Groupe de travail Réseau
Request for Comments : 2782
RFC rendue obsolète : 2052
Catégorie : En cours de normalisation
Traduction Claude Brière de L'Isle

A. Gulbrandsen, Troll Technologies
P. Vixie, Internet Software Consortium
L. Esibov, Microsoft Corp.
février 2000

RR du DNS pour spécifier la localisation des services (DNS SRV)

Statut du présent Mémo

La présente RFC spécifie un protocole de normalisation pour la communauté Internet et appelle à des discussions et suggestions pour son amélioration. Prière de se reporter à l'édition en cours des "Internet Official Protocol Standards" (*normes officielles du protocole Internet*) (STD 1) pour connaître l'état de la normalisation et le statut du présent protocole. La distribution du présent mémo n'est pas soumise à restriction.

Résumé

Le présent document décrit un enregistrement de ressource du DNS qui spécifie la localisation du ou des serveurs pour un protocole et domaine spécifiques.

Généralités et motivations

Actuellement, on doit soit connaître l'adresse exacte d'un serveur à contacter, soit diffuser une question.

Le RR SRV permet aux administrateurs d'utiliser plusieurs serveurs pour un seul domaine, de déplacer des services d'un hôte à un autre avec le minimum de confusion, et de désigner certains hôtes comme serveurs principaux pour un service et les autres comme sauvegarde.

Les clients demandent un service/protocole spécifique pour un domaine spécifique (le mot domaine est utilisé ici dans le strict sens de la RFC 1034), et reçoivent en retour les noms de tous les serveurs disponibles.

Noter que lorsque le présent document se réfère à des "enregistrements d'adresse", il signifie des RR A, des RR AAAA, ou leurs équivalents les plus modernes.

Définitions

Les mots clés "DOIT", "NE DOIT PAS", "DEVRAIT", "NE DEVRAIT PAS" et "PEUT" utilisés dans le présent document sont à interpréter comme spécifié dans [BCP 14]. Les autres termes utilisés dans le présent document sont définis dans la spécification du DNS, la RFC 1034.

Déclaration d'applicabilité

En général, il est prévu que les enregistrements SRV seront utilisés par les clients pour des applications où la spécification de protocole pertinente indique que les clients devraient utiliser l'enregistrement SRV. Une telle spécification DOIT définir le nom symbolique à utiliser dans le champ Service de l'enregistrement SRV, comme décrit ci-dessous. Elle DOIT aussi inclure des considérations pour la sécurité. Les enregistrements SRV de Service NE DEVRAIENT PAS être utilisés en l'absence d'une telle spécification.

Exemple introductif

Si un client LDAP à capacité SRV veut découvrir un serveur LDAP qui prend en charge le protocole TCP et fournit le service LDAP pour le domaine example.com., il fait une recherche sur

```
_ldap._tcp.example.com
```

comme décrit dans [ARM]. Le fichier de la zone d'exemple vers la fin du présent mémoire contient des RR de réponse à une interrogation SRV.

Note : LDAP est choisi comme exemple pour les seuls besoins d'illustration, et les exemples de LDAP utilisés dans le présent document ne devraient pas être considérés comme une déclaration péremptoire sur la façon recommandée d'utiliser LDAP avec les enregistrements SRV. Comme décrit plus haut au paragraphe de déclaration d'applicabilité, consulter les

documents LDAP appropriés pour connaître la procédure recommandée.

Format de l'enregistrement de ressource SRV

Voici le format du SRV RR, dont le code de type DNS est 33 :

_Service._Proto.Nom TTL Classe SRV Priorité Poids Port Cible

(Il y a un exemple vers la fin de ce document.)

Service
Nom symbolique du service désiré, comme défini dans les Numéros alloués [STD 2] ou localement. Un souligné (_) est ajouté devant l'identifiant de service pour éviter les collisions avec les étiquettes DNS qui surviennent dans l'environnement. Certains services largement utilisés, notamment POP, n'ont pas un seul nom universel. Si les Numéros alloués désignent le service indiqué, ce nom est le seul nom légal pour les recherches de SRV. Le Service est insensible à la casse.

Proto
Nom symbolique du protocole désiré, avec un souligné (_) ajouté devant pour éviter les collisions avec les étiquettes du DNS qui surviennent dans l'environnement. _TCP et _UDP sont à présent les valeurs les plus utiles pour ce champ, bien qu'on puisse utiliser tout nom défini par les Numéros alloués ou localement (comme pour Service). Le Proto est insensible à la casse.

