Groupe de travail Réseau
Request for Comments : 1996
RFC mise à jour: 1035
Catégorie : En cours de normalisation

P. Vixie, ISC
août 1996

Traduction Claude Brière de L'Isle

Mécanisme de notification rapide des changements de zone (DNS NOTIFY)

Résumé
Le présent mémoire décrit l'opcode NOTIFY pour le DNS, par lequel un serveur maître avise un ensemble de serveurs esclaves de la modification des données du maître et qu'une interrogation devrait être initiée pour découvrir les nouvelles données.

1. Raisons et portée

1.1 La lenteur de la propagation des données nouvelles et des changements dans une zone du DNS peut être due à des temps de rafraîchissement relativement longs dans la zone. Des temps de rafraîchissement plus longs sont bénéfiques en ce qu'ils réduisent la charge sur les serveurs maîtres, mais ce bénéfice est au prix de longs intervalles d'incohérence parmi les serveurs d'autorité chaque fois que la zone est mise à jour.

1.2 La transaction NOTIFY du DNS permet aux serveurs maîtres d'informer les serveurs esclaves quand la zone change – une rupture par rapport au modèle d'interrogation – dont il est espéré qu'elle va réduire le délai de propagation tout en n'augmentant pas indûment la charge des maîtres. La présente spécification permet seulement aux esclaves d'avoir notification des changements de RR SOA, mais l'architecture de NOTIFY est destinée à être extensible aux autres types de RR.

1.3 Le présent document donne intentionnellement plus de définition aux rôles de serveur "maître," "esclave" et "furtif", à leur énumération dans les RR NS, et au champ MNAME de SOA. En ce sens, le présent document peut être considéré comme un addendum à la [RFC1035].

2. Définitions et invariants

2.1 Définitions utilisées dans le document

esclave — un serveur d'autorité qui utilise le transfert de zone pour restituer la zone. Tous les serveurs esclaves sont nommés dans les RR NS pour la zone.

maître — tout serveur d'autorité configuré pour être la source des transferts de zone pour un ou plusieurs serveurs esclaves.

maître principal — serveur maître à la racine du graphe de dépendance des transferts de zone. Le maître principal est nommé dans le champ SOA MNAME de la zone et facultativement par un RR NS. Il n'y a, par définition, qu'un seul serveur maître principal par zone.

furtif — comme un serveur esclave sauf qu'il ne figure pas sur la liste d'un RR NS pour la zone. Un serveur furtif, sauf configuré explicitement pour faire autrement, va établir le bit AA dans les réponses et sera capable d'agir comme un maître. Un serveur furtif ne sera connu par d'autres serveurs que si ils ont reçu des données de configuration statique qui indiquent son existence.

ensemble notifié — ensemble de serveurs auxquels sont notifiés les changements de certaines zones. C'est pas défaut tous les serveurs désignés dans le RRset NS, excepté tout serveur aussi désigné dans le SOA MNAME. Certaines mises en œuvre permettent à l'administrateur de serveur de noms d'outrepasser cet ensemble ou d'y

ajouter des éléments (comme, par exemple, des serveurs furtifs).

2.2 Les serveurs de la zone doivent être organisés en un graphe de dépendance tel qu'il y ait un maître principal, et tous les autres serveurs doivent utiliser AXFR ou IXFR soit à partir du maître principal, soit à partir d'un esclave qui est aussi un maître. Aucune boucle n'est permise dans le graphe de dépendance AXFR.

3. Message NOTIFY

3.1 Lorsque un maître a mis à jour un ou plusieurs RR auxquels les serveurs esclaves peuvent être intéressés, il peut envoyer le nom des RR changés, ainsi que leur classe, type, et facultativement le ou les nouveaux RDATA, à chaque serveur esclave connu en utilisant un protocole au mieux fondé sur l'opcode NOTIFY.

