

Groupe de travail Réseau
Request for Comments : 4501
 Catégorie : Sur la voie de la normalisation

S. Josefsson, SJD
 mai 2006
 Traduction Claude Brière de L'Isle

Identifiants de ressource universels dans le système des noms de domaines

Statut du présent mémoire

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

Notice de Copyright

Copyright (C) The Internet Society (2006).

Résumé

Le présent document définit les identifiants de ressource universels pour les ressources du système des noms de domaines.

Table des matières

1. Introduction et fondements.....	1
2. Modèle d'usage.....	2
3. Enregistrement d'URI du DNS.....	2
4. Exemples.....	4
5. Remerciements.....	4
6. Considérations sur la sécurité.....	4
7. Considérations relatives à l'IANA.....	5
8. Conditions de copie.....	5
9. Références.....	5
9.1 Références normatives.....	5
9.2 Références pour information.....	5
Adresse de l'auteur.....	6
Déclaration complète de droits de reproduction.....	6

1. Introduction et fondements

Le système des noms de domaines (DNS, *Domain Name System*) [RFC1034] [RFC1035] est un système largement déployé, utilisé, entre autres choses, pour traduire les noms d'hôtes en adresses IP. Plusieurs protocoles utilisent les identifiants de ressources universels (URI, *Uniform Resource Identifier*) pour se référer aux données. En définissant un schéma d'URI pour les données du DNS, on comble le fossé entre ces deux mondes. Le schéma d'URI DNS défini ici peut être utilisé pour faire référence à toutes données mémorisées dans le DNS.

Les navigateurs peuvent prendre en charge les URI DNS en formant des interrogations au DNS et en rendant les réponses du DNS en utilisant HTML [RFC2854], qui est similaire à ce qui est couramment fait pour les ressources FTP [RFC0959]. Les applications qui ont la capacité de traiter les extensions multi objets de messagerie Internet (MIME, *Multipurpose Internet Mail Extensions*) [RFC2048] peuvent étiqueter les données du DNS restituées en utilisant ce schéma avec les types `text/dns` ou `application/dns` spécifiés dans la [RFC4027].

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. Modèle d'usage

On se référera à la Section 1 de la [RFC3986] pour une discussion en profondeur de la classifications des URI. En particulier, le lecteur est supposé être familiarisé avec la distinction entre "nom" et "localisateur". Cette Section décrit comment le schéma d'URI DNS est destiné à être utilisé et précise les futurs travaux qui pourraient être requis pour utiliser les URI avec le DNS pour certaines applications.

Le schéma d'URI décrit dans le présent document se concentre sur les données mémorisées dans le DNS. À ce titre, il n'y a pas de dispositions pour spécifier les champs du protocole actuel du DNS. Ceci est destiné à ce que l'URI puisse être utilisé même dans des situations où le protocole du DNS n'est pas utilisé directement. Deux exemples pour cela sont les éditeurs de fichiers de zone et les fichiers de configuration en rapport avec le DNS, qui peuvent utiliser ce schéma d'URI pour identifier les données. L'application ne va pas utiliser le protocole DNS pour résoudre les URI.

Une limitation de cette conception est qu'elle ne s'accommode pas de tous les paramètres de protocole au sein du protocole DNS. On s'attend à ce que, pour certaines applications, une syntaxe d'URI plus détaillée qui transpose plus étroitement le protocole DNS puisse être exigée. Cependant, une telle définition d'URI n'est pas incluse dans ce document. Ce document spécifie un URI qui est principalement destiné à désigner les ressources du DNS, mais qui peut aussi être utilisé pour localiser lesdites ressources pour des applications simples, et courantes.

3. Enregistrement d'URI du DNS

Cette Section contient le gabarit d'enregistrement pour le schéma d'URI DNS en accord avec la [RFC2717].

Nom de schéma d'URL : "dns".