Nom
C'est le domaine auquel se réfère ce RR. Le RR SRV est unique en ce que le nom qu'on recherche n'est pas ce nom ; l'exemple en fin de document montre cela clairement.

TTL
Signification standard du DNS de la [RFC 1035] *(durée de vie)*.

Classe
Signification standard du DNS de la [RFC 1035]. Les enregistrements SRV surviennent dans la classe IN.

Priorité
C'est la priorité de cet hôte cible. Un client DOIT essayer de contacter l'hôte cible ayant la priorité de plus faible numéro qu'il peut atteindre ; les hôtes cibles avec la même priorité DEVRAIENT être essayés dans un ordre défini par le champ Poids. La gamme est de 0 à 65 535. C'est un entier non signé de 16 bits dans l'ordre des octets du réseau.

Poids
Mécanisme de sélection de serveur. Le champ Poids spécifie une pondération relative pour les entrées qui ont la même priorité. Les plus gros poids DEVRAIENT être donnés à une probabilité de choix proportionnellement plus élevée. La gamme de ce nombre est de 0 à 65 535. C'est un entier de 16 bits non signé dans l'ordre des octets du réseau. Les administrateurs de domaine DEVRAIENT utiliser le poids 0 lorsqu'il n'y a aucun choix de serveur à faire, pour rendre la lecture du RR plus facile pour l'homme (moins bruyante). En présence d'enregistrements qui contiennent des poids supérieurs à 0, les enregistrements ayant des poids de 0 devraient avoir une très faible probabilité de choix.

En l'absence d'un protocole dont la spécification appelle à l'utilisation d'autres informations de pondération, un client arrange les RR SRV de la même Priorité dans l'ordre dans lequel les hôtes cible, spécifiés par les RR SRV, seront contactés. L'algorithme suivant DEVRAIT être utilisé pour ordonner les RR SRV de la même priorité :

Pour choisir la prochaine cible à contacter, arranger tous les RR SRV (qui n'ont pas encore été ordonnés) dans n'importe quel ordre, sauf que tous ceux qui sont de poids 0 sont placés au commencement de la liste.

Calculer la somme des poids de ces RR, et à chaque RR, associer la somme courante dans l'ordre choisi. Puis choisir un nombre aléatoire uniforme entre 0 et la somme calculée (incluse), et choisir le RR dont la valeur de somme courante est la première dans l'ordre choisi qui est supérieure ou égale au nombre aléatoire choisi. L'hôte cible spécifié dans le RR SRV choisi est le prochain que le client contactera. Retirer ce RR SRV de l'ensemble des RR SRV non ordonnés et appliquer l'algorithme décrit aux RR SRV non ordonnés pour choisir le prochain hôte cible. Continuer le processus de rangement jusqu'à ce qu'il n'y ait plus de RR SRV non ordonné. Ce processus est répété pour chaque Priorité.

Port
C'est l'accès sur l'hôte cible de ce service. La gamme est de 0 à 65 535. C'est un entier de 16 bits non signé dans l'ordre des octets du réseau. C'est souvent celui qui est spécifié dans les Numéros alloués, mais pas nécessairement.

Cible
C'est le nom de domaine de l'hôte cible. Il DOIT y avoir un ou plusieurs enregistrements d'adresse pour ce nom, le nom NE DOIT PAS être un alias (au sens de la RFC 1034 ou de la RFC 2181). Les développeurs sont invités, sans que ce soit obligatoire, à retourner le ou les enregistrements d'adresse dans la section Données supplémentaires. Sauf si cela devenait autorisé par de futures actions de normalisation, et jusqu'à ce que cela le devienne, la compression de nom n'est pas permise pour ce champ.

Une cible de "." signifie que le service est délibérément indisponible sur ce domaine.

Avis aux administrateurs de domaine

Espérer que chacun va mettre à jour ses applications client lorsque le premier serveur publiera un RR de SRV est futile (même si ce serait souhaitable). Donc SRV aura à coexister avec des recherches d'enregistrement d'adresse pour les protocoles existants, et les administrateurs du DNS devraient essayer de fournir les enregistrements d'adresse pour prendre en charge les vieux clients :

- Lorsque les services pour un seul domaine sont étalés sur plusieurs hôtes, il semble recommandable d'avoir une liste des enregistrements d'adresse sur le même nœud DNS que le RR SRV, avec une liste raisonnable (mais peut-être sous optimale) des hôtes de secours pour Telnet, NNTP et les autres protocoles qui seront vraisemblablement utilisés avec ce nom. Noter que certains programmes essayent seulement la première adresse qu'ils obtiennent par exemple de . gethostbyname(), et on ne sait pas si ce comportement est très répandu.