3.2 NOTIFY utilise le format de message du DNS, bien qu'il n'utilise qu'un sous-ensemble des champs disponibles. Les champs qui ne sont pas autrement décrits ici sont à remplir avec des zéros binaires (0), et les mises en œuvre doivent ignorer tous les messages pour lesquels ce n'est pas le cas.

3.3 NOTIFY est similaire à QUERY en ce qu'il est un message de demande avec le fanion d'en-tête QR "non établi" et un message de réponse avec QR "établi". Le message de réponse ne contient pas d'informations utiles, mais sa réception par le maître est l'indication que l'esclave a reçu le NOTIFY et que le maître peut retirer l'esclave de toute file d'attente pour réessayer cet événement NOTIFY.

3.4 Le protocole de transport utilisé pour une transaction NOTIFY sera UDP sauf si le maître a des raisons de croire que TCP est nécessaire ; par exemple, si un pare-feu a été installé entre le maître et l'esclave, et que seul TCP est admis; ou, si le RR changé est trop grand pour tenir dans un datagramme UDP/DNS.

3.5 Si TCP est utilisé, le maître et l'esclave doivent tous deux continuer d'offrir le service des noms durant la transaction, même lorsque la transaction TCP ne progresse pas. La demande NOTIFY est envoyée une fois, et une "fin de temporisation" est dite être survenue si aucune réponse NOTIFY n'est reçue dans un intervalle raisonnable.

3.6 Si UDP est utilisé, un maître envoie périodiquement une demande NOTIFY à un esclave jusqu'à ce que trop de copies aient été envoyées (une "fin de temporisation") ou qu'un message ICMP indiquant que l'accès est injoignable, ou qu'une réponse NOTIFY soit reçue de l'esclave avec un identifiant d'interrogation, QNAME, adresse IP de source, et numéro d'accès UDP de source qui correspondent.

Note : L'intervalle entre les transmissions, et le nombre total de retransmissions, devraient être des paramètres de fonctionnement spécifiables par l'administrateur du serveur de noms, peut-être zone par zone. Un intervalle par défaut raisonnable est de 60 secondes (ou une temporisation si on utilise TCP) et un maximum de cinq retransmissions (pour UDP). Il est considéré comme raisonnable d'utiliser un repli additif ou exponentiel pour l'intervalle entre les essais.

3.7 Une demande NOTIFY a QDCOUNT > 0, ANCOUNT ≥ 0, AUCOUNT ≥ 0, ADCOUNT ≥ 0. Si ANCOUNT > 0, la section Réponse représente alors une indication non sûre au nouveau RRset pour ce tuplet <QNAME, QCLASS, QTYPE>. Un esclave qui reçoit une telle indication est libre de traiter l'équivalence de cette section Réponse avec ses données locales comme l'indication que "aucun autre travail n'est nécessaire". Si ANCOUNT = 0, ou ANCOUNT > 0 et si la section Réponse diffère des données locales de l'esclave, celui-ci devrait alors interroger ses maîtres connus pour la restitution des nouvelles données.

3.8 La section Réponse d'une demande NOTIFY ne doit en aucun cas être utilisée pour mettre à jour les données locales d'un esclave, ou pour indiquer qu'il est nécessaire d'entreprendre un transfert de zone, ou de changer les temporisateurs de rafraîchissement de zone de l'esclave.

Seule une condition "données présentes ; mêmes données" peut conduire un esclave à agir, si ANCOUNT > 0, différemment de ce qu'il ferait si ANCOUNT = 0.

3.9 La présente version de la spécification NOTIFY n'utilise pas les sections Autorité ou Données supplémentaires, et donc les mises en œuvre conformes devraient régler AUCOUNT = 0 et ADCOUNT = 0 lors de la transmission des demandes. Comme une future révision de la présente spécification pourrait définir une utilisation rétro compatible pour l'une ou/et l'autre de ces sections, les mises en œuvre actuelles doivent ignorer ces sections, mais pas le message entier, si AUCOUNT > 0 et/ou ADCOUNT > 0.

