Groupe de travail Réseau
**Request for Comments : 3597**
Catégorie : En cours de normamisation

A. Gustafsson, Nominum Inc.
septembre 2003
Traduction Claude Brière de L'Isle

# Traitement des types d'enregistrement de ressource (RR) inconnus du DNS

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



**Résumé**
Étendre le système de nom de domaine (DNS, *Domain Name System*) avec de nouveaux types d'enregistrement de ressource (RR, *Resource Record*) exige actuellement des changements au logiciel de serveur de noms. Le présent document spécifie les changements nécessaires pour permettre aux mises en œuvre futures du DNS de traiter de façon transparente les nouveaux types de RR.

## 1. Introduction

Le DNS est conçu pour être extensible afin de prendre en charge de nouveaux services par l'introduction de nouveaux types d'enregistrement de ressource (RR). En pratique, déployer un nouveau type de RR exige actuellement des changements du logiciel de serveur de noms non seulement au serveur DNS d'autorité qui fournit les nouvelles informations et au client qui les utilise, mais aussi de tous les serveurs esclaves pour la zone les contenant, et dans certains cas aussi aux serveurs de noms qui les gardent en antémémoire et aux transmetteurs utilisés par le client.

Parce que le déploiement de nouveaux logiciels de serveur est lent et coûteux, le potentiel du DNS à prendre en charge de nouveaux services n'a jamais été pleinement réalisé. Le présent mémoire propose des changements aux serveurs de noms et aux procédures pour définir de nouveaux types de RR visant à simplifier le déploiement futur de nouveaux types de RR.

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 la [RFC2119].

## 2. Définition

Un "RR de type inconnu" est un RR dont le format RDATA n'est pas connu de la mise en œuvre actuelle du DNS, et dont le type n'est pas un QTYPE ou Meta-TYPE alloué comme spécifié dans la [RFC2929] (paragraphe 3.1) ni dans la gamme réservée dans cette section pour l'allocation aux seuls QTYPE et Meta-TYPE. Un tel RR ne peut pas être converti en un format de texte spécifique du type, compressé, ou traité autrement d'une façon spécifique d'un type.

Dans le cas d'un type dont le format RDATA est spécifique d'une classe, un RR est considéré comme étant de type inconnu lorsque le format RDATA pour cette combinaison de type et de classe n'est pas connu.

## 3. Transparence

Pour permettre de déployer de nouveaux types de RR sans changement aux serveurs, les serveurs de noms et les résolveurs DOIVENT traiter les RR de type inconnu de façon transparente. C'est-à-dire qu'ils doivent traiter la section RDATA de tels RR comme des données binaires non structurées, les mémorisant et les transmettant sans changement [RFC1123].

Pour assurer le fonctionnement correct de la comparaison d'égalité (section 6) et de la forme canonique du DNSSEC (section 7) lorsque le type RR est connu de certains mais pas de tous les serveurs impliqués, les serveurs DOIVENT aussi préserver

exactement le RDATA des RR de type connu, sauf pour les changements dus à la compression ou la décompression lorsque elle est permise par la section 4 du présent mémoire. En particulier, la casse de caractère des noms de domaine qui ne sont pas soumis à compression DOIT être préservée.

## 4. Compression de nom de domaine

Les RR qui contiennent des pointeurs de compression dans la partie RDATA ne peuvent pas être traités de façon transparente, car les pointeurs de compression n'ont de sens que dans le contexte d'un message DNS. La copie transparente du RDATA dans un nouveau message DNS serait cause que les pointeurs de compression pointeraient sur la localisation correspondante dans le nouveau message, qui contient maintenant des données sans rapport. Cela causerait la corruption du nom compressé.

Pour éviter une telle corruption, les serveurs NE DOIVENT PAS compresser les noms de domaine incorporés dans le RDATA des types qui sont spécifiques de classe ou pas bien connus. Cette exigence a été posée dans la [RFC1123] sans qu'elle définissent le terme "bien connu" ; il est spécifié ici que seuls les types de RR définis dans la [RFC1035] sont considérés comme "bien connus".

La spécification des quelques types de RR existants a explicitement permis une compression contraire à la présente spécification : la [RFC2163] spécifiait que la compression s'applique aux RR PX, et la [RFC2535] permettait la compression dans les RR SIG et les RR NXT. Comme la présente spécification déconseille la compression dans ces cas, il s'agit d'une mise à jour de la [RFC2163] (section 4) et de la [RFC2535] (paragraphes 4.1.7 et 5.2).

Les serveurs receveurs DOIVENT décompresser les noms de domaine dans les RR de type bien connu, et DEVRAIENT aussi décompresser les RR de type RP, AFSDB, RT, SIG, PX, NXT, NAPTR, et SRV (bien que la spécification actuelle du RR SRV dans la [RFC2782] interdise la compression, la [RFC2052] la rendait obligatoire, et certains serveurs qui suivent cette ancienne spécification sont toujours en service).

De futures spécifications pour de nouveaux types de RR qui contiennent des noms de domaines dans leur RDATA NE DOIVENT PAS permettre l'utilisation de la compression de nom pour ces noms, et DEVRAIENT explicitement déclarer que les noms de domaine incorporés NE DOIVENT PAS être compressés.

