

Groupe de travail Réseau
Request for Comments : 3405
BCP : 65
Catégorie : Bonnes pratiques actuelles

M. Mealling
VeriSign
octobre 2002
Traduction Claude Brière de L'Isle

Système de découverte dynamique de délégation (DDDS) Partie V : Procédures d'allocation d'URI.ARPA

Statut de ce mémoire

Le présent document spécifie les bonnes pratiques actuelles pour la communauté de l'Internet et appelle à des discussions et suggestions pour son amélioration. La distribution du présent mémoire n'est soumise à aucune restriction.

Notice de copyright

Copyright (C) The Internet Society (2002). Tous droits réservés.

Résumé

Le présent document est le cinquième d'une série qui est complètement spécifiée dans "Système de découverte dynamique de délégation (DDDS) Partie I : DDDS complet" [RFC3401]. Il est important de noter qu'il est impossible de lire et comprendre un des documents de cette série sans lire les autres.

(Incorpore les errata 2687 et 2688 du 20/01/2011)

Table des Matières

1.	Introduction.....
2.	Résolution d'URI contre résolution d'URN.....
3.	Politiques d'enregistrement.....
4.	Exigences relatives aux indications.....
5.	Procédure de soumission.....
6.	Gabarit d'enregistrement.....
7.	Gabarit exemple.....
8.	Enregistrement d'URN dans la zone URI.ARPA.....
9.	Considérations relatives à l'IANA.....
10.	Considérations pour la sécurité.....
11.	Remerciements.....
12.	Références.....
13.	Adresse de l'auteur.....
14.	Déclaration complète de droits de reproduction.....

1. Introduction

Le présent document définit les politiques et procédures pour insérer des enregistrements de pointeurs d'autorité de désignation (NAPTR, *Naming Authority Pointer*) dans les zones "URI.ARPA" et "URN.ARPA" pour les besoins de la résolution des identifiants de ressource uniformes (URI, *Uniform Resource Identifier*) conformément au "Système de découverte dynamique de délégation (DDDS) Partie IV : Application de résolution d'URI" [RFC3402], qui est une application qui utilise la base de données du DDDS fondée sur le système des noms de domaines (DNS, *Domain Name System*). Tous ces concepts sont définis dans la [RFC3401]. Il est important de noter qu'il est impossible de comprendre correctement ce document sans lire la RFC3401 et les documents qu'elle spécifie.

La [RFC3403] définit comment est utilisé le DNS comme base de données DDDS qui contient les règles de délégation d'URI (parfois appelées indications de résolution). Ce document spécifie que la première étape de cet algorithme est d'ajouter "URI.ARPA" au schéma d'URI et de restituer l'enregistrement NAPTR pour ce nom de domaine. C'est-à-dire que la première étape de la résolution de "http://foo.com/" serait de rechercher un enregistrement NAPTR pour le domaine "http.URI.ARPA". La résolution d'URN suit aussi une procédure similaire mais utilise la zone "URN.ARPA" comme racine. Le présent document décrit les procédures d'insertion d'une nouvelle règle dans les zones "URI.ARPA" et "URN.ARPA".

2. Résolution d'URI contre résolution d'URN

La [RFC3402] définit à la fois le travail de résolution d'URI [RFC2396] et de résolution d'URN [RFC2141] lorsque le DNS est utilisé comme base de données de règles de délégation (ou d'indications). Elle dit précisément que les instructions initiales ("indications") pour la résolution des URI fondée sur le DNS sont mémorisées comme enregistrements de ressources dans la zone "URI.ARPA" du DNS.

Comme un URN est un schéma d'URI, une indication pour la résolution du préfixe d'URI "urn:" va aussi être mémorisée dans la zone "URI.ARPA". Cette règle déclare que l'identifiant d'espace de noms [RFC2141] est extrait, "URN.ARPA" est ajouté à la fin de l'identifiant d'espace de noms, et le résultat est utilisé comme clé pour restituer un enregistrement NAPTR [RFC3404] ultérieur.

3. Politiques d'enregistrement

La création d'un schéma d'identifiant d'espace de noms (NID, *namespace id*) d'URI ou d'URN suit les documents d'enregistrement appropriés pour ces espaces. Les schémas d'URI suivent les "Procédures d'enregistrement pour les noms de schémas d'URL" [RFC2717]. Les identifiants d'espace de noms d'URN suivent les "Mécanismes de définition d'espace de noms d'URN" [RFC2611](ou leurs mises à jour).

3.1 Enregistrement URI.ARPA

3.1.1 Seuls schémas admis dans l'arborescence IETF

Pour être inséré dans la zone URI.ARPA, le schéma d'URI suivant DOIT être enregistré sous l'arborescence d'URI de l'IETF. Les exigences pour cette arborescence sont spécifiées dans la [RFC2717].

