

Groupe de travail Réseau
Request for Comments : 1995
RFC mise à jour : 1035
Catégorie : En cours de normalisation

M. Ohta, Tokyo Institute of Technology
août 1996

Traduction Claude Brière de L'Isle

Transfert de zone par incrément dans le DNS

Statut de ce mémoire

Le présent document spécifie un protocole en cours de normalisation de l'Internet pour la communauté de l'Internet, et appelle à des discussions et suggestions pour son amélioration. Prière de se référer à l'édition actuelle des "Normes officielles de protocole de l'Internet" (STD 1) pour l'état de normalisation et le statut de ce protocole. La distribution du présent mémoire n'est soumise à aucune restriction.

Résumé

Le présent document propose des extensions au protocole DNS pour fournir un mécanisme de transfert de zone par incrément (IXFR, *incremental zone transfer*).

1. Introduction

Pour la propagation rapide des changements d'une base de données du DNS [STD13], il est nécessaire de réduire la latence en notifiant activement les serveurs du changement. Cela est accompli par l'extension NOTIFY du DNS [RFC1996].

Le mécanisme actuel de transfert complet de zone (AXFR) n'est pas un moyen efficace de propager les changements à une petite partie d'une zone, car il transfère le fichier entier de la zone.

Le transfert incrémentaire (IXFR) proposé est un mécanisme plus efficace, car il ne transfère que la ou les portions modifiées d'une zone.

Dans le présent document, un serveur de noms secondaire qui demande IXFR est appelé un client IXFR et un serveur de noms principal ou secondaire qui répond à la demande est appelé un serveur IXFR.

2. Brève description du protocole

Si un client IXFR, qui a vraisemblablement une version plus ancienne d'une zone, pense qu'il a besoin de nouvelles informations sur la zone (normalement par une fin de temporisation de rafraîchissement de SOA ou par le mécanisme NOTIFY), il envoie un message IXFR contenant le numéro de série du SOA de sa copie de zone, dont il présume qu'elle est périmée.

Un serveur IXFR devrait garder un enregistrement de la dernière version de la zone et des différences entre cette copie et plusieurs versions plus anciennes. Lorsque une demande IXFR est reçue avec un numéro de version plus ancien, le serveur IXFR a seulement besoin d'envoyer les différences pour actualiser cette version. Autrement, le serveur peut choisir de transférer la zone entière juste comme dans un transfert de zone normal.

Lorsque une zone a été mise à jour, elle devrait être sauvegardée dans une mémoire stable avant que la nouvelle version ne soit utilisée pour répondre aux demandes IXFR (ou AXFR). Autrement, si le serveur a une défaillance, les données qui ne sont plus disponibles peuvent avoir été distribuées aux serveurs secondaires, qui peuvent causer des incohérences persistantes de la base de données.

Si une interrogation IXFR avec le même numéro de version ou un plus récent que celui du serveur est reçue, il y est répondu par un seul enregistrement SOA de la version actuelle du serveur, tout comme dans AXFR.

Le transport d'une interrogation peut être par UDP ou par TCP. Si une interrogation IXFR se fait via UDP, le serveur IXFR peut tenter de répondre en utilisant UDP si la réponse entière peut être contenue dans un seul paquet DNS. Si la réponse UDP ne tient pas, on répond à l'interrogation avec un seul enregistrement SOA de la version actuelle du serveur pour informer le client qu'une interrogation TCP devrait être lancée.

Donc, un client devrait d'abord faire une interrogation IXFR en utilisant UDP. Si le type d'interrogation n'est pas reconnu par le serveur, on devrait essayer une AXFR (précédée d'une interrogation de SOA en UDP), pour s'assurer de la rétro

compatibilité. Si la réponse à l'interrogation est un seul paquet avec la nouvelle zone entière, ou si le serveur n'a pas de version plus récente que celle du client, il n'y a rien de plus à faire. Autrement, une interrogation IXFR devrait être essayée sur TCP.

Pour s'assurer de l'intégrité, les serveurs devraient utiliser les sommes de contrôle UDP pour toutes les réponses UDP. Un client prudent qui reçoit un paquet UDP avec une valeur de somme de contrôle de zéro devrait ignorer le résultat et essayer à la place une interrogation IXFR sur TCP.

La valeur du type d'interrogation de IXFR allouée par l'IANA est 251.

3. Format d'interrogation

Le format du paquet d'interrogation IXFR est le même que celui d'une interrogation normale du DNS; mais avec le type d'interrogation de IXFR et la section Autorité contenant l'enregistrement SOA de la version de la zone du client.