Syntaxe de schéma d'URL : un URI DNS désigne un ensemble d'enregistrements de ressource du DNS, référencé par un nom de domaine, une classe, un type, et facultativement, l'autorité. L'URI DNS suit la syntaxe générique de la [RFC3986] et est décrit en utilisant l'ABNF [RFC4234]. Les chaînes ne sont pas sensibles à la casse, et la libre insertion d'espaces blanches linéaires n'est pas permise.

```
dnsurl = "dns:" [ "/" dnsauthority "/" ] dnsname [ "?" dnsquery ]
```

```
dnsauthority = host [ ":" port ]
; voir dans la RFC 3986 la définition de "host" et "port".
```

```
dnsname = *pchar
; voir dans la RFC 3986 la définition de "pchar".
; le champ "dnsname" peut être un nom "relatif" ou "absolu", conformément au paragraphe 3.1 de la RFC 1034.
; Noter de plus qu'une valeur vide de "dnsname" est interprétée comme la racine elle-même. Voir ci-dessous pour les dnsnames relatifs.
```

```
dnsquery = dnsqueryelement [ ";" dnsquery ]
```

```
dnsqueryelement = ( "CLASS=" dnsclassval ) / ( "TYPE=" dnstypeval )
; chaque clause NE DOIT PAS être utilisée plus d'une fois.
```

```
dnsclassval = 1*digit / "IN" / "CH" / <tout mnémonique de classe DNS enregistré par l'IANA>
```

```
dnstypeval = 1*digit / "A" / "NS" / "MD" / <tout mnémonique de type DNS enregistré par l'IANA>
```

Sauf spécifié dans l'URI, l'autorité ("dnsauthority") est supposée être connue localement, la classe ("dnsclassval") être la classe Internet ("IN"), et le type ("dnstypeval") être le type d'adresse ("A"). Ces valeurs par défaut correspondent à l'utilisation normale du DNS : aux adresses de recherche pour les noms d'hôtes.

Un élément dnsquery NE DOIT PAS contenir plus d'une occurrence des champs "CLASS" et "TYPE". Par exemple, "dns:exemple?TYPE=A;TYPE=TXT" et "dns:exemple?TYPE=A;TYPE=A" sont tous deux invalides. Cependant, les champs peuvent apparaître dans n'importe quel ordre, de sorte que "dns:exemple?TYPE=A;CLASS=IN" et "dns:exemple?CLASS=IN;TYPE=A" sont tous deux valides.

La représentation chiffrée des types et classes PEUT être utilisée quand un mnémonique pour la valeur correspondante n'est pas bien connue (par exemple, pour les types ou classes d'introduction récente) mais NE DEVRAIT PAS être utilisée pour les types ou classes définis dans la spécification du DNS [RFC1035]. Toutes les mises en œuvre DOIVENT reconnaître les mnémoniques définis dans la [RFC1035].

Pour éviter des ambiguïtés, les valeurs relatives de "dnsname" (c'est-à-dire, celles qui ne se terminent pas par ".") sont supposées être relatives à la racine. Par exemple, "dns: host.exemple" et "dns:host.exemple." se réfèrent toutes deux au même nom de possesseur, à savoir, "host.exemple.". De plus, une valeur vide de "dnsname" est considérée comme une forme dégénérée d'un nom relatif, qui se réfère à la racine ("").

Pour résoudre un URI DNS en utilisant le protocole DNS [RFC1035], une interrogation est créée qui utilise comme entrée le dnsname, dnsclassval, et dnstypeval provenant de la chaîne d'URI (ou des valeurs par défaut appropriées). Si une autorité ("dnsauthority") est donnée dans la chaîne d'URI, cela indique le serveur qui devrait recevoir l'interrogation au DNS. Autrement, le serveur DNS par défaut devrait la recevoir.

Noter que les URI DNS pourraient être résolus par d'autres protocoles que le DNS, ou en utilisant le protocole DNS d'une façon autre que celle décrite ci-dessus (par exemple, le DNS en diffusion groupée). Les URI DNS n'exigent pas l'utilisation du protocole DNS, mais on s'attend à ce que ce soit l'usage normal. Le paragraphe précédent illustre seulement comment les URI DNS sont résolus en utilisant le protocole DNS.

Un client PEUT vouloir vérifier qu'il comprend les dnsclassval et dnstypeval avant d'envoyer une interrogation, afin qu'il soit capable de comprendre la réponse. Cependant, un exemple typique de client qui n'aurait pas besoin de vérifier la dnsclassval et la dnstypeval serait un mandataire qui va juste traiter la réponse reçue comme des données opaques.