3.1.2 L'enregistrement de schéma a la priorité

L'enregistrement d'un enregistrement NAPTR pour un schéma d'URI NE DOIT PAS précéder l'enregistrement approprié de ce schéma et la publication d'une spécification stable conformément à la [RFC2717]. L'IESG ou son expert désigné vont revoir la demande pour s'assurer

1. qu'elle est correcte et fondée techniquement,
2. qu'elle est cohérente avec la spécification d'URI publiée,
3. et pour s'assurer que l'enregistrement NAPTR pour un URI fondé sur le DNS ne délègue pas la résolution de l'URI à une autre partie que le détenteur du nom du DNS. Cette dernière règle a pour but de s'assurer qu'une indication de résolution d'URI donnée ne capture pas (par inadvertance ou autrement) du trafic réseau pour un certain domaine.

3.1.3 L'enregistrement NAPTR peut accompagner l'enregistrement de schéma

Une demande d'enregistrement d'un URI.ARPA PEUT accompagner une demande pour un schéma d'URI (conformément à la [RFC2717]) auquel cas les deux demandes seront révisées de concert par l'IESG ou ses experts désignés.

3.1.4 Enregistrement ou changements après un enregistrement de schéma

Une demande pour un enregistrement NAPTR (ou une demande de changement d'un enregistrement existant de NAPTR) PEUT être soumis après l'enregistrement du préfixe d'URI. Si la spécification du préfixe d'URI est contrôlée par quelqu'un d'autre que l'IETF, l'IESG demandera l'approbation du propriétaire/gestionnaire de cette spécification avant d'accepter la spécification. Ceci s'ajoute à toute révision technique de l'enregistrement du NAPTR faite par l'IESG ou ses experts désignés.

3.2 Enregistrement d'URN.ARPA

3.2.1 L'enregistrement NID a la priorité

L'enregistrement d'un enregistrement NAPTR pour un NID d'URN NE DOIT PAS précéder l'enregistrement approprié de ce NID et la publication d'une spécification stable conformément à la [RFC2611]. Ceci est destiné à empêcher que l'enregistrement d'un enregistrement de NAPTR dans l'URN.ARPA circonvienne le processus d'enregistrement de NID.

3.2.2 Un enregistrement de NAPTR peut accompagner un enregistrement de NID

Une demande d'enregistrement d'un URN.ARPA PEUT accompagner une demande d'un NID (conformément à la [RFC2611]) auquel cas les deux demandes seront revues en même temps.

3.2.3 Enregistrement ou changements après un enregistrement de schéma

Une demande pour un enregistrement NAPTR (ou pour changer un enregistrement NAPTR existant) PEUT être soumise après l'enregistrement du NID. Si la spécification du NID est contrôlée par quelqu'un d'autre que l'IETF, l'IESG exigera l'approbation du propriétaire/gestionnaire de cette spécification avant que l'enregistrement soit accepté. Ceci s'ajoute à toute révision technique de l'enregistrement du NAPTR faite par l'IESG ou ses experts désignés.

Noter que ceci s'applique à tous les enregistrements NAPTR pour un NID particulier, même si un enregistrement NAPTR pouvait n'affecter qu'une partie de l'espace d'URN alloué à un NID

4. Exigences relatives aux indications

La délégation d'un espace de noms peut survenir de deux façons. Dans le cas de la plupart des URI, la clé qui est déléguée est codée avec l'identifiant lui-même (par exemple, un nom d'hôte dans un URI HTTP). La syntaxe pour l'emplacement de cette nouvelle clé est prédéterminée par la syntaxe du schéma. Dans d'autres cas, la nouvelle clé peut faire partie de l'indication elle-même. C'est l'équivalent fonctionnel de dire : "si cette règle correspond, alors ceci est toujours la clé."

Pour minimiser la charge des interrogations sur les zones URI.ARPA et URN.ARPA, on prévoit que les enregistrements de ressources dans ces zones auront des "durées de vie" (TTL) extrêmement longues, peut-être mesurées en années.

Donc, pour tout préfixe d'URI ou espace de nom d'URN pour lequel les indications de résolution vont vraisemblablement changer, la règle réelle devrait être mémorisée dans une autre zone (moins stable) du DNS, et au sein de URI.ARPA ou URN.ARPA, un enregistrement stable du NAPTR devrait être utilisé pour déléguer les interrogations à une zone moins stable.