- Lorsque un service est fourni par plusieurs hôtes, on peut fournir les enregistrements d'adresse pour tous les hôtes (auquel cas le mécanisme de round-robin, lorsqu'il est disponible, va partager également la charge) ou juste pour un (vraisemblablement le plus rapide).

- Si un hôte est destiné à fournir un service seulement lorsque le ou les serveurs principaux sont en panne, il ne devrait probablement pas figurer sur la liste des enregistrements d'adresse.

- Les hôtes qui sont référencés par des enregistrements d'adresse de sauvegarde doivent utiliser le numéro d'accès spécifié dans les Numéros alloués pour le service.

- Les concepteurs de protocoles futurs pour lesquels des "serveurs secondaires" ne sont pas utiles (ou significatifs) peuvent choisir de ne pas utiliser la prise en charge de SRV pour les serveurs secondaires. Les clients pour de tels protocoles peuvent utiliser ou ignorer les RR SRV avec une Priorité supérieure à celle du RR de la plus basse Priorité pour un domaine.

Il y a actuellement une limite pratique de 512 octets aux réponses du DNS. Jusqu'à ce que tous les résolveurs puissent traiter de plus grandes réponses, il est vivement conseillé aux administrateurs de domaines de conserver leurs réponses SRV en dessous de 512 octets.

Tous les chiffres ronds sont faux écrivait le Dr. Johnson, et ces chiffres sont très ronds : un paquet de réponse a un en-tête de 30 octet plus le nom du service ("_ldap._tcp.example.com" par exemple) ; chaque RR de SRV ajoute 20 octets en plus du nom de l'hôte cible ; chaque RR NS dans la section NS a 15 octets en plus du nom de l'hôte serveur ; et finalement, chaque RR A dans la section de données supplémentaires fait 20 octets environ, et il y a des A pour chaque RR SRV et NS RR mentionné dans la réponse. Cette estimation de taille est extrêmement approximative, mais ne devrait pas sous estimer de beaucoup la taille réelle de la réponse. Si une réponse peut être proche de la limite, l'utilisation d'un outil d'interrogation du DNS (par exemple, "dig") pour chercher la réponse réelle est une bonne idée.

Le champ "Poids"

Poids, le champ de choix du serveur, n'est pas entièrement satisfaisant, mais la charge réelle sur les serveurs normaux changes beaucoup trop rapidement pour être conservée dans les antémémoires du DNS. Il semble aux auteurs qu'offrir aux administrateurs un moyen de dire "cette machine est trois fois plus rapide que cette autre" est le mieux qui puisse être fait en pratique.

La seule façon dont nous pensons qu'on puisse obtenir une "meilleure" figure de charge est de demander un serveur distinct lorsque le client choisit un serveur et le contacte. Pour les services de courte durée de vie, une étape supplémentaire dans l'établissement de la connexion semble trop coûteuse, et pour les services de longue durée, la charge peut fort bien

complètement changer d'aspect une minute après l'établissement de la connexion lorsque quelqu'un d'autre commence ou termine une grosse tâche.

Note : Il y a actuellement diverses expériences de fourniture d'une estimation de la proximité relative du réseau, de la bande passante disponible, et des services similaires. L'utilisation de l'enregistrement SRV avec de telles facilités, et en particulier l'interprétation du champ Poids lorsque ces facilités sont utilisées, fera l'objet d'études complémentaires. Poids est seulement destiné au choix de serveur statique, et non pas dynamique. L'utilisation du poids SRV pour le choix dynamique du serveur exigerait d'allouer des TTL déraisonnablement courts aux RR SRV, ce qui limiterait l'utilité du mécanisme de mise en antémémoire du DNS, accroissant donc la charge globale du réseau et diminuant la fiabilité globale. Le choix de serveur via SRV est seulement destiné à exprimer des informations statiques telles que "ce serveur a un CPU plus rapide que cet autre" ou "ce serveur a une bien meilleure connexion réseau que cet autre".

Le numéro d'accès

Actuellement, la traduction du nom de service au numéro d'accès se produit chez le client, en utilisant souvent un fichier tel que /etc/services.

