Groupe de travail RéseauHamilton & Wright
Request for Comments : 2219
BCP 17
Catégorie : Bonnes practiques actuelles

M. Hamilton, Loughborough University
R. Wright, Lawrence Berkeley Laboratory
octobre 1997
Traduction Claude Brière de L'Isle

Utilisation d'alias du DNS pour les services réseau

Résumé
Il est devenu de pratique courante d'utiliser des noms symboliques (habituellement des CNAME) dans le service des noms de domaines (DNS, *Domain Name Service*) [RFC1034], [RFC1035], pour se référer aux services réseau tels que les serveurs FTP anonyme [RFC0959], les serveurs Gopher [RFC1436], et plus précisément les serveurs HTTP de la Toile [RFC1945]. Ceci est souhaitable pour un certain nombre de raisons. Cela donne un moyen de déplacer des services d'une machine à une autre de façon transparente, et un mécanisme grâce auquel les gens ou les agents peuvent découvrir avec un programme qu'une organisation gère, par exemple, un serveur de la Toile.

Bien que cette approche ait été adoptée presque de façon universelle, il n'y a pas de document de normalisation ou spécification similaire pour ces noms d'utilisation courante. Le présent document cherche à rectifier cette situation en rassemblant le "folklore" existant sur les conventions de dénomination, et propose un mécanisme pour s'accommoder des nouveaux protocoles.

Il est important de noter que ces conventions de dénomination ne fournissent pas une solution complète à long terme au problème de trouver un service réseau particulier pour un site. Des efforts sont faits dans d'autres groupes de travail de l'IETF pour trouver une solution à long terme à ce problème, comme le travail sur les enregistrements de ressource de localisation de serveur (DNS SRV) de la [RFC2052].

1. Motifs

Lorsque on veut localiser les services réseau offerts sur un domaine Internet particulier, on se trouve en face d'un choix à faire à partir d'un nombre croissant de bases de données centralisées – normalement des "outils de recherche" de la Toile ou de Usenet News, ou de tenter d'inférer l'existence de services réseau à partir de toute information du DNS qui se trouve disponible. La première approche n'est pas praticable dans certains cas, notamment lorsque l'entité qui recherche les informations de service est un programme.

Peut-être que l'exemple opérationnel le plus visible de la dernière approche est le cas des serveurs http de la Toile Mondiale. Il est de pratique courante d'essayer de mettre en préfixe au nom de domaine d'une organisation "http://www." afin d'atteindre son site de la Toile Mondiale, par exemple, en prenant "hivnet.fr" pour arriver à "http://www.hivnet.fr." Certains navigateurs populaires de la Toile Mondiale sont allés jusqu'à prendre en charge automatiquement cette expansion du nom de domaine.

Idéalement, le DNS ou quelque service d'annuaire complémentaire pourrait fournir un moyen pour que les programmes déterminent automatiquement les services réseau qui sont offerts à un domaine Internet particulier, les protocoles qui sont utilisés pour les livrer, et d'autres informations techniques. Malheureusement, bien que beaucoup de travail ait été fait pour développer de telles technologies de services d'annuaire et définir de nouveaux types d'enregistrements de ressources du DNS pour fournir ce type d'informations, il n'y a pas à ce problème de solution largement déployée ou faisant l'objet d'un consensus général — excepté dans un petit nombre de cas.

Le premier cas est lorsque le DNS fournit déjà une capacité de recherche pour le type d'informations recherchées. Par exemple, les enregistrements d'échangeur de messagerie (MX, *Mail Exchanger*) spécifient comment devrait être acheminée la messagerie sur un domaine particulier [RFC0974], les enregistrements de début d'autorité (SOA, *Start of Authority*) rendent possible de déterminer qui est responsable d'un certain domaine, et les enregistrements de serveur de nom (NS, *Name Server*) indiquent quel hôte fournit le service des noms du DNS pour un domaine donné.

Le second cas est lorsque le DNS ne fournit pas une capacité de recherche appropriée, mais qu'il y a une convention largement acceptée pour trouver cette information. Il a été fait un certain usage des enregistrements Text (TXT) [RFC1035] dans ce scénario, mais dans la vaste majorité des cas, on utilise un nom canonique (CNAME, *Canonical Name*) ou un

pointeur d'enregistrement d'adresse (A, *Address*) pour indiquer le ou les hôtes qui fournissent le service. Le présent document propose une légère formalisation de cette approche bien connue des alias.

