutes façons être capable de saisir la totalité du contenu afin qu'il soit utile. Donc, le format de présentation doit prendre en charge des données binaires arbitraires.

Dans les cas où l'opérateur du serveur de noms déduit la charge utile de NSID de données textuelles, une forme textuelle comme des chaînes US-ASCII ou UTF-8 pourrait à première vue sembler plus facile à traiter pour un utilisateur. Il y a cependant un certain nombre de problèmes complexes impliquant le texte internationalisé qui, s'il était pleinement traité ici, exigerait un ensemble de règles significativement plus long que le reste de cette spécification. Voir dans la [RFC2277] une vue d'ensemble de certaines de ces questions.

Il est beaucoup plus important pour les données de charge utile de NSID d'être passées sans ambiguïté de l'administrateur de serveur à l'utilisateur et retour qu'il ne l'est pour les données de charge utile d'être belles dans le transit. En particulier, il est critique qu'il soit direct pour un utilisateur de copier/coller une copie exacte du résultat de la charge utile de NSID par un outil de débogage dans d'autres formats comme ceux des messages électroniques ou des formes de la Toile sans distortion. Les chaînes hexadécimales, bien que vilaines, sont aussi robustes.

3.4 Troncature

Dans certains cas, ajouter l'option NSID à un message de réponse peut déclencher la troncature du message. La présente spécification ne change en aucune façon les règles de troncature de message du DNS, mais les mises en œuvre devront faire attention à ce problème.

Inclure l'option NSID dans une réponse est toujours facultatif, et donc la présente spécification n'exige jamais des serveurs de noms qu'ils tronquent les messages de réponse.

Par définition, un résolveur qui demande des réponses NSID prend aussi en charge EDNS, de sorte qu'un résolveur qui demande des réponses NSID peut aussi utiliser le champ "Taille de charge utile UDP de l'envoyeur" du pseudo RR OPT pour signaler une taille de mémoire tampon de réception assez grande pour rendre la troncature improbable.

4. Considérations relatives à l'IANA

IANA a alloué le code d'option EDNS de 3 à l'option NSID (paragraphe 2.3).

5. Considérations sur la sécurité

Le présent document décrit un mécanisme de signalisation de canal destiné principalement au débogage. Les mécanismes de sigalisation de canal sortent par nature du domaine d'application de DNSSEC. Les applications qui exigent la protection de l'intégrité des données signalées devront utiliser un mécanisme de sécurité du canal comme TSIG [RFC2845].

Le paragraphe 3.1 discute d'un certain nombre de différentes sortes d'informations qu'un opérateur de serveur de noms pourrait choisir comme valeur de l'option NSID. Certains de ces types d'informations sont sensibles à la sécurité dans certains environnements. La présente spécification laisse délibérément la syntaxe et la sémantique du contenu de l'option NSID à la mise en œuvre et à l'opératreur de serveur de noms.

Deux des sortes possibles de données de charge utile discutées au paragraphe 3.1 impliquent respectivement une signature numérique et le chiffrement. Bien que cette spécification discute de certains des pièges qui peuvent s'ouvrir sous les pieds d'utilisateurs négligents de ces sortes de données de charge utile, une analyse complète des problèmes qui seraient impliqués dans ces types de données de charge utile exigerait la connaissance du contenu à signer ou chiffrer, des algorithmes à utiliser, et ainsi de suite, ce qui sort du domaine d'application de ce document. Ceux qui mettent en œuvre devrait rechercher des avis compétents avant de tenter d'utiliser ces sortes de charge utile de NSID.

6. Remerciements

Merci à Joe Abley, Harald Alvestrand, Dean Anderson, Mark Andrews, Roy Arends, Steve Bellovin, Alex Bligh, Randy Bush, David Conrad, John Dickinson, Alfred Hoenes, Johan Ihren, Daniel Karrenberg, Peter Koch, William Leibzon, Ed Lewis, Thomas Narten, Mike Patton, Geoffrey Sisson, Andrew Sullivan, Mike StJohns, Tom Taylor, Paul Vixie, Sam Weiler, et Suzanne Woolf, dont aucun n'est responsable de ce que l'auteur a fait de leurs commentaires et suggestions. Mes excuses à tous ceux qui auraient par inadvertance été omis de la liste ci-dessus.

7. Références

7.1 Références normatives

[RFC2119] S. Bradner, "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997. *(MàJ par* RFC8174)

[RFC2671] P. Vixie, "Mécanismes d'extension pour le DNS (EDNS0)", août 1999. *(P.S.) (Remplacée par* RFC6891)

[RFC2845] P. Vixie et autres, "Authentification de transaction de clé secrète pour DNS (TSIG)", mai 20000 (*MàJ par* RFC3645 *; remplacée par* RFC8945 *; P.S.)*

7.2 Références pour information

[RFC2277] H. Alvestrand, "Politique de l'IETF en matière de jeux de caractères et de langages", BCP 18, janvier 1998.

Adresse de l'auteur

Rob Austein
ISC
950 Charter Street
Redwood City, CA 94063
USA

mél : sra@isc.org

Déclaration complète de droits de reproduction

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