Comme noté dans la [RFC1123], le nom du propriétaire d'un RR est toujours susceptible de compression.

## 5. Représentation de texte

Dans le champ "type" d'une ligne de fichier maître, un type de RR inconnu est représenté par le mot "TYPE" immédiatement suivi par le nombre décimal du type de RR, sans espace interposée. Dans le champ "class", un classe inconnue est similairement représentée par le mot "CLASS" immédiatement suivi par le nombre décimal de la classe.

Cette convention permet que les types et classes soient distingués les uns des autres et des valeurs de TTL, ce qui permet que les deux formes "[<TTL>] [<class>] <type> <RDATA>" et "[<class>] [<TTL>] <type> <RDATA>" de la [RFC1035] soient analysées sans ambiguïté.

La section RDATA d'un RR de type inconnu est représentée par une séquence de mots séparés par des espaces blanches comme suit :

- Le jeton spécial \# (barre oblige inverse immédiatement suivie par un signe dièse) qui identifie le RDATA comme ayant le codage générique défini ici plutôt qu'un codage spécifique de type traditionnel.
- Un entier décimal non signé spécifiant la longueur du RDATA en octets.
- Zéro, un ou plusieurs mots de données en hexadécimal codant le champ RDATA réel, contenant chacun un nombre pair de chiffres hexadécimaux.

Si le RDATA est de longueur zéro,la représentation de texte contient seulement le jeton \# et le seul zéro qui représente la longueur.

Une mise en œuvre PEUT aussi choisir de représenter des RR de type connu en utilisant la représentations générique ci-dessus pour le type, la classe et/ou le RDATA, qui présente l'avantage de rendre le fichier maître résultant portable aux serveurs où ces types sont inconnus. Utiliser la représentation générique pour le RDATA d'un RR de type connu peut aussi être utile dans le cas d'un type de RR où le format du texte varie selon la version, le protocole, ou champs similaires incorporés dans le RDATA lorsque un tel champ a un valeur pour laquelle aucun format de texte n'est connu, par exemple, un RR LOC [RFC1876] avec une VERSION autre que 0.

Bien qu'un RR de type connu représenté dans le format \# soit effectivement traité comme un type inconnu pour les besoins de l'analyse de la représentation du texte du RDATA, tout le reste du traitement par le serveur DOIT le considérer comme un type connu et prendre en compte toutes les règles spécifiques du type applicables concernant la compression, la canonisation, etc.

Voici des exemples de RR représentés de cette manière, illustrant diverses combinaisons de codages génériques et spécifiques du type pour les différents champs du format de fichier maître :

```
a.example.   CLASS32     TYPE731        \# 6 abcd (  ef 01 23 45 )
b.example.   HS          TYPE62347      \# 0
e.example.   IN          A              \# 4 0A000001
e.example.   CLASS1      TYPE1          10.0.0.2
```

## 6. Comparaison d'égalité

Certains protocoles du DNS, en particulier Dynamic Update [RFC2136], exigent que les RR soient comparés en égalité. Deux RR du même type inconnu sont considérés égaux lorsque leurs RDATA sont égaux bit par bit. Pour s'assurer que le résultat de la comparaison est identique que le RR soit connu ou non du serveur, les spécifications des nouveaux types de RR NE DOIVENT PAS spécifier de règles de comparaison spécifiques du type.

Cela implique que les noms de domaine incorporés, étant inclus dans la comparaison globale bit par bit, sont comparés de façon sensible à la casse.

Il en résulte que lorsque un nouveau type de RR contient un ou plusieurs noms de domaine incorporés, il est possible d'avoir plusieurs RR possédés par le même nom qui ne diffèrent que par la casse de caractères du ou des noms de domaine incorporés. Ceci est similaire à la possibilité existante de plusieurs enregistrements TXT ne différant que par la casse des caractères, et qui ne sont pas supposés causer de problème en pratique.

## 7. Forme et ordre canonique de DNSSEC

DNSSEC définit une forme canonique et un ordre pour les RR [RFC2535] (paragraphe 8.1). Dans cette forme canonique, les noms de domaine incorporés dans le RDATA sont convertis en minuscules.

Le changement de casse est nécessaire pour assurer que les signatures du DNSSEC sont correctes lorsque les distinctions de casse dans les noms de domaine sont perdues à cause de la compression, mais comme la connaissance de la présence et de la position des noms de domaine incorporés est nécessaire, il ne peut pas être appliqué aux types inconnus.

Pour assurer une cohérence continue de la forme canonique des types de RR où la compression est permise, et pour une interopérabilité continue avec les mises en œuvre existantes qui appliquent déjà la forme canonique de la [RFC2535] et l'appliquent aux types de RR qu'elles connaissent, la forme canonique reste inchangée pour tous les types de RR dont la publication initiale comme RFC était antérieure à la publication initiale de la présente spécification comme RFC (RFC 3597).