Considérations de codage de caractères : les caractères sont codés conformément à la [RFC3986]. Le protocole DNS ne prend pas en compte les jeux de caractères ; il transporte simplement des données opaques. En particulier, le champ "dnsname" de l'URI DNS est à considérer comme un créneau de nom de domaine ignorant des noms de domaines internationalisés (IDN, *internationalized domain name*) dans la terminologie de la [RFC3490]. Les considérations sur "host" et "port" sont discutées dans la [RFC3986].

Parce que "." est utilisé comme séparateur des étiquettes du DNS, un mécanisme d'échappement est nécessaire pour coder un "." qui fait partie d'une étiquette du DNS. Le mécanisme d'échappement est décrit au paragraphe 5.1 de la [RFC1035]. Par exemple, une étiquette DNS de "exe.mple" peut être esquivée avec "exe\\.mple" ou "exe\046mple". Cependant, la spécification d'URI ne permet pas que le caractère "\" se produise directement dans les URI, de sorte qu'il doit être échappé par "%5c". La seule étiquette DNS "exe.mple" est donc codée comme "exe% 5c.mple". Le même mécanisme peut être utilisé pour coder d'autres caractères, par exemple, "?" et ";". Noter que "." et "%2e" sont équivalents au sein de dnsname et sont interchangeables.

Cette spécification d'URI permet que tous les noms de domaines possibles soient codés, pourvu que les règles de codage de la [RFC3986] soient observées). Cependant, certaines applications peuvent restreindre le jeu des caractères valides. Il faut veiller à ce que dans ces contextes des caractères invalides ne causent pas de dommages. En particulier, les noms d'hôtes dans le DNS ont certaines restrictions. Il appartient à ces applications de limiter ce sous ensemble ; ce schéma d'URI ne pose aucune restriction.

Utilisation prévue : chaque fois qu'il est utile pour les ressources du DNS d'être référencées par des identifiants indépendants du protocole. Souvent, cela survient quand les données sont plus importantes que la méthode d'accès. Comme les logiciels en général s'en sont passés jusqu'ici, il n'est pas prévu que ce soit largement mis en œuvre, ni que les systèmes existants y migrent, mais des solutions spécifiques (en particulier relatives à la sécurité) peuvent trouver cela approprié.

Les applications et/ou protocoles qui utilisent ce schéma incluent les logiciels relatifs à la sécurité, les outils d'administration du DNS, et les paquetages de programmation du réseau.

Considérations d'interopérabilité : les données référencées par ce schéma d'URI peuvent être transférées par des protocoles qui ne connaissent pas les URI (comme le protocole DNS). Il n'est pas prévu que cela ait d'impact d'interopérabilité sérieux.

Des problèmes d'interopérabilité peuvent survenir si une entité comprend un nouveau mnémonique de classe/type du DNS qu'une autre entité ne comprend pas. C'est un problème d'interopérabilité pour le logiciel du DNS en général, bien que cela ne soit pas un problème pratique majeur pour les déploiements actuels du DNS, car les types et classes du DNS sont très statiques. Pour garantir l'interopérabilité, les mises en œuvre peuvent utiliser des entiers pour tous les mnémoniques non définis dans la [RFC1035].

L'interaction avec les étiquettes binaires [RFC2673] ou autres types d'étiquettes étendus n'a pas été encore analysée. Cependant, l'usage des étiquettes binaires est peu fréquent en pratique.

