Groupe de travail Réseau
Request for Comments : 4701
Catégorie : Sur la voie de la normalisation
Traduction Claude Brière de L'Isle

M. Stapp, Cisco Systems
T. Lemon, Nominum
A. Gustafsson, Araneus Information Systems
octobre 2006

Enregistrement de ressource du DNS pour le codages d'informations du protocole de configuration dynamique d'hôte (RR DHCID)

Résumé
Il est possible aux clients du protocole de configuration dynamique d'hôte (DHCP, *Dynamic Host Configuration Protocol*) de tenter de mettre à jour le même nom de domaine pleinement qualifié (FQDN, *Fully Qualified Domain Name*) du DNS ou de metttre à jour un FQDN DNS qui a été ajouté au DNS pour un autre objet que d'obtenir un prêt DHCP. Que le serveur DHCP ou les clients eux-mêmes effectuent les mises à jour du DNS, des conflits peuvent survenir. Pour résoudre de tels conflits, la RFC 4703 propose de mémoriser les identifiants de client dans le DNS pour ôter les ambiguïtés associées aux noms de domaines avec les clients DHCP auxquels ils se réfèrent. Le présent mémoire définit à cette fin un type d'enregistrement de ressource (RR, *Resource Record*) distinct à utiliser par les clients et serveurs DHCP : le RR "DHCID".

Table des matières

1. Introduction

Un ensemble de procédures pour permettre aux clients et serveurs DHCP [RFC2131], [RFC3315] de mettre à jour automatiquement le DNS ([RFC1034], [RFC1035]) est proposé dans la [RFC4703].

Des conflits peuvent survenir si plusieurs clients DHCP souhaitent utiliser le même nom DNS ou si un client DHCP tente d'utiliser un nom ajouté dans un autre dessein. Pour résoudre de tels conflits, la [RFC4703] propose de mémoriser les identifiants de client dans le DNS pour associer sans ambiguïté les noms de domaines aux clients DHCP qui les utilisent.

Pour être clair, il est préférable que ces informations DHCP utilisent un type de RR distinct. Le présent mémoire définit à cette fin un RR distinct pour l'usage de clients ou serveurs DHCP : le RR "DHCID".

Afin d'obscurcir les informations d'identification de clients potentiellement sensibles, les données mémorisées sont le résultat d'un calcul de hachage unidirectionnel SHA-256. Le hachage inclut les informations provenant du message du client DHCP ainsi que le nom de domaine lui-même, afin que les données mémorisées dans le RR DHCID dépendent à la fois de l'identification du client utilisée dans l'interaction de protocole DHCP et du nom de domaine. Cela signifie que les RDATA DHCID vont varier si un seul client est associé au fil du temps à plus d'un nom. Cela rend difficile le "traçage" d'un client lorsque il est associé à divers noms de domaines.

2. 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].

3. RR DHCID

Le RR DHCID est défini avec le mnémonique DHCID et le code de type 49. Le RR DHCID est seulement défini dans la classe IN. Les RR DHCID ne causent pas de traitement de section supplémentaire.

3.1 Format de RDATA DHCID

La section RDATA d'un RR DHCID en transmission contient RDLENGTH octets de données binaires. Le format de ces données et son interprétation par les serveurs et clients DHCP sont décrits ci-dessous.

Le logiciel DNS devrait considérer la section RDATA comme opaque. Les clients ou serveurs DHCP utilisent le RR DHCID pour associer l'identité d'un client DHCP à un nom DNS, afin que plusieurs clients et serveurs DHCP puissent effectuer de façon déterministe les mises à jour du DNS de la même zone. Du point de vue de celui qui met à jour, le RDATA d'enregistrement de ressource DHCID consiste en un type d'identifiant de deux octets, dans l'ordre des octets du réseau, suivis par un octet de type de résumé, suivi par un ou plusieurs octets représentant l'identifiant réel :

< 2 octets > Code de type d'identifiant
< 1 octet > Code de type de résumé
< n octets > Résumé (la longueur dépend du type de résumé)

3.2 Format de présentation de DHCID

Dans les fichiers maîtres du DNS, les RDATA sont représentées comme un seul bloc codé en base-64 identique à celui utilisé pour représenter les données binaires à la Section 3 de la [RFC3548]. Les données peuvent être divisées en un nombre quelconque de sous chaînes séparées par des espaces, jusqu'à un seul chiffre en base-64, qui sont enchaînées pour former les RDATA complètes. Ces sous chaînes peuvent s'étendre sur plusieurs lignes en utilisant les parenthèses standard.

