Groupe de travail Réseau
Request for Comments : 4095
Catégorie : Sur la voie de la normalisation
Traduction Claude Brière de L'Isle

C. Malamud, Memory Palace Press

mai 2005

Découvrir la signification des mots clés de classe de sollicitation

Statut de ce 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 "Normes officielles des protocoles de l'Internet" (STD 1) pour connaître l'état de la 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 (2005).

Résumé
Le présent document propose un mécanisme pour trouver un URI associé à un mot-clé de classe de sollicitation, qui est défini dans la RFC 3865, l'extension de service SMTP "Pas de sollicitation" *(No Soliciting)*. Les mots-clés de classe "Solicitation" sont de simples étiquettes consistant en un nom de domaine qui a été inversé, comme "org.example.adv". Ces mots-clés de classe de sollicitation sont insérés dans des champs d'en-tête choisis ou utilisés dans l'extension de service ESMTP, incluant un nouvel en-tête "No-Solicit:", qui peut contenir un ou plusieurs mots-clés de classe de sollicitation insérés par l'envoyeur.

Le présent document spécifie une application fondée sur le système de découverte de délégation dynamique (DDDS, *Dynamic Delegation Discovery System*) décrit dans la [RFC3401] et les documents qui s'y rapportent. Un algorithme est spécifié pour associer un mot clé de classe de sollicitation à un URI qui contient plus d'informations sur la signification et l'usage de ce mot-clé de classe de sollicitation. Par exemple, celui qui enregistre le domaine "example.org" pourrait utiliser ce mécanisme pour créer un URI contenant des informations détaillées sur le mot-clé de classe de sollicitation "org.example.adv".

Table des Matières

1. Mots clés de classe de sollicitation

La [RFC3865] définit le concept d'un "mot-clé de classe de sollicitation", qui est une chaîne ou étiquette arbitraire qui peut être associée à un message électronique et transportée par le service de messagerie ESMTP comme défini dans la [RFC2821] et les documents qui s'y rapportent. Les mots-clés de classe de sollicitation sont formatés comme des noms de domaines, mais inversés. Par exemple, l'administrateur de zone de "example.com" pourrait spécifier un mot-clé de classe de sollicitation particulier tel que "com.example.adv" qui pourrait être inséré dans un en-tête "No-Solicit:" par l'envoyeur d'un message ou dans un champ de trace par un agent de transfert de message (MTA, *message transfer agent*). Ce mot-clé de classe de sollicitation est inséré par l'envoyeur du message, qui peut aussi insérer divers autres mots-clés de classe de sollicitation comme défini par l'envoyeur ou d'autres parties.

La [RFC3865] place explicitement la découverte de la signification d'un mot-clé de classe de sollicitation en dehors du domaine d'application de l'extension au service de base ESMTP. Pour les besoins du transport de message, ces mots-clés de classe de sollicitation sont opaques. Cependant, si la RFC 3865 devient largement utilisée, un message électronique pourrait contenir un grand nombre de mots-clés de classe de sollicitation. L'en-tête "No-Solicit:" a des mots-clés insérés par l'envoyeur du message, qui peut inclure les propres mots-clés de l'envoyeur, ainsi que ceux rendus obligatoires par des autorités réglementaires ou recommandés par des associations industrielles volontaires. De même, les champs de trace "received:" peuvent contenir un grand nombre de mots-clés produits par les agents de transfert de message, un logiciel de filtrage, un logiciel de transmission dans l'agent d'utilisateur de message (MUA, *message user agent*), ou tout autre système dans la chaîne de livraison.

Avec la croissance du nombre de mots-clés employés, il va être important de trouver une méthode pour découvrir la signification des divers mots-clés de classe de sollicitation. Le présent document spécifie ce mécanisme, associant un mot-clé de classe de sollicitation à un URI qui contient plus d'informations en utilisant l'enregistrement de ressource *(RR)* NAPTR du DNS, qui est défini dans la [RFC3403]. Un but explicite de conception est de garder le système aussi simple que possible. Des approches comme celles définissant une structure fondée sur XML qui contiendrait des métadonnées spécifiques sur le mot-clé de classe de sollicitation ou d'autres approches qui définissent le format de l'explication ont été écartées. Le but est plutôt simplement d'associer un mot-clé de classe de sollicitation à un URI, qui à son tour contient une explication du mot-clé.