Contact : simon@josefsson.org

Auteur/contrôleur des changements : simon@josefsson.org

4. Exemples

Un URI DNS va suivre la forme générale ci-après qui est destinée à illustrer le schéma, et non à le définir :

```
dns:[//authority/]domain[?CLASS=class;TYPE=type]
```

Illustration d'un URI pour une ressource avec le nom absolu "www.exemple.org.", la classe Internet (IN) et le type d'adresse (A) :

```
dns:www.exemple.org.?clAsS=IN;tYpE=A
```

Comme la classe par défaut est IN et le type par défaut est A, la même ressource peut être identifiée par un URI plus court utilisant un nom relatif :

```
dns:www.exemple.org
```

Illustration d'un URI pour une ressource avec le nom "simon.exemple.org" pour le type CERT dans la classe Internet (IN) :

```
dns:simon.exemple.org?type=CERT
```

Illustration d'un URI pour une ressource avec le nom "ftp.exemple.org", dans la classe Internet (IN) et le type d'adresse (A), mais de l'autorité DNS 192.168.1.1 au lieu de l'autorité par défaut

```
dns://192.168.1.1/ftp.exemple.org?type=A
```

Illustration de diverses techniques d'échappement. Le nom du possesseur serait "world wide web.exemple\domain.org", où le "\" note le caractère "." au titre d'une étiquette, et "." note le séparateur d'étiquettes :

```
dns:world%20wide%20web.example%5c.domain.org?TYPE=TXT
```

Illustration d'une ressource DNS étrange mais valide :

```
dns://fw.exemple.org/*.%20%00.exemple?type=TXT
```

5. Remerciements

Merci à Stuart Cheshire, Donald Eastlake, Pasi Eronen, Bill Fenner, Ted Hardie, Russ Housley, Peter Koch, Andrew Main, Larry Masinter, Michael Mealling, Steve Mattson, Marcos Sanz, Jason Sloderbeck, Paul Vixie, Sam Weiler, et Bert Wijnen de leurs commentaires et suggestions. L'auteur remercie les RSA Laboratories qui ont soutenu le travail qui a conduit au présent document.

6. Considérations sur la sécurité

Si un URI DNS fait référence à des domaines dans l'environnement DNS de l'Internet, l'URI lui-même et les informations référencées par l'URI sont des informations publiques. Si un URI DNS est utilisé au sein d'un environnement DNS "interne", l'URI DNS et les données référencées devraient être traités en utilisant les mêmes considérations que celles qui s'appliquent aux données dans l'environnement "interne".

Si les informations référencées par des URI DNS sont utilisées pour prendre des décisions de sécurité (de telles données incluent sans s'y limiter des certificats mémorisés dans le DNS [RFC2538]) les mises en œuvre peuvent devoir employer des techniques de sécurité comme le DNS sécurisé [RFC4033], CMS [RFC3852], ou OpenPGP [RFC2440], pour protéger les données durant le transport. La façon de le mettre en œuvre va dépendre du scénario d'usage, et il n'appartient pas à ce schéma d'URI de définir comment les données référencées par les URI DNS devraient être protégées.

Si les applications acceptent des valeurs inconnues de dnsqueryelement dans un URI (par exemple, l'URI "dns:www.exemple.org?secret=value") sans savoir ce que signifie le "secret=value" dnsqueryelement, un canal couvert utilisé pour faire "fuir" les informations peut être activé. Les implications de canaux couverts devraient être comprises par les applications qui acceptent des valeurs de dnsqueryelement inconnues.

De légères variations, comme la différence entre des majuscules et des minuscules dans le champ dnsname, peuvent être utilisées comme canal couvert pour faire fuiter des informations.

7. Considérations relatives à l'IANA

L'IANA a enregistré le schéma d'URI DNS, en utilisant le gabarit de la Section 3, conformément à la [RFC2717].

8. Conditions de copie

Copyright (c) 2000, 2001, 2002, 2003, 2004, 2005, 2006 Simon Josefsson

Concernant ce document entier ou toute portion de celui-ci, l'auteur ne donne aucune garantie et n'est pas responsable de tout dommage résultant de son utilisation. L'auteur accorde la permission irrévocable à tous de l'utiliser, le modifier et le distribuer de toutes façons qui ne diminuent pas les droits de tous autres de l'utiliser, le modifier, et le distribuer, pourvu que les travaux dérivés redistribués ne contiennent pas d'informations trompeuses sur l'auteur ou la version. Les travaux dérivés n'ont pas besoin d'être licenciés sous des termes similaires.