On devrait noter que le DNS fournit une capacité de recherche de services bien connus (WKS, *Well Known Services*) [RFC1035] qui rend possible de déterminer les services réseau offerts sur un certain nom de domaine. En pratique, il n'est pas très utilisé, peut-être à cause de l'absence d'une interface de programmation convenable. L'usage de WKS pour l'acheminement de la messagerie a été déconseillé dans la spécification des exigences pour les hôtes [RFC1123] en faveur de l'enregistrement MX, et à long terme, il est concevable que les enregistrements SRV vont supplanter les enregistrements à la fois WKS et MX.

2. Cadre générique

Notre approche du traitement des alias pour les protocoles est directe. On définit un ensemble standard d'alias du DNS pour les services réseau les plus courants qui existent actuellement (voir le paragraphe sur les "Cas particuliers" ci-dessous). Pour les protocoles qui ne sont pas explicitement énumérés dans ce document, la spécification du protocole doit proposer un nom.

3. Cas particuliers

Alias	**Service**
archie	archie [ARCHIE]
finger	Finger [RFC1288]
ftp	File Transfer Protocol [RFC0959]
gopher	Internet Gopher Protocol [RFC1436]
ldap	Lightweight Directory Access Protocol [RFC1777]
mail	SMTP mail [RFC0821]
news	Usenet News via NNTP [RFC0977]
ntp	Network Time Protocol [RFC1305]
ph	CCSO nameserver [PH]
pop	Post Office Protocol [RFC1939]
rwhois	Referral WHOIS [RFC1714]
wais	Wide Area Information Server [RFC1625]
whois	NICNAME/WHOIS [RFC0954]
www	World-Wide Web HTTP [RFC1945]

4. (Ab)us du DNS comme service d'annuaire

L'utilisation généralisée de ces alias courants signifie effectivement qu'il est parfois possible de "deviner" les noms de domaines associés aux services réseau d'une organisation, bien que cela devienne plus difficile au fur et à mesure qu'augmente le nombre des organisations enregistrées dans le DNS.

Les utilisateurs doivent comprendre que l'existence d'une entrée du DNS telle que www.hivnet.fr ne constitue pas un enregistrement d'un service de la Toile Mondiale. Il n'est nulle part exigé qu'un nom de domaine se résolve en une ou des adresses IP. Il n'est pas non plus exigé qu'un hôte écoute les connexions HTTP, ou s'il le fait, que le serveur HTTP fonctionne sur l'accès 80. Finalement, même si tout cela est vrai, il ne peut y avoir aucune garantie que le serveur de la Toile Mondiale soit prêt à honorer les demandes provenant de clients arbitraires.

Ceci étant dit, les alias fournissent bien des "indications" utiles sur les services offerts. Nous proposons qu'ils soient vus dans cet esprit.

Les conventions décrites dans le présent document ne sont, essentiellement, utiles que lorsque le nom de domaine d'une organisation peut être déterminé — par exemple, à partir d'une base de données externe. Un certain nombre de groupes, y compris l'IETF, ont travaillé sur les moyens de trouver les noms de domaines à partir d'un ensemble d'informations telles qu'un nom d'organisation, une localisation, et un type d'activité. On espère que l'un ou l'autre va finalement rendre possible d'augmenter le service de recherches de base que fournit le DNS d'une capacité plus générale de recherche et de restitution.

5. Configuration de serveur du DNS

À court terme, bien que soient développés la technologie des services d'annuaire et d'autres types d'enregistrements de ressource du DNS, les administrateurs de noms de domaines sont encouragés à utiliser des noms communs pour les services réseau qu'ils gèrent. Il rendront plus facile aux personnes de l'extérieur de trouver des informations sur leur organisation, et rendront aussi plus facile le déplacement des services d'une machine à l'autre.

Il y a deux approches conventionnelles à la création de ces entrées du DNS. L'une est d'ajouter un seul enregistrement CNAME à la configuration de votre serveur DNS, par exemple "ph.hivnet.fr. IN CNAME baby.hivnet.fr".

Noter que dans ce scénario, aucune information sur ph.hivnet.fr ne devrait exister dans le DNS à part l'enregistrement CNAME. Par exemple, ph.hivnet.fr pourrait ne pas contenir un enregistrement MX.