1.1 Terminologie

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. Application NAPTR No-Solicit

Le cadre de DDDS de la [RFC3401] et les documents qui s'y rapportent fournissent un ensemble puissant de mécanismes qui peuvent donner des applications sophistiquées telles que ENUM, spécifié dans la [RFC3761]. Il y a une simplification du cadre de DDDS appelée l'application NAPTR directe (S-NAPTR, *Straightforward-NAPTR*) qui est spécifiée dans la [RFC3958]. Malheureusement, S-NAPTR ne permet pas l'utilisation du fanion "U" pour les recherches terminales et ne prend pas en charge le champ d'expression régulière du RR NAPTR. Comme un champ de remplacement dans un enregistrement NAPTR doit contenir seulement un nom de domaine, et que notre but est de trouver un URI, le présent document n'utilise pas le mécanisme S-NAPTR.

Le présent document utilise le RR NAPTR pour faire une seule recherche à partir du mot-clé de classe de sollicitation en URI. Le caractère "." est d'abord substitué à toute instance du caractère ":" et ensuite le mot-clé de classe de sollicitation est inversé, en utilisant le caractère "." comme délimiteur. Cela devient la clé de la recherche de nom de domaine. Par exemple, "org.example:ADV" devient "ADV.example.org".

Note sur les noms de domaines : la RFC3865 déclare qu'un mot-clé de classe de sollicitation consiste en un nom de domaine valide suivi du caractère ":" et des caractères valides supplémentaires. Plusieurs points importants sont à rappeler pour la mise en œuvre. Comme les noms de domaines sont insensibles à la casse et que le caractère ":" est traduit en caractère ".", pour les besoins de cette application DDDS, les mots-clés de classe de sollicitation suivants sont syntaxiquement équivalents : "com.example:ADV", "com.Example:adv", et "com:example:ADV". De plus, il est important de se rappeler que la chaîne résultante doit satisfaire aux autres vérifications de validité du DNS. En particulier, les étiquettes de domaines sont limitées à une longueur de 63 caractères et la longueur totale de la chaîne résultante doit être inférieure à 253 caractères. Tous les caractères non ASCII doivent être codés en utilisant les spécifications des noms de domaines internationalisés (IDN, *Internationalized Domain Names*) de la [RFC3490] et des documents en rapport. Noter que des caractères non ASCII peuvent aussi être codés après le caractère ":".

Les champs du RR NAPTR sont utilisés comme suit :

- Les champs "ORDER" et "PREFERENCE" doivent être traités comme spécifié dans la [RFC3403] : si plusieurs enregistrements sont retournés, celui ou ceux avec la plus faible valeur de "ORDER" qui ont un champ "SERVICE" qui correspond DOIVENT être utilisés. De ceux qui ont la plus faible valeur de ORDER, ceux qui ont la plus faible valeur de "PREFERENCE" DEVRAIENT être utilisés.
- Le champ "FLAGS" DOIT contenir le caractère "U".
- Le champ "SERVICES" DOIT contenir seulement la chaîne "no-solicit".
- Le champ "REGEXP" DOIT contenir un URI valide comme spécifié plus loin .
- Le champ "REPLACEMENT" DOIT être vide.

Le champ "REGEXP" est défini dans la [RFC3402] comme consistant en un caractère de délimitation *(delim-character)*, une expression régulière étendue POSIX, un autre caractère de délimitation, une valeur de remplacement, et un caractère de délimitation final. Pour la présente application, on applique les règles suivantes :

- Le caractère de délimitation PEUT être tout caractère valide comme défini au paragraphe 3.2 de la [RFC3402].
- L'expression étendue régulière DOIT être vide.
- La valeur de remplacement DOIT contenir un URI valide comme spécifié dans la [RFC3986].
- La valeur de remplacement DEVRAIT contenir un URI limité aux schémas "ftp", "http", et "https" comme spécifié dans les [RFC3986] et [RFC2660].
- Le document restitué par l'URI DEVRAIT se conformer à [HTML-4.01], incluant les lignes directrices d'accessibilité qui y sont contenues.