3.3 Codes de type d'identifiant du RR DHCID

Le code de type de l'identifiant de RR DHCID spécifie quelles données provenant de la demande du client DHCP ont été utilisées comme entrée dans la fonction de hachage. Les codes de type d'identifiant sont définis dans un registre tenu par l'IANA, comme spécifié à la Section 7. La liste initiale des valeurs allouées pour les code de type d'identifiant et l'identifiant de ce type est :

Code de type d'identifiant	Identifiant
0x0000	"htype" de un octet suivi par "hlen" octets de "chaddr" provenant de la DHCPREQUEST [RFC2131] du client DHCPv4.
0x0001	Octets de données (c'est-à-dire, les champs Type et Identifiant de client) provenant de l'option Identifiant de client [RFC2132] du client DHCPv4.

0x0002	DUID du client (c'est-à-dire, les octets de données de l'option Identifiant de client d'un client DHCPv6 [RFC3315] ou le champ DUID provenant de l'option Identifiant de client d'un client DHCPv4[RFC4361).
0x0003 – 0xfffe	Indéfini ; disponible pour être alloué par l'IANA.
0xffff	Indéfini ; réservé.

3.4 Code de type de résumé de RR DHCID

Le code de type de résumé du RR DHCID est un identifiant pour l'algorithme de résumé utilisé. Le résumé est calculé sur un identifiant et le FQDN canonique comme décrit au paragraphe suivant.

Les codes de type de résumé sont définis dans un registre tenu par l'IANA, comme spécifié à la Section 7. La liste initiale des valeurs allouées pour les codes de type de résumé est : la valeur 0 est réservée, et la valeur 1 est SHA-256. Réserver d'autres types exige une action de normalisation de l'IETF. Définir de nouvelles valeurs va aussi exiger une action de normalisation de l'IETF pour documenter comment ceux qui mettent à jour le DNS traitent plusieurs types de résumé.

3.5 Calcul des RDATA

Les RDATA DHCID sont formées par l'enchaînement des deux octets du code de type d'identifiant avec les données de longueur variable.

Les RDATA pour tous les codes de type autres que 0xffff, qui est réservé pour une future expansion, sont formées par l'enchaînement des deux octets de code de type d'identifiant, du code de type de résumé de un octet, et de la valeur du résumé (32 octets pour SHA-256).

< type d'identifiant > < type de résumé > < résumé >

L'entrée à la fonction de hachage de résumé est définie comme étant :

résumé = SHA-256(< identifiant > < FQDN >)

Le FQDN est représenté dans la mémoire tampon dans le format canonique du réseau comme décrit dans la [RFC4034], paragraphe 6.2. Le code de type d'identifiant et l'identifiant sont en relation comme spécifié au paragraphe 3.3 : le code de type d'identifiant décrit la source de l'identifiant.

Une mise à jour DHCPv4 utilise le code de type 0x0002 si une option Identifiant de client est présente dans les messages DHCPv4 et elle est codée comme spécifié dans la [RFC4361. Autrement, la mise à jour utilise 0x0001 si une option Identifiant de client est présente, et 0x0000 si elle ne l'est pas.

Une mise à jour DHCPv6 utilise toujours le code de type 0x0002.

3.5.1 Utilisation du DUID du client

Quand la mise à jour utilise le DUID du client (à partir d'une option Identifiant de client DHCPv6 ou d'une portion de l'option Identifiant de client DHCPv4 comme spécifiée dans la [RFC4361), les deux premiers octets du RR DHCID DOIVENT être 0x0002, dans l'ordre des octets de réseau. Le troisième octet est le code de type de résumé (1 pour SHA-256). Le reste du RR DHCID DOIT contenir le résultat du calcul du hachage SHA-256 sur les octets du DUID suivis par le FQDN.