Une autre approche serait de créer un enregistrement A pour chaque adresse IP associée à "ph.hivnet.fr", par exemple, "ph.hivnet.fr. IN A 194.167.157.2".

Ce n'est pas une chose simple que de recommander de faire des CNAME sur des enregistrements A. Chaque site a son propre ensemble d'exigences qui peut rendre une approche meilleure que l'autre. La [RFC1912] expose certaines des questions de configuration impliquées par l'utilisation des CNAME.

De récentes mises en œuvre du DNS fournissent une caractéristique de "round-robin" qui provoque le retour des adresses IP de l'hôte dans un ordre différent chaque fois qu'une recherche est faite sur l'adresse.

Il commence à apparaître des clients réseau qui, lorsque ils rencontrent un hôte avec plusieurs adresses, utilisent une heuristique pour déterminer l'adresse à contacter — par exemple, de prendre celle qui a le plus court délai d'aller-retour. Donc, si un serveur a des miroirs (est dupliqué) sur un certain nombre de localisations, il peut être souhaitable de faire la liste des adresses IP des serveurs miroirs comme enregistrements A sur le serveur principal. Ceci ne sera vraisemblablement approprié que si les serveurs miroirs sont les copies exactes du serveur d'origine.

6. Limitations de cette approche

Certains services exigent qu'un client ait plus d'informations que le simple nom de domaine du serveur. Par exemple, un client LDAP a besoin de connaître un point de départ de recherche au sein de l'arborescence du répertoire d'informations afin d'avoir un dialogue significatif avec le serveur. Le présent document n'essaye pas de résoudre ce problème.

7. Nom de service CCSO

Il y a actuellement au moins trois alias différents en usage courant pour le serveur de noms CCSO — par exemple "ph", "cso" et "ns". Il semble qu'il serait dans l'intérêt de tous de rétrécir le choix des alias à un seul nom. "ns" semblerait être le meilleur choix car c'est le nom le plus couramment utilisé. Cependant, "ns" est aussi utilisé par le DNS pour pointer sur le serveur DNS. En fait, l'usage prévalent de "ns" est pour designer les serveurs du DNS. Pour cette raison, on suggère l'utilisation de "ph" comme meilleur nom à utiliser pour les serveurs de noms CCSO.

Les sites qui ont des serveurs CCSO existants qui utilisent certains de ces alias peuvent estimer souhaitable de les utiliser tous les trois. Cela augmente la probabilité de trouver le service.

Comme on l'a note plus haut, les mises en œuvre devraient être résilientes pour le cas où le nom ne pointe pas sur le service attendu.

8. Considérations pour la sécurité

Le DNS est ouvert à de nombreuses sortes d'attaques "d'usurpation d'identité", et il ne peut être garanti que le résultat retourné par une recherché du DNS est bien sûr l'information authentique. L'usurpation d'identité peut prendre la forme d'un déni de service, comme de diriger le client sur une adresse non existante, ou une attaque passive telle qu'un serveur d'un intrus qui se fait passer pour le serveur légitime.

Des travaux sont en cours pour remédier à cette situation dans la mesure où le DNS est concerné [RFC2065]. Pendant ce temps là, on notera que les plus forts mécanismes d'authentification comme ceux de cryptographie à clé publique avec de grandes tailles de clé sont un pré requis si le DNS est utilisé dans des situations sensibles. Des exemples en seraient les transactions financières en ligne, et toute situation où la confidentialité est en jeu — comme l'interrogation d'un fichier médical sur le réseau. On peut aussi conseiller un chiffrement fort du trafic réseau, pour protéger contre la capture d'une connexion TCP et le "reniflage" des paquets.

9. Conclusions

Les noms de service énumérés dans le présent document fournissent en ensemble significatif de valeurs par défaut qui peuvent servir d'aide pour déterminer les hôtes qui offrent des services particuliers pour un certain nom de domaine.

Le présent document a noté des exceptions qui, soit ne conviennent pas, par nature, à ce traitement, soit ont déjà une base installée substantielle qui utilise d'autres alias.