3.10 Si un esclave reçoit une demande NOTIFY de la part d'un hôte qui n'est pas un maître connu pour la zone qui

contient le QNAME, il devrait ignorer la demande et produire un message d'erreur dans son journal de fonctionnement.

Note : Cela implique que les esclaves d'un maître multi rattachements doivent soit connaître leur maître par la "plus proche" des adresses d'interface du maître, soit connaître toutes les adresses d'interface du maître. Autrement, une demande NOTIFY valide pourrait venir d'une adresse qui n'est pas sur la liste d'état des maîtres pour la zone de l'esclave, ce qui serait une erreur.

3.11 Le seul événement NOTIFY défini pour le moment est que le RR SOA a changé. À l'achèvement d'une transaction NOTIFY pour QTYPE = SOA, l'esclave devrait se comporter comme si la zone donnée dans le QNAME avait atteint l'intervalle REFRESH (voir la [RFC1035]) c'est-à-dire qu'il devrait interroger ses maîtres sur la SOA de la zone donnée dans le QNAME du NOTIFY, et vérifier la réponse pour voir si le SOA SERIAL a été incrémenté depuis la dernière fois qu'il est allé chercher la zone. S'il en est ainsi, un transfert de zone (AXFR ou IXFR) devrait être lancé.

Note : Comme un graphe de dépendance des serveurs poussé peut avoir des chemins multiples entre le maître principal et un esclave donné, il est possible qu'un esclave reçoive un NOTIFY de l'un de ses maîtres connus bien que le reste de ses maîtres connus n'ait pas encore mis à jour leur copie de la zone. Donc, lors de la production d'une QUERY pour la SOA de zone, l'interrogation devrait être dirigée sur le maître connu comme source de l'événement NOTIFY, et pas sur les autres maîtres connus. Cela représente une différence avec la [RFC1035], qui spécifie qu'à l'expiration de l'intervalle REFRESH de la SOA, tous les maîtres connus devraient être interrogés tour à tour.

3.12 Si une demande NOTIFY est reçue par un esclave qui ne met pas en œuvre l'opcode NOTIFY, il va répondre par un message NOTIMP (erreur Caractéristique non mise en œuvre). Un serveur maître qui reçoit un tel NOTIMP devrait considérer la transaction NOTIFY comme terminée pour cet esclave.

4. Détails et exemples

4.1 La conservation des informations d'état des interrogations lors du réamorçage des hôtes est facultative, mais il est raisonnable de simplement exécuter une transaction NOTIFY de SOA sur chaque zone d'autorité lorsqu'un serveur démarre.

4.2 Chaque esclave va vraisemblablement recevoir plusieurs copies de la même demande NOTIFY: Une du maître principal, et une de chaque autre esclave lorsque celui-ci transfère la nouvelle zone et le notifie à ses homologues potentiels. Le protocole NOTIFY prend en charge cette multiplicité en exigeant que NOTIFY soit envoyé par un esclave/maître seulement APRÈS qu'il a mis à jour le RR SOA ou qu'il a déterminé qu'aucune mise à jour n'était nécessaire, ce qui en pratique signifie après un transfert de zone réussi. Donc, en interdisant le réarrangement des livraisons, le dernier NOTIFY que reçoit tout esclave est celui qui indique le dernier changement. Comme un esclave demande toujours les SOA et les AXFR/IXFR des seuls maîtres connus, il aura l'opportunité de réessayer son QUERY pour le SOA après que chacun de ses maîtres a terminé la mise à jour de chaque zone.

4.3 Si un serveur maître cherche à éviter de causer un grand nombre de transferts simultanés de zones sortantes, il peut retarder d'un délai arbitraire l'envoi d'un message NOTIFY à un esclave donné. On suppose que ce délai sera choisi de façon aléatoire, de sorte que chaque esclave commence son transfert à un instant unique. Le délai ne devra en aucun cas être supérieur au délai REFRESH de la SOA.