Par exemple, l'espace de noms d'URN "foo" a des règles souples pour la façon dont a lieu la délégation. Au lieu de mettre ces règles dans la zone URN.ARPA, l'entrée renvoie plutôt ces règles à un serveur de noms qui a une durée de vie plus courte. L'enregistrement dans l'URN.ARPA ressemblerait à :

```
foo IN NAPTR 100 10 "" "" "" urn-resolver.foo.com.
```

Donc, lorsque le client commence le processus de résolution, la première étape sera d'interroger "foo.URN.ARPA" pour trouver l'enregistrement ci-dessus, la seconde étape est de commencer à demander à "urn-resolver.foo.com" les enregistrements NAPTR qui contiennent les règles de résolution. Le TTL à la racine est très long. Le TTL à "urn-resolver.foo.com" est beaucoup plus court.

À l'inverse, le schéma d'URI "http" adhère à une syntaxe particulière qui spécifie que l'hôte à demander est spécifié dans l'URI en question. Comme cette syntaxe ne change pas, cette règle peut être spécifiée dans la zone URI.ARPA. L'enregistrement ressemblerait à ceci :

```
http IN NAPTR 100 100 "" "" "http:\\\\([^\V:]+)\1/i" .
```

Donc, la seconde étape de résolution est d'utiliser le nom de domaine trouvé dans l'URI comme la nouvelle clé dans le cycle. Si, par exemple, ce NAPTR est terminal et contient un nom d'hôte dans le champ Remplacement, le client pourrait alors contacter cet hôte afin de poser des questions sur cet URI particulier.

5. Procédure de soumission

En utilisant le mécanisme d'enregistrement de type de contenu MIME [RFC2048] comme modèle de mécanisme réussi d'enregistrement, les procédures "URI.ARPA" et "URN.ARPA" consistent en un gabarit de demande soumis à une liste de diffusion ouverte constituée de parties intéressées. Si aucune objection n'est faite pendant une période de deux semaines, un représentant de l'autorité d'enregistrement considère la soumission comme acceptée et l'entre dans le serveur de noms.

- o Les enregistrements pour la zone "URI.ARPA" sont envoyées à "register@URI.ARPA".
- o Les enregistrements pour la zone "URN.ARPA" sont envoyés à "register@URN.ARPA".

L'autorité d'enregistrement est l'Autorité d'allocation des numéros de l'Internet (IANA).

Les objections sont restreintes à ceux qui invoquent un impact sur la zone elle-même ou sur le DNS en général. Les objections au schéma d'URI ou à l'identifiant d'espace de noms d'URN ne sont pas admises, car elles devraient être soulevées dans leurs forums respectifs. La conclusion logique de cela est que TOUT schéma d'URI ou espace de nom d'URI sanctionné DOIT être admis à l'enregistrement si il satisfait aux exigences spécifiées dans le présent document en ce qui concerne la durée de vie et l'impact général sur le DNS.

6. Gabarit d'enregistrement

Le gabarit à envoyer à la liste appropriée DOIT contenir les valeurs suivantes :

6.1 Clé

C'est le NID d'URN ou le schéma d'URI, qui est utilisé comme portion domaine de l'entrée au DNS. Elle doit être valide selon les procédures spécifiées dans le document d'allocation d'identifiant d'espace de nom de l'URN et dans toute norme future pour l'enregistrement de nouveaux schémas d'URI.

6.2 Autorité

C'est l'individu ou l'organisation (entité) qui a autorité pour enregistrer l'enregistrement. Elle doit être une autorité reconnue comme l'IESG ou toute autorité définie dans les documents du NID de l'URN [RFC2611] ou d'enregistrement du schéma de l'URI [RFC2717].

6.3 Enregistrements

Les enregistrements réels du DNS qui représentent l'ensemble de règles pour la clé. Les valeurs exigées sont Préférence, Ordre, Fanions, Services, Regex, et Remplacement comme défini par la [RFC3404].

7. Gabarit exemple

```
To: register@URN.ARPA
From: joe@foo.com
Key: foo
Authority: Foo Technology, Inc as specified in RFCFOO
Record: foo IN NAPTR 100 100 "" "" "" urn.foo.com.
```

8. Enregistrement d'URN dans la zone URI.ARPA

Comme le présent document discute des zones URI.ARPA et URN.ARPA et de la règle d'URN qui existe dans la zone URI.ARPA, il est normal que le gabarit d'enregistrement pour la règle URN URI soit spécifié ici :

```
To: register@URI.ARPA
From: The IETF URN Working Group
Key: urn
Authority: RFC2141
Record: urn IN NAPTR 0 0 "" "" "" "/^urn:([\^:]+)\|/i" .
```

9. Considérations relatives à l'IANA

L'IANA a créé les zones URN.ARPA et URI.ARPA. La structure hiérarchique des noms, et les seuls noms à allouer dans ces zones, sont les "clés" comme décrit au paragraphe 6.1 du présent document. La gestion administrative et fonctionnelle de ces zones est prise en charge par l'IANA. Les enregistrements du DNS à insérer dans ces zones sont soumis au processus de révision décrit dans ce document.