3.5.2 Utilisation de l'option Identifiant de client

Quand la mise à jour utilise l'option Identifiant de client DHCPv4 envoyée par le client dans son message DHCPREQUEST, les deux premiers octets du RR DHCID DOIVENT être 0x0001, dans l'ordre des octets du réseau. Le troisième octet est le code de type de résumé (1 pour SHA-256). Le reste du RR DHCID DOIT contenir le résultat du calcul du hachage SHA-256 sur les octets de données (c'est-à-dire, les champs Type et Identifiant de client) de l'option, suivis par le FQDN.

3.5.3 Utilisation du htype et chaddr du client

Quand la mise à jour utilise l'adresse de couche de liaison du client comme identifiant, les deux premiers octets des RDATA DHCID DOIVENT être des zéros. Le troisième octet est le code de type de résumé (1 pour SHA-256). Pour générer le reste de l'enregistrement de ressource, la mise à jour calcule un hachage unidirectionnel utilisant l'algorithme SHA-256 à travers une mémoire tampon contenant le type de matériel réseau du client, son adresse de couche de liaison, et les données du FQDN. Précisément, le premier octet de la mémoire tampon contient le type de matériel réseau comme il apparaît dans le champ 'htype' DHCP du message DHCPREQUEST du client. Tous les octets significatifs du champ 'chaddr' dans le message DHCPREQUEST du client suivent, dans le même ordre où les octets apparaissent dans le message DHCPREQUEST. Le nombre d'octets significatifs dans le champ 'chaddr' est spécifié dans le champ 'hlen' du message DHCPREQUEST. Les données du FQDN, comme spécifié ci-dessus, suivent.

3.6 Exemples

3.6.1 Exemple 1

Un serveur DHCP alloue l'adresse IPv6 2001:DB8::1234:5678 à un client qui a inclus les donnés d'option Identifiant de client DHCPv6 00:01: 00:06:41:2d:f1:66:01:02:03:04:05:06 dans sa demande DHCPv6. Le serveur met à jour le nom "chi6.exemple.com" au nom du client et utilise les données d'option Identifiant de client DHCP comme entrée pour former un RR DHCID. Les RDATA DHCID sont formées en réglant les deux octets de type à la valeur 0x0002, l'octet de type de résumé à 1 pour SHA-256, et en effectuant un calcul de hachage SHA-256 sur une mémoire tampon contenant les 14 octets provenant de l'option Identifiant de client et le FQDN (représenté comme spécifié au paragraphe 3.5).

```
chi6.exemple.com.    AAAA    2001:DB8::1234:5678
chi6.exemple.com.    DHCID   ( AAIBY2/AuCccgoJbsaxcQc9TUapptP69lOjxfNuVAA2kjEA= )
```

Si le type de RR DHCID n'est pas pris en charge, les RDATA vont être codées [RFC3597] comme :

```
\# 35 ( 000201636fc0b8271c82825bb1ac5c41cf5351aa69b4febd94e8f17cdb95000da48c40 )
```

3.6.2 Exemple 2

Un serveur DHCP alloue l'adresse IPv4 192.0.2.2 à un client qui a inclus les données d'option d'identifiant de client DHCP 01:07:08:09:0a:0b:0c dans sa demande DHCP. Le serveur met à jour le nom "chi.exemple.com" au nom du client et utilise les données d'option Identifiant de client DHCP comme entrée pour former un RR DHCID. Les RDATA DHCID sont formées en réglant les deux octets de type à la valeur 0x0001, l'octet de type de résumé à 1 pour SHA-256, et en effectuant un calcul de SHA-256 sur une mémoire tampon contenant les sept octets provenant de l'option Identifiant de client et le FQDN (représenté comme spécifié au paragraphe 3.5).

```
chi.exemple.com.     A       192.0.2.2
chi.exemple.com.     DHCID   ( AAEBOSD+XR3Os/0LozeXVqcNc7FwCfQdWL3b/NaiUDlW2No= )
```