3. Exemple

Dans cet exemple, un ensemble d'enregistrements NAPTR est ajouté à la zone "example.com" et peut être restitué en utilisant "dig" ou d'autres utilitaires du DNS :

```
[carl@example.com]% dig 2795.example.com naptr

  ; <<>> DiG 9.2.3 <<>> 2795.example.com naptr
  ;; global options:  printcmd
  ;; Got answer:
  ;; ->>HEADER<<- opcode: QUERY,
     status: NOERROR, id: 43494
  ;; flags: qr aa rd ra; QUERY: 1, ANSWER: 5,
     AUTHORITY: 2, ADDITIONAL: 1

  ;; QUESTION SECTION:
  ;2795.example.com.            IN      NAPTR

  ;; ANSWER SECTION:
  2795.example.com.       86400   IN
      NAPTR   1 1 "U" "iam+invalid"
      "!!http://invalid.example.com/contact.html!" .
  2795.example.com.       86400   IN
      NAPTR   1 1 "U" "sip+invalid"
      "!!http://invalid.example.com/contact.html!" .
  2795.example.com.       86400   IN
      NAPTR   1 2 "U" "no-solicit"
      "!!http://infinite.example.com/keywordinfo.html!" .
  2795.example.com.       86400   IN
      NAPTR   2 1 "U" "no-solicit"
      "!!http://infinite.example.com/keywordinfo.html!" .
  2795.example.com.       86400   IN
      NAPTR   1 1 "U" "no-solicit"
      "!!http://infinite.example.com/keywordinfo.html!" .
```

Un simple utilitaire écrit en PERL accepte une clé de recherche et retourne un URI en utilisant les spécifications du présent document. Cet exemple est seulement à des fins d'illustration :

```
  #!/usr/bin/perl

# Cet échantillon de code n'est pas normatif

# Ce programme accepte un mot-clé de classe de sollicitation et retourne un URI en cas de succès. Il s'arrête en douceur en cas d'échec.
  use strict;

# http://www.net-dns.org/
  use Net::DNS;
```

```
# inverser l'étiquette pour créer un nom de domaine
  $ARGV[0] =~ tr/:/./ ;
  my $target = join( ".", reverse( split( /\./, $ARGV[0] ) ) );

# crée un résolveur.
  my $res = Net::DNS::Resolver->new;

# trouve tous les enregistrements naptr.
  my $query = $res->query( "$target", "NAPTR" ) || exit ;

# Faire ici ses vérifications DNSSEC, éliminer tous les RR invalides.

# Obtenir les réponses, éliminer les services qui ne correspondent pas, triés par ordre, préference.
  my @rr =
    sort {
# Trier les enregistrements par ordre numérique, préférence.
      $a->order <=> $b->order
        || $a->preference <=> $b->preference
    }
    grep { $_->service =~ /no-solicit/ } $query->answer;

# Imprimer le premier enregistrement qualifié, éliminer les marqueurs regexp.
  my $op = substr( my $answer = $rr[0]->regexp , 0, 1 )
    || exit ;
  print split ( $op, $answer ) ; exit ;
```

Le fonctionnement de l'échantillon de code donne les résultats suivants :

```
  [carl@example.com]% lynx -source `./discover.pl com.example.2795`
  <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
  <html>
    <head>
      <title>About Our Mot-clé de classe de sollicitation</title>
    </head>
    <body>
      <center>
        <a href="monkey.mp3">
          <img alt="bouncy monkey logo"
              src="images/monkey_fpo.gif" border="0" />
          <br />
        </a>
        <br />
        Sur com.example.2795:<br />
        Il a été déterminé que le contenu de ce message<br />
        est conforme à l'esprit de la RFC 2795.
        Félicitations ?
      </center>
    </body>
  </html>
```