Note : Ce délai devrait être un paramètre que chaque serveur de nom maître principal peut spécifier, peut-être sur la base de la zone. Des délais aléatoires de 30 à 60 secondes sembleraient adéquats si les serveurs partagent un LAN et si les zones sont de taille modérée.

4.4 Un esclave qui reçoit un NOTIFY valide devrait différer d'agir sur tout NOTIFY ultérieur avec le même tuplet <QNAME, QCLASS, QTYPE> jusqu'à ce qu'il ait achevé la transaction commencée par le premier NOTIFY. Ce rejet des dupliqués nécessaire pour éviter d'avoir plusieurs notifications conduit à maltraiter le serveur maître.

4.5 La zone est mise à jour sur le maître principal

Le maître principal envoie une demande NOTIFY à tous les serveurs désignés dans l'ensemble NOTIFY. La demande NOTIFY a les caractéristiques suivantes :

identifiant d'interrogation : (nouveau)

code d'opération :	NOTIFY (4)
réponse :	NOERROR
fanions :	AA
qcount :	1
qname :	(nom de zone)
qclass :	(classe de zone)
qtype :	T_SOA

4.6 La zone est mise à jour sur un esclave qui est aussi maître

Comme ci-dessus en 4.5, sauf que l'ensemble NOTIFY de ce serveur peut être différent de celui du maître principal du fait d'une spécification statique facultative des serveurs furtifs locaux.

4.7 L'esclave reçoit une demande NOTIFY d'un maître

Lorsque un serveur esclave reçoit une demande NOTIFY de l'un de ses maîtres désignés localement pour la zone qui comporte le QNAME en question, avec QTYPE = SOA et QR = 0, il devrait entrer dans l'état dans lequel il serait si le temporisateur de rafraîchissement de la zone était arrivé à expiration. Il va aussi renvoyer une réponse NOTIFY à la source de la demande NOTIFY, avec les caractéristiques suivantes :

identifiant d'interrogation :	(le même)
code d'opération :	NOTIFY (4)
réponse :	NOERROR
fanions :	QR AA
qcount :	1
qname :	(nom de zone)
qclass :	(classe de zone)
qtype :	T_SOA

C'est destiné à être identique à la demande NOTIFY, sauf que le bit QR est aussi mis. L'identifiant d'interrogation de la réponse doit être le même que celui reçu dans la demande.

4.8 Le maître reçoit une réponse NOTIFY de l'esclave

Lorsque un serveur maître reçoit une réponse NOTIFY, il supprime cette interrogation de la file d'attente de réessais, terminant ainsi le "processus de notification" de "ce" changement de RRset pour "ce" serveur.

5. Considérations pour la sécurité

On estime que les seules considérations pour la sécurité de l'opération NOTIFY sont :

1. qu'une demande NOTIFY avec une adresse IP/UDP de source falsifiée peut être cause qu'un esclave envoie des interrogations de SOA parasites à ses maîtres, ce qui conduirait à une attaque bénigne de déni de service si les fausses demandes sont envoyées très souvent ;

2. qu'une parodie de TCP pourrait être utilisée contre un serveur esclave en donnant un NOTIFY comme moyen de synchroniser une interrogation de SOA, et une parodie d'UDP/DNS comme moyen de forcer un transfert de zone.

6. Références

[RFC1035] P. Mockapetris, "Noms de domaines – Mise en œuvre et spécification", STD 13, RFC 1035, novembre 1987.

[IXFR] M. Ohta, " Transfert de zone par incrément", RFC1995, août 1996.

7. Adresse de l'auteur

Paul Vixie
Internet Software Consortium
Star Route Box 159A
Woodside, CA 94062
USA
téléphone : +1 415 747 0204
mél : paul@vix.com