10. Remerciements

Merci à Jeff Allen, Tom Gillman, Renato Iannella, Thomas Lenggenhager, Bill Manning, Andy Powell, Sri Sataluri, Patrik Faltstrom, Paul Vixie et Greg Woods pour leurs commentaires sur les versions préparatoires au présent document.

Le présent travail a été soutenu par la dotation 12/39/01de UK Electronic Libraries Programme (eLib), par la dotation RE 1004 du programme pour la recherche télématique de la Commission européenne, et par le contrat numéro DE-AC03-76SF00098 du Ministère de l'Énergie des U.S.A.

11. Références

Les documents des demandes de commentaires (RFC, *Request For Comments*) sont disponibles à <URL:ftp://ftp.internic.net/rfc> et sur de nombreux autres sites miroirs.

[ARCHIE] A. Emtage, P. Deutsch. "archie - An Electronic Directory Service for the Internet", Winter Usenix Conference Proceedings 1992. Pages 93-110.

[PH] R. Hedberg, S. Dorner, P. Pomes, "The CCSO Nameserver (Ph) Architecture", Non publié.

[RFC0768] J. Postel, "Protocole de datagramme d'utilisateur (UDP)", (STD 6), 28 août 1980.

[RFC0793] J. Postel (éd.), "Protocole de commande de transmission – Spécification du protocole du programme Internet DARPA", STD 7, septembre 1981.

[RFC0821] J. Postel, "Protocole simple de transfert de messagerie", STD 10, août 1982.

[RFC0954] K. Harrenstien, M. Stahl, E. Feinler, "NICNAME/Qui-est-qui", octobre 1985. *(Rendue obsolète par 3912)*

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

[RFC0974] C. Partridge, "L'acheminement de la messagerie et le système des domaines", janvier 1986. *(obsolète, voir la RFC 2821)*

[RFC0977] B. Kantor et P. Lapsley, "Protocole de transfert des nouvelles du réseau", février 1986. *(Obsolète, voir RFC3977)*

[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.

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

[RFC1288] D. Zimmerman, "Protocole d'information d'utilisateur de Finger", décembre 1992.

[RFC1305] D. Mills, "Protocole de l'heure du réseau, version 3, spécification, mise en œuvre et analyse", STD 12, mars 1992. *(Remplacée par RFC5905)*

[RFC1436] F. Anklesaria, M. Cahill, P. Lindner, D. Johnson, D. Torrey et B. Albert, "Protocole Gopher Internet (un protocole de recherche et restitution de documents répartis)", mars 1993. *(Information)*

[RFC1590] J. Postel, "Procédures d'enregistrement des types de support" mars 1994. *(Info., remplacée par les RFC2045-49)*

[RFC1625] St. Pierre et autres, "WAIS sur Z39.50-1988", juin 1994. *(Information)*

[RFC1700] J. Reynolds et J. Postel, "Numéros alloués", STD 2, octobre 1994. *(Historique, voir www.iana.org)*

[RFC1714] S. Williamson, M. Kosters, "Protocole de référence Qui est qui (RWhois)", novembre 1994. *(rempl. par 2167)*

[RFC1777] W. Yeong, T. Howes, S. Kille, "Protocole léger d'accès de répertoire", mars 1995. *(Obsolète, voir* RFC3494) *(Historique)*

[RFC1912] D. Barr, "Erreurs opérationnelles et de configuration courantes sur le DNS", février 1996. *(Information)*

[RFC1939] J. Myers, M. Rose, "Protocole Post Office - version 3", mai 1996. (*MàJ par* RFC1957, RFC2449) (STD0053)

[RFC1945] T. Berners-Lee, R. Fielding, H. Frystyk, "Protocole de transfert Hypertext -- HTTP/1.0", mai 1996. *(Information)*

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

[RFC2065] D. Eastlake 3rd, C. Kaufman, "Extensions de sécurité du système de noms de domaines", janvier 1997. (*Obsolète, voir* RFC2535) (MàJ RFC1034, RFC1035) *(P.S.)*

12. Adresse des auteurs

Martin Hamilton
Department of Computer Studies
Loughborough University of Technology
Leics. LE11 3TU, UK
mél : m.t.hamilton@lut.ac.uk

Russ Wright
Information & Computing Sciences Division
Lawrence Berkeley National Laboratory
1 Cyclotron Road, Berkeley
Mail-Stop: 50A-3111
CA 94720, USA
mél : wright@lbl.gov