4. Spécification d'application DDDS

Les définitions suivantes s'appliquent à la présente application :

- Chaîne unique d'application : la chaîne unique d'application est un mot-clé de classe de sollicitation comme défini dans la [RFC3865].
- Première règle bien connue : le caractère "." est substitué au caractère ":" et ensuite le mot-clé de classe de sollicitation est inversé afin de produire un nom de domaine valide. Par exemple, "com.example:adv" va devenir "adv.example.com".
- Des bases de données valides : le DNS est la base de données.
- Résultat attendu : un URI.

o Le champ "SERVICE" DOIT contenir la chaîne "no-solicit", le champ "FLAGS" DOIT contenir la chaîne "U", le champ "REPLACEMENT" DOIT être vide, et le champ "REGEXP" DOIT être formaté comme spécifié à la Section 2.

Les caractères génériques *(wildcards)* sont appropriés pour cette application, permettant que plusieurs mots-clés de classe de sollicitation qui partagent un préfixe commun pointent tous sur le même URI. Noter que l'enregistrement de ressource NAPTR est connu comme RR de "sous typage", ce qui signifie que des sélecteurs supplémentaires sont disponibles au sein du RR pour passer les choix au crible. Cela signifie que plus d'enregistrements sont retournés qu'il n'est en réalité nécessaire, d'où résulte plus de trafic.

Mais, cela signifie aussi que les caractères génériques peuvent avoir l'effet inattendu que plusieurs types d'enregistrement de ressource NAPTR sont utilisés. Les développeurs et les administrateurs de zone devraient être prudents lors de l'utilisation de tels caractères génériques dans cette application.

5. Remerciements

L'auteur tient à remercier les personnes suivantes de leurs utiles suggestions et relectures du présent document : Leslie Daigle, Spencer Dawkins, Arnt Gulbrandsen, Ted Hardie, Scott Hollenbeck, Russ Housley, David Kessens, Peter Koch, Michael Mealling, Pekka Savola, Mark Townsley, et Margaret Wasserman.

6. Considérations sur la sécurité

Ce document spécifie une application qui dépend du système des noms de domaines pour associer un mot-clé de classe de sollicitation à un URI. Quatre considérations sur la sécurité sont soulevées par cette application :

1. Si la recherche de nom de domaine a été compromise, l'application peut retourner un URI avec des indications incorrectes sur l'utilisation d'un mot-clé de classe de sollicitation particulier. En particulier, si l'application retourne un URI avec le schéma "https:" et si les extensions de sécurité du DNS telles que définies dans la [RFC4033] et les documents en rapport ne sont pas utilisées, l'utilisateur va avoir une illusion non garantie d'authenticité rendant la possibilité d'attaques actives un problème sérieux. Même si les extensions de sécurité du DNS et les schéma "https:" sont tous deux utilisés, le client aura besoin de prendre des mesures supplémentaires pour s'assurer que les deux contextes différents de validation de signature numérique sont administrés par le même possesseur de domaine.

2. La RFC 3865 fonde les mots-clés de classe de sollicitation sur les noms de domaines. Cependant, elle ne définit pas à qui un utilisateur devrait faire confiance. Un envoyeur ou un MTA intermédiaire pourrait insérer un mot-clé de classe de sollicitation dans un message et ensuite utiliser l'application définie dans ce document pour tromper le receveur du message. Par exemple, un vendeur en ligne malveillant pourrait insérer un mot-clé du genre "org.example.certified.message" et utiliser un URI pour indiquer d'une certaine façon (à tort) que le message aurait un statut officiel. Comme avec tout URI, les utilisateurs doivent prendre des mesures qui sortent du domaine d'application de la présente spécification pour déterminer quoi et qui croire.