Si le type de RR DHCID n'est pas pris en charge, les RDATA vont être codées [RFC3597] comme :

```
\# 35 ( 0001013920fe5d1dceb3fd0ba3379756a70d73b17009f41d58bddbfcd6a2503956d8da )
```

3.6.3 Exemple 3

Un serveur DHCP alloue l'adresse IPv4 192.0.2.3 à un client avec l'adresse Ethernet MAC 01:02:03:04:05:06 en utilisant le nom de domaine "client.exemple.com" et utilise l'adresse de couche de liaison du client pour identifier le client. Les RDARA DHCID sont composées en réglant les deux octets de type à zéro, l'octet de type de résumé à 1 pour SHA-256, et en effectuant un calcul de SHA-256 sur une mémoire tampon contenant la valeur de un octet de 'htype' pour Ethernet, 0x01, suivie par les six octets de l'adresse MAC Ethernet, et le nom de domaine (représenté comme spécifié au paragraphe 3.5).

```
client.exemple.com.  A       192.0.2.3
client.exemple.com.  DHCID   ( AAABxLmlskllE0MVjd57zHcWmEH3pCQ6VytcKD//7es/deY= )
```

Si le type de RR DHCID n'est pas pris en charge, les RDATA vont être codées [RFC3597] comme :

```
\# 35 ( 000001c4b9a5b249651343158dde7bcc77169841f7a4243a572b5c283fffedeb3f75e6 )
```

4. Utilisation du RR DHCID

Ce RR NE DOIT PAS être utilisé pour tout autre objet que détaillé dans la [RFC4703]. Bien que ce RR contienne des données qui sont opaques aux serveurs du DNS, les données doivent être cohérentes sur toutes les entités qui mettent à jour et interprètent cet enregistrement. Donc, les nouveaux formats de données peuvent seulement être définis pas des actions du groupe de travail DHC, par suite d'une révision de la [RFC4703].

5. Comportement de celui qui met à jour

Les données dans le RR DHCID permettent aux mises à jour de déterminer si plus d'un client DHCP désire utiliser un FQDN particulier. Cela permet aux administrateurs de site d'établir leur politique de mises à jour du DNS. Le RR DHCID n'établit pas lui-même de politique.

Les mises à jour utilisent des données provenant de la demande d'un client DHCP et du nom de domaine que le client désire utiliser pour calculer le hachage de l'identité du client, et ensuite comparer ce hachage aux données dans les RR DHCID sur le nom qu'elles souhaitent associer à l'adresse IP du client. Si une mise à jour découvre des RR DHCID dont les RDATA ne correspondent pas à l'identité du client qu'elle a calculé, la mise à jour DEVRAIT en conclure qu'un client différent est actuellement associé au nom en question. La mise à jour DEVRAIT alors procéder conformément à la politique administrative du site. Cette politique pourrait imposer le choix d'un nom différent, ou elle pourrait permettre que la mise à jour se continue.

6. Considérations de sécurité

L'enregistrement DHCID n'introduit par lui-même aucun nouveau problème de sécurité pour le DNS. Afin d'obscurcir les informations d'identité du client, un hachage unidirectionnel est utilisé. De plus, afin de rendre difficile de 'tracer' un client en examinant les noms associés à une valeur de hachage particulière, le FQDN est inclus dans le calcul du hachage. Donc, les RDATA dépendent à la fois des données d'identification de client DHCP et de chaque FQDN associé au client.

Cependant, on devrait noter qu'un attaquant qui a des connaissances, en particulier des adresses MAC couramment utilisées dans les données d'identification de client DHCP, peut être capable de découvrir l'identité du client DHCP en utilisant une attaque en force brute. Même sans connaissances supplémentaires, le nombre de bits inconnus utilisés pour calculer le hachage est normalement seulement de 48 à 80 bits.

Les administrateurs devraient se soucier de permettre des mises à jour non sécurisées des zones du DNS, qu'elles soient ou non exposées sur l'Internet mondial. Les clients et serveurs DHCP DEVRAIENT utiliser une forme d'authentification de mise à jour (par exemple, de la [RFC2845]) quand ils effectuent des mises à jour du DNS.