Par courtoisie à l'égard des mises en œuvre, on note ici que l'ensemble complet des types de RR publiés antérieurement qui contiennent des noms de domaine incorporés, et dont la forme canonique de DNSSEC implique donc la transformation en minuscules conformément aux règles du DNS pour les comparaisons de caractères, comporte les types de RR NS, MD, MF, CNAME, SOA, MB, MG, MR, PTR, HINFO, MINFO, MX, HINFO, RP, AFSDB, RT, SIG, PX, NXT, NAPTR, KX, SRV, DNAME, et A6.

Le présent document spécifie que pour tous les autres types de RR (qu'ils soient traités comme des types inconnus ou des types connus selon la définition d'un type de RR d'une RFC plus récente que la RFC 3597) la forme canonique est telle qu'aucune réduction de casse des noms de domaine incorporés n'a lieu, et par ailleurs identique à la forme canonique spécifiée dans la [RFC2535] paragraphe 8.1.

Noter que le nom du propriétaire est toujours établi en minuscules, conformément aux règles du DNS pour les comparaisons de caractères, sans considération du type de RR.

L'ordre canonique de RR de DNSSEC est celui spécifié dans la [RFC2535] paragraphe 8.3, où la séquence d'octets est la forme canonique telle que révisée par la présente spécification.

## 8. Traitement de section supplémentaire

Les types de RR inconnus ne causent pas de traitement de section supplémentaire. De futures spécifications de type de RR PEUVENT spécifier des règles de traitement de section supplémentaires spécifique de type, mais un tel traitement DOIT être facultatif car il ne peut être effectué que par des serveurs pour lesquels le type de RR en cause est connu.

## 9. Considérations relatives à l'IANA

Le présent document n'exige aucune action de la part de l'IANA.

## 10. Considérations sur la sécurité

On ne pense pas que la présente spécification cause de nouveau problème de sécurité, ni qu'elle en résolve d'existants.

## 11. Références normatives

[RFC1034] P. Mockapetris, "Noms de domaines - Concepts et facilités", STD 13, novembre 1987.

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

[RFC1123] R. Braden, éditeur, "Exigences pour les hôtes Internet – Application et prise en charge", STD 3, octobre 1989.

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

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

[RFC2163] C. Allocchio, "Utilisation du DNS Internet pour distribuer des transpositions d'adresses mondiales conformes à MIXER (MCGAM)", janvier 1998. (*MàJ par* RFC3597) *(P.S.)*

[RFC2929] D. Eastlake 3rd, E. Brunner-Williams et B. Manning, "Considérations relatives à l'IANA pour le système des noms de domaine (DNS)", BCP 42, septembre 2000. *(Obsolète, voir la* RFC5395)

## 12. Références pour information

[RFC1876] C. Davis, P. Vixie, T. Goodwin, I. Dickinson, "Un moyen pour exprimer les informations de localisation dans le système des noms de domaine", janvier 1996. *(MàJ* RFC1034, RFC1035) *(Expérimentale)*

[RFC2052] A. Gulbrandsen, P. Vixie, "Enregistrement DNS pour spécifier la localisation de services (DNS SRV)", octobre 1996. (*Obsolète, voir* RFC2782) *(Expérimentale)*

[RFC2136] P. Vixie, S. Thomson, Y. Rekhter et J. Bound, "Mises à jour dynamiques dans le système de noms de domaine (DNS UPDATE)", avril 1997.

[RFC2782] A. Gulbrandsen, P. Vixie et L. Esibov, "Enregistrement de ressource DNS pour la spécification de la localisation des services (DNS SRV)", février 2000.

## 13. Déclaration de propriété intellectuelle

L'IETF ne prend pas position sur la validité et la portée de tout droit de propriété intellectuelle ou autres droits qui pourrait être revendiqués au titre de la mise en œuvre ou l'utilisation de la technologie décrite dans le présent document ou sur la mesure dans laquelle toute licence sur de tels droits pourrait être ou n'être pas disponible ; pas plus qu'elle ne prétend avoir accompli aucun effort pour identifier de tels droits. Les informations sur les procédures de l'ISOC au sujet des droits dans les documents

de l'ISOC figurent dans les BCP 78 et BCP 79.

Des copies des dépôts d'IPR faites au secrétariat de l'IETF et toutes assurances de disponibilité de licences, ou le résultat de tentatives faites pour obtenir une licence ou permission générale d'utilisation de tels droits de propriété par ceux qui mettent en œuvre ou utilisent la présente spécification peuvent être obtenues sur répertoire en ligne des IPR de l'IETF à http://www.ietf.org/ipr.

L'IETF invite toute partie intéressée à porter son attention sur tous copyrights, licences ou applications de licence, ou autres droits de propriété qui pourraient couvrir les technologies qui peuvent être nécessaires pour mettre en œuvre la présente norme. Prière d'adresser les informations à l'IETF à ietf-ipr@ietf.org.

## 14. Adresse de l'auteur

Andreas Gustafsson
Nominum, Inc.
2385 Bay Rd
Redwood City, CA 94063
USA

téléphone : +1 650 381 6004
mél : gson@nominum.com

## 15. Déclaration complète de droits de reproduction



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