3. Les noms de domaines ne sont pas des identifiants permanents. Comme avec toute application qui utilise les noms de domaines, incluant la Toile mondiale, si un nom de domaine ou un URI est incorporé dans un message électronique, il y a une possibilité qu'à l'avenir le nom de domaine soit contrôlé par un administrateur de zone différent et que l'utilisation de l'application décrite dans ce document donne avec le temps un résultat différent et éventuellement discordant.

4. Un envoyeur malveillant pourrait insérer un grand nombre de mots-clés de classe de sollicitation ou des mots-clés de sollicitation formatés de façon impropre, effectuant ainsi une attaque de déni de service sur les ressources du receveur par l'utilisation d'un nombre excessif de recherches dans le DNS. Si un tel message est envoyé à un grand nombre de receveurs, il peut en résulter une attaque de déni de service contre le fournisseur à un URI particulier (par exemple, un grand nombre de demandes tentant d'accéder à un URI comme "http://example.net/index.html"). Des mots-clefs de classe de sollicitation formatés de façon impropre, en particulier ceux avec un domaine de niveau supérieur ou de second niveau inexistant, pourraient résulter en une attaque de déni de service sur les fournisseurs de registre du DNS ou les serveurs racine du DNS.

7. Considérations relatives à l'IANA

Il n'y a pas de registre central tenu par l'IANA des valeurs qui pourraient apparaître dans le champ "SERVICE" d'un enregistrement de ressource NAPTR. Donc, aucune action directe de l'IANA n'est requise.

Cependant, l'IANA tient bien un registre des étiquettes de service d'application qui est utilisé pour prendre en charge l'application DDDS S-NAPTR définie dans la [RFC3958]. Il est indiqué à l'IANA que la valeur "no-solicit" pour le champ SERVICE est utilisée selon le présent document et ne devrait donc pas être utilisée dans le registre des étiquettes de service d'application pour d'autres applications.

8. Références

8.1 Références normatives

[HTML-4.01] Raggett, D., Hors, A., and I. Jacobs, "HTML 4.01 Specification", W3C REC REC-html401-19991224, décembre 1999.

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

[RFC2660] E. Rescorla, A. Schiffman, "Protocole de transfert HyperText sécurisé", août 1999. *(Expérimentale)*

[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.)*

[RFC3865] C. Malamud, "Extension de service Pas de démarchage du protocole simple de transfert de messagerie (SMTP)", septembre 2004. *(P.S.)*

[RFC3958] L. Daigle, A. Newton, "Localisation de service d'application fondée sur le domaine avec les enregistrements de ressource de SRV et le service de recherche dynamique de délégation (DDDS)", janvier 2005. *(P.S.)*

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

8.1 Références pour information

[RFC2795] S. Christey, "Suite de protocole du singe infini (IMPS)", 1er avril 2000. *(Information)*

[RFC2821] J. Klensin, éditeur, "Protocole simple de transfert de messagerie", STD 10, avril 2001. *(Obsolète, voir* RFC5321)

[RFC3401] M. Mealling, "Système de découverte dynamique de délégation (DDDS) Partie I : DDDS complet", octobre 2002. *(Info.)*

[RFC3490] P. Faltstrom et autres, "Internationalisation des noms de domaine dans les applications (IDNA)", mars 2003. (*Remplacée par les* RFC5890 et 5891, *P.S.*)

[RFC3761] P. Faltstrom, M. Mealling, "Application de E.164 au système de découverte dynamique de délégation (DDDS) d'identifiants de ressource uniformes (URI) (ENUM)", avril 2004. *(P.S.) (Obsolète, voir la* RFC6116)

[RFC4033] R. Arends, et autres, "Introduction et exigences pour la sécurité du DNS", mars 2005.

Adresse de l'auteur

Carl Malamud
Memory Palace Press
PO Box 300
Sixes, OR 97476
US
mél : carl@media.org

Déclaration complète de droits de reproduction

Copyright (C) The Internet Society (2005).

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 fournies 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 ci encloses ne violent 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 pourraient 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 actuellement fourni par la Internet Society.