9. Références

9.1 Références normatives

[RFC1034] P. Mockapetris, "Noms de domaines - [Concepts et facilités](#)", STD 13, novembre 1987. (MàJ par [RFC1101](#), [1183](#), [1348](#), [1876](#), [1982](#), [2065](#), [2181](#), [2308](#), [2535](#), [4033](#), [4034](#), [4035](#), [4343](#), [4035](#), [4592](#), [5936](#), [8020](#), [8482](#), [8767](#))

[RFC1035] P. Mockapetris, "Noms de domaines - [Mise en œuvre](#) et spécification", STD 13, novembre 1987. (MàJ par [RFC1101](#), [1183](#), [1348](#), [1876](#), [1982](#), [1995](#), [1996](#), [2065](#), [2136](#), [2181](#), [2137](#), [2308](#), [2535](#), [2673](#), [2845](#), [3425](#), [3658](#), [4033](#), [4034](#), [4035](#), [4343](#), [5936](#), [5966](#), [6604](#), [7766](#), [8482](#), [8767](#))

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

[RFC3986] T. Berners-Lee, R. Fielding et L. Masinter, "[Identifiant de ressource uniforme](#) (URI) : Syntaxe générique", STD 66, janvier 2005. (P.S. ; MàJ par [RFC8820](#))

[RFC4234] D. Crocker et P. Overell, "[BNF augmenté pour les spécifications de syntaxe](#) : ABNF", octobre 2005. (Remplace [RFC2234](#), remplacée par [RFC5234](#))

9.2 Références pour information

[RFC0959] J. Postel et J. Reynolds, "Protocole de [transfert de fichiers](#) (FTP)", STD 9, octobre 1985. (MàJ par [RFC7151](#))

- [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 [4288-4289](#)*)
- [RFC2440] J. Callas, L. Donnerhackle, H. Finney et R. Thayer, "[Format de message OpenPGP](#)", novembre 1998. (*Obs. voir [4880](#)*)
- [RFC2538] D. Eastlake 3rd, O. Gudmundsson, "Mémorisation des certificats dans le système des noms de domaines (DNS)", mars 1999. (*Obsolète, voir [RFC4398](#)*) (P.S.)
- [RFC2673] M. Crawford, "[Étiquettes binaires dans le système des noms de domaine](#)", août 1999. (*Remplacée par [RFC6891](#)*)
- [RFC2717] R. Petke, I. King, "Procédures d'enregistrement des noms de schéma d'URL", novembre 1999. (*Obsolète, voir [RFC4395](#)*) ([BCP0035](#))
- [RFC2854] D. Connelly et L. Masinter, "Type de support 'text/html'", juin 2000. (*Information*)
- [RFC3490] P. Faltstrom et autres, "Internationalisation des noms de domaine dans les applications (IDNA)", mars 2003. (*Remplacée par les RFC [5890](#) et [5891](#), P.S.*)
- [RFC3852] R. Housley, "Syntaxe de message cryptographique (CMS)", juillet 2004. (*Obsolète, voir la RFC [5652](#)*)
- [RFC4027] S. Josefsson, "Types de support du système de noms de domaines", avril 2005. (*Information*)
- [RFC4033] R. Arends, et autres, "Introduction et [exigences pour la sécurité du DNS](#)", mars 2005.

Adresse de l'auteur

Simon Josefsson
SJD

mél : simon@josefsson.org

Déclaration complète de droits de reproduction

Copyright (C) The IETF Trust (2006).

Le présent document est soumis aux droits, licences et restrictions contenus dans le BCP 78, et à www.rfc-editor.org, et sauf pour ce qui est mentionné ci-après, les auteurs conservent tous leurs droits.

Le présent document et les informations contenues sont fournis sur une base "EN L'ÉTAT" et le contributeur, l'organisation qu'il ou elle représente ou qui le/la finance (s'il en est), la INTERNET SOCIETY et la INTERNET ENGINEERING TASK FORCE déclinent toutes garanties, exprimées ou implicites, y compris mais non limitées à toute garantie que l'utilisation des informations encloses ne viole aucun droit ou aucune garantie implicite de commercialisation ou d'aptitude à un objet particulier.

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.

Remerciement

Le financement de la fonction d'édition des RFC est fourni par l'activité de soutien administratif (IASA) de l'IETF.