4. Format de réponse

Si le transfert de zone par incrément n'est pas disponible, la zone entière est retournée. Le premier et le dernier RR de la réponse est l'enregistrement SOA de la zone. C'est-à-dire que l comportement est le même que pour une réponse AXFR, sauf que le type d'interrogation est IXFR.

Si le transfert de zone par incrément est disponible, une ou plusieurs séquences de différences sont retournées. La liste des séquences de différences est précédée et suivie d'une copie de la version actuelle de la SOA du serveur.

Chaque séquence de différence représente une mise à jour de la zone (un changement dans la série de la SOA) consistant en RR supprimés et en RR ajoutés. Le premier des RR supprimés est l'ancien RR de SOA et le premier des RR ajoutés est le nouveau RR de SOA.

La modification d'un RR est effectuée en retirant d'abord le RR d'origine puis en ajoutant le RR modifié.

Les séquences d'informations différentielles sont ordonnées de la plus ancienne à la plus récente. Donc, les séquences différentielles sont l'histoire des changements faits depuis la version connue du client IXFR jusqu'à la version actuelle du serveur.

Les RR peuvent être partiels dans les messages de transfert incrémentaire. C'est à dire que si un seul RR parmi plusieurs RR du même type de RR change, seul le RR modifié est transféré.

Un client IXFR ne devrait remplacer une version ancienne par une nouvelle qu'après que toutes les différences ont été traitées avec succès.

Une réponse incrémentaire est différente d'une réponse non incrémentaire en ce qu'elle commence par deux RR SOA, le RR SOA actuel du serveur suivi du RR SOA de la version du client qui va être remplacée.

5. Stratégie de purge

Un serveur IXFR peut n'être pas obligé de détenir pour toujours toutes les versions antérieures, et peut les supprimer à tout moment. En général, il y a un compromis entre la taille de l'espace mémoire et la possibilité d'utiliser IXFR.

Les informations sur les anciennes versions devraient être purgées si la longueur totale d'une réponse IXFR serait plus longue que celle d'une réponse AXFR. Comme l'objet de IXFR est de réduire la redondance de AXFR, cette stratégie est assez raisonnable. Elle assure que la quantité de mémoire requise est au plus deux fois celle des informations de la zone actuelle.

Les informations plus anciennes que la période de péremption de la SOA peuvent aussi être purgées.

6. Condensation facultative de plusieurs versions

Un serveur IXFR peut facultativement condenser plusieurs séquences de différences en une seule séquence de différences, et donc, abandonner les informations sur les versions intermédiaires.

Cela peut être bénéfique si beaucoup de versions, dont toutes ne sont pas utiles, ont été générées. Par exemple, si plusieurs serveurs FTP partagent un seul nom DNS et si l'adresse IP associée à ce nom est changée une fois par minute pour équilibrer la charge entre les serveurs FTP, il n'est pas si important de garder trace de tout l'historique des changements.

Mais cette caractéristique peut n'être pas aussi utile si un client IXFR a accès à deux serveurs IXFR, A et B, avec des résultats de condensation incohérents. La version actuelle du client IXFR, reçue du serveur A, peut être inconnue du serveur B. Dans un tel cas, le serveur B ne peut pas fournir de données incrémentaires à partir d'une version inconnue, et un transfert de zone complet est nécessaire.

La condensation est entièrement facultative. Les clients ne peuvent pas détecter à partir de la réponse si le serveur a condensé ou non la réponse.

Pour l'interopérabilité, les serveurs IXFR, y compris ceux qui n'ont pas la caractéristique de condensation, ne devraient pas afficher une erreur même si ils reçoivent la demande IXFR d'un client avec un numéro de version inconnu et devraient plutôt essayer d'effectuer un transfert de zone complet.

7. Exemple

Soient les trois générations de données suivantes, avec le numéro de série actuel de 3,

```
JAIN.AD.JP.          IN SOA NS.JAIN.AD.JP. mohta.jain.ad.jp. (1 600 600 3600000 604800)
                   IN NS  NS.JAIN.AD.JP.
NS.JAIN.AD.JP.      IN A  133.69.136.1
NEZU.JAIN.AD.JP.    IN A  133.69.136.5
```

NEZU.JAIN.AD.JP. est retiré et JAIN-BB.JAIN.AD.JP. est ajouté

```
jain.ad.jp.         IN SOA ns.jain.ad.jp. mohta.jain.ad.jp. (2 600 600 3600000 604800)
                   IN NS  NS.JAIN.AD.JP.
NS.JAIN.AD.JP.      IN A  133.69.136.1
JAIN-BB.JAIN.AD.JP. IN A  133.69.136.4
                   IN A  192.41.197.2
```