L'IANA a aussi créé deux listes de discussion, "register@uri.arpa" et "register@urn.arpa", pour les besoins décrits dans ce document. L'IANA gèrera ces listes de diffusion.

10. Considérations pour la sécurité

Les zones "uri.arpa" et "urn.arpa" seront un point d'attaque courant pour les entrées de déni de service et d'usurpation d'identité afin de rediriger les chemins de délégation. Toute entité qui fait fonctionner des serveurs de noms qui contiennent ces zones devrait prendre les mesures appropriées pour sécuriser un composant de niveau infrastructure de l'Internet. Lorsque il deviendra possible à un serveur de noms de signer de façon fiable les enregistrements dans sa zone, il devrait le faire.

11. Remerciements

L'auteur tient à remercier Ron Daniel qui était à l'origine co-auteur de ces documents. L'implication originale de Ron dans les règles de délégation par nature compliquées a rendu possible le DDDS lui-même.

12. Références

- [RFC2048] N. Freed, J. Klensin et J. Postel, "Extensions multi-objets de la messagerie Internet (MIME) Partie 4 : Procédures d'enregistrement", BCP 13, novembre 1996. (*Rendue obsolète par les RFC 4288-89*)
- [RFC2141] R. Moats, "[Syntaxe des URN](#)", mai 1997.
- [RFC2396] T. Berners-Lee, R. Fielding et L. Masinter, "Identifiants de ressource uniformes (URI) : [Syntaxe générique](#)", août 1998. (*Obsolète, voir RFC3986*)
- [RFC2483] M. Mealling et R. Daniel, "Services de [résolution d'URI](#) nécessaires pour la résolution d'URN", janvier 1999.
- [RFC2611] L. Daigle et autres, "Mécanismes de définition d'espace de nom d'URN", juin 1999. (*Obsolète, voir RFC3406*) ([BCP0033](#))
- [RFC2717] R. Petke, I. King, "Procédures d'enregistrement des noms de schéma d'URL", novembre 1999. (*Obsolète, voir RFC4395*) ([BCP0035](#))
- [RFC3401] M. Mealling, "Système de découverte dynamique de délégation (DDDS) Partie I : [DDDS complet](#)", octobre 2002. (*Info.*)
- [RFC3402] M. Mealling, "Système de découverte dynamique de délégation (DDDS) Partie II : [l'algorithme](#)", octobre 2002. (*P.S.*)
- [RFC3403] M. Mealling, "Système de découverte dynamique de délégation (DDDS) Partie III : [base de données](#) du système de noms de domaines (DNS)", octobre 2002. (*P.S.*)
- [RFC3405] M. Mealling, "Système de découverte dynamique de délégation (DDDS) Partie V : [Procédures d'allocation](#) de URI.ARPA", octobre 2002. ([BCP0065](#))

13. Adresse de l'auteur

Michael Mealling
VeriSign
21345 Ridgetop Circle
Sterling, VA 20166
USA
mél : michael@neonym.net
URI : <http://www.verisignlabs.com>

14. Déclaration complète de droits de reproduction

Copyright (C) The Internet Society (2002). Tous droits réservés.

Ce document et les traductions de celui-ci peuvent être copiés et diffusés, et les travaux dérivés qui commentent ou expliquent autrement ou aident à sa mise en œuvre peuvent être préparés, copiés, publiés et distribués, partiellement ou en totalité, sans restriction d'aucune sorte, à condition que l'avis de droits de reproduction ci-dessus et ce paragraphe soit inclus sur toutes ces copies et œuvres dérivées. Toutefois, ce document lui-même ne peut être modifié en aucune façon, par exemple en supprimant le droit d'auteur ou les références à l'Internet Society ou d'autres organisations Internet, sauf si c'est nécessaire à l'élaboration des normes Internet, auquel cas les procédures pour les droits de reproduction définis dans les

processus de normes pour Internet doivent être suivies, ou si nécessaire pour le traduire dans des langues autres que l'anglais.

Les permissions limitées accordées ci-dessus sont perpétuelles et ne seront pas révoquées par la Société Internet ou ses successeurs ou ayants droit.

Ce document et les renseignements qu'il contient sont fournis "TELS QUELS" et L'INTERNET SOCIETY et L'INTERNET ENGINEERING TASK FORCE déclinent toute garantie, expresse ou implicite, y compris mais sans s'y limiter, toute garantie que l'utilisation de l'information ici présente n'enfreindra aucun droit ou aucune garantie implicite de commercialisation ou d'adaptation à un objet particulier.

Remerciement

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