7. Considérations relatives à l'IANA

L'IANA a alloué un numéro de type de RR du DNS pour l'enregistrement de type DHCID.

La présente spécification définit un nouvel espace de numéros pour les codes de type d'identifiant de deux octets associés au RR DHCID. L'IANA a établi un registre des valeurs pour cet espace de numéros. Trois valeurs initiales sont allouées au paragraphe 3.3, et la valeur de 0xFFFF est réservée pour une utilisation future. Les nouveaux codes de type d'identifiant de RR DHCID sont alloués par action de normalisation, comme défini dans la [RFC2434].

La présente spécification définit un nouvel espace de numéros pour les codes de type de résumé d'un octet associés au RR DHCID. L'IANA a établi un registre des valeurs pour cet espace de numéros. Deux valeurs initiales sont allouées au paragraphe 3.4. Les nouveaux codes de type de résumé de RR DHCID sont alloués par action de normalisation, comme défini dans la [RFC2434].

8. Remerciements

Tous nos remerciements à Harald Alvestrand, Ralph Droms, Olafur Gudmundsson, Sam Hartman, Josh Littlefield, Pekka Savola, et tout particulièrement à Bernie Volz pour leur relecture et leurs suggestions.

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)

[RFC2434] T. Narten et H. Alvestrand, "Lignes directrices pour la rédaction d'une section Considérations relatives à l'IANA dans les RFC", BCP 26, octobre 1998. *(Rendue obsolète par la* RFC5226)

[RFC4361] T. Lemon, B. Sommerfeld, "Identifiants de client spécifique de nœud pour le protocole de configuration dynamique d'hôte version 4 (DHCPv4)", février 2006. (*MàJ* RFC2131, RFC2132, RFC3315) *(P.S.)*

[RFC4703] M. Stapp, B. Volz, "Résolution des conflits de nom de domaine pleinement qualifié (FQDN) entre clients du protocole de configuration dynamique d'hôte (DHCP)", octobre 2006. *(P.S.)*

9.2 Références pour information

[RFC2131] R. Droms, "Protocole de configuration dynamique d'hôte", mars 1997. *(DS) (Mà J par* RFC3396, RFC4361, RFC5494, et RFC6849)

[RFC2132] S. Alexander et R. Droms, "Options DHCP et Extensions de fabricant BOOTP", mars 1997.

[RFC2845] P. Vixie et autres, "Authentification de transaction de clé secrète pour DNS (TSIG)", mai 20000 (*MàJ par* RFC3645 *; remplacée par* RFC8945 *; P.S.)*

[RFC3315] R. Droms, J. Bound, B. Volz, T. Lemon, C. Perkins et M. Carney, "Protocole de configuration dynamique d'hôte pour IPv6 (DHCPv6)", juillet 2003. (*MàJ par* RFC6422 et RFC6644, RFC7227 *; rendue obsolète par* RFC8415)

[RFC3548] S. Josefsson, "Codages de données Base16, Base32, et Base64", juillet 2003. *(Obsolète, voir* 4648) *(Info)*

[RFC3597] A. Gustafsson, "Traitement des types inconnus d'enregistrement de ressource du DNS ", septembre 2003. *(P.S.)*

[RFC4034] R. Arends et autres, "Enregistrements de ressources pour les extensions de sécurité au DNS", mars 2005.

Adresses des auteurs

Mark Stapp
Cisco Systems, Inc.
1414 Massachusetts Ave.

Ted Lemon
Nominum, Inc.
950 Charter St.

Andreas Gustafsson
Araneus Information Systems Oy
Ulappakatu 1

Boxborough, MA 01719
USA
téléphone : 978.936.1535
mél : mjs@cisco.com

Redwood City, CA 94063
USA
mél : mellon@nominum.com

02320 Espoo
Finland
mél : gson@araneus.fi

Déclaration complète de droits de reproduction

Remerciement
Le financement de la fonction d'édition des RFC est actuellement assuré par l'activité de soutient administratif de l'IETF (IASA).