Une des adresses IP de JAIN-BB.JAIN.AD.JP. est changée.

```
JAIN.AD.JP.         IN SOA ns.jain.ad.jp. mohta.jain.ad.jp. (3 600 600 3600000 604800)
                   IN NS  NS.JAIN.AD.JP.
NS.JAIN.AD.JP.      IN A  133.69.136.1
JAIN-BB.JAIN.AD.JP. IN A  133.69.136.3
                   IN A  192.41.197.2
```

L'interrogation IXFR suivante

En-tête	OPCODE=SQUERY
Question	QNAME=JAIN.AD.JP., QCLASS=IN, QTYPE=IXFR
Réponse	<vide>
Autorité	JAIN.AD.JP. IN SOA serial=1
Supplémentaire	<vide>

pourrait recevoir une réponse avec le message de transfert de zone complète suivant :

En-tête	OPCODE=SQUERY, RESPONSE
Question	QNAME=JAIN.AD.JP., QCLASS=IN, QTYPE=IXFR
Réponse	JAIN.AD.JP. IN SOA serial=3 JAIN.AD.JP. IN NS NS.JAIN.AD.JP. NS.JAIN.AD.JP. IN A 133.69.136.1 JAIN-BB.JAIN.AD.JP. IN A 133.69.136.3 JAIN-BB.JAIN.AD.JP. IN A 192.41.197.2 JAIN.AD.JP. IN SOA serial=3
Autorité	< vide>
Supplémentaire	< vide>

ou avec le message incrémentaire suivant :

En-tête	OPCODE=SQUERY, RESPONSE
Question	QNAME=JAIN.AD.JP., QCLASS=IN, QTYPE=IXFR
Réponse	JAIN.AD.JP. IN SOA serial=3 JAIN.AD.JP. IN SOA serial=1 NEZU.JAIN.AD.JP. IN A 133.69.136.5 JAIN.AD.JP. IN SOA serial=2 JAIN-BB.JAIN.AD.JP. IN A 133.69.136.4 JAIN-BB.JAIN.AD.JP. IN A 192.41.197.2 JAIN.AD.JP. IN SOA serial=2 JAIN-BB.JAIN.AD.JP. IN A 133.69.136.4 JAIN.AD.JP. IN SOA serial=3 JAIN-BB.JAIN.AD.JP. IN A 133.69.136.3 JAIN.AD.JP. IN SOA serial=3
Autorité	< vide>
Supplémentaire	< vide>

ou avec le message incrémentaire condensé suivant :

En-tête	OPCODE=SQUERY, RESPONSE
Question	QNAME=JAIN.AD.JP., QCLASS=IN, QTYPE=IXFR
Réponse	JAIN.AD.JP. IN SOA serial=3 JAIN.AD.JP. IN SOA serial=1 NEZU.JAIN.AD.JP. IN A 133.69.136.5 JAIN.AD.JP. IN SOA serial=3 JAIN-BB.JAIN.AD.JP. IN A 133.69.136.3 JAIN-BB.JAIN.AD.JP. IN A 192.41.197.2 JAIN.AD.JP. IN SOA serial=3
Autorité	<vide>
Supplémentaire	<vide>

ou, si survient un débordement de paquet UDP, avec le message suivant :

En-tête	OPCODE=SQUERY, RESPONSE
Question	QNAME=JAIN.AD.JP., QCLASS=IN, QTYPE=IXFR
Réponse	JAIN.AD.JP. IN SOA serial=3
Autorité	<vide>
Supplémentaire	<vide>

8. Remerciements

L'idée d'origine de IXFR a été conçue par Anant Kumar, Steve Hotz et Jon Postel.

De nombreuses personnes ont contribué à l'affinage du protocole et de sa documentation, y compris, mais sans s'y limiter, Anant Kumar, Robert Austein, Paul Vixie, Randy Bush, Mark Andrews, Robert Elz et les membres du groupe de travail

DNSIND de l'IETF.

9. Références

[RFC1996] P. Vixie, " Mécanisme de notification rapide des changements de zone (DNS NOTIFY)", août 1996.

[STD13] P. Mockapetris, " Système des noms de domaines", STD 13, RFC 1034 et RFC 1035), novembre 1987.

10. Considérations pour la sécurité

Bien que le DNS soit touché par plusieurs problèmes de sécurité, le présent document ne tente en aucune façon de les régler.

On estime que le présent document n'introduit aucun problème supplémentaire de sécurité au protocole DNS actuel.

11. Adresse de l'auteur

Masataka Ohta
Computer Center
Tokyo Institute of Technology
2-12-1, O-okayama, Meguro-ku, Tokyo 152, JAPAN

téléphone : +81-3-5734-3299

Fax : +81-3-5734-3415

mél : mohta@necom830.hpcl.titech.ac.jp