Amener cette information au DNS rend moins nécessaire la mise à jour de ces fichiers sur chaque ordinateur du réseau chaque fois qu'on ajoute un nouveau service, et rend possible le déplacement de services standard hors de la gamme d'accès "racine-seule" sur unix.

Règles d'utilisation

Un client à capacité SRV DEVRAIT utiliser cette procédure pour localiser une liste des serveurs et se connecter au préféré :

Faire une recherche pour QNAME=_service._protocol.target, QCLASS=IN, QTYPE=SRV.
Si la réponse est NOERROR, ANCOUNT>0 et si il y a au moins un RR SRV qui spécifie le service et protocole demandés dans la réponse :
Si il y a précisément un RR SRV, et si sa cible est "." (le domaine racine), abandonner.
Autrement, pour tous les RR, construire une liste des tuplets (Priorité, Poids, Cible)
Trier la liste par priorité (par valeurs croissantes)
Créer une nouvelle liste vide pour chaque niveau de priorité distinct tant qu'il y a encore des éléments à ce niveau de priorité
Choisir un élément comme spécifié ci-dessus, dans la description de Poids au paragraphe "Format du RR de SRV", et le placer en queue de la nouvelle liste
Pour chaque élément de la nouvelle liste interroger le DNS sur les enregistrements d'adresse pour la Cible ou utiliser tout enregistrement trouvé dans la section Données supplémentaires d'une réponse SRV antérieure.
Pour chaque enregistrement d'adresse trouvé, essayer de se connecter au (protocole, adresse, service).
Autrement
Faire une recherche pour QNAME=target, QCLASS=IN, QTYPE=A
Pour chaque enregistrement d'adresse trouvé, essayer de se connecter au (protocole, adresse, service).

Notes :
- Les numéros d'accès NE DEVRAIENT PAS être utilisés à la place des noms symboliques de service ou de protocole (pour la même raison que les variantes de nom ne peuvent pas être admises : les applications auraient a faire d'autant plus de recherches).
- Si une réponse tronquée revient d'une interrogation de SRV, les règles décrites dans la [RFC 2181] doivent être appliquées.
- Un client DOIT analyser tous les RR de la réponse.
- Si la section Données supplémentaires ne contient pas d'enregistrement d'adresse pour tous les RR SRV et si le client veut se connecter à l'hôte ou aux hôtes cible impliqués, le client DOIT rechercher les enregistrements d'adresse. (Cela arrive assez souvent lorsque l'enregistrement d'adresse a un TTL plus bref que celui du RR SRV ou NS.)
- Des protocoles pourront à l'avenir être conçus pour utiliser des recherches de RR SRV comme moyens par lesquels des clients localisent leurs serveurs.

Exemple fictif

Le présent exemple utilise le service fictif "foobar" pour aider à comprendre les enregistrements SRV. Si jamais un service "foobar" est mis en œuvre, il n'est pas prévu qu'il doive nécessairement utiliser des enregistrements SRV. Ceci est le fichier de zone (partiel) pour example.com, domaine encore inutilisé :

```
    $ORIGIN example.com.
    @           SOA server.example.com. root.example.com. ( 1995032001 3600 3600 604800 86400 )
                NS  server.example.com.
                NS  ns1.ip-provider.net.
                NS  ns2.ip-provider.net.
; foobar - utiliser une vieille boîte lente ou une nouvelle boîte rapide s'il en est de disponible, fait passer les trois quarts des connexions à une nouvelle boîte rapide.
    _foobar._tcp    SRV 0 1 9 old-slow-box.example.com.
                    SRV 0 3 9 new-fast-box.example.com.
; si ni la vieille boîte lente ni la nouvelle boîte rapide ne sont actives, passer à l'utilisation de la boîte sysdmin et au serveur
                    SRV 1 0 9 sysadmins-box.example.com.
                    SRV 1 0 9 server.example.com.
    server          A   172.30.79.10
    old-slow-box    A   172.30.79.11
    sysadmins-box   A   172.30.79.12
    new-fast-box    A   172.30.79.13
; AUCUN autre service n'est pris en charge
    *._tcp          SRV  0 0 0 .
    *._udp          SRV  0 0 0 .
```

Dans cet exemple, un client du service "foobar" dans le domaine "example.com." a besoin d'une recherche de SRV de "_foobar._tcp.example.com." et éventuellement de recherches A de "new-fast-box.example.com." et/ou des autres hôtes nommés. La taille de la réponse SRV est approximativement de 365 octets :

30 octets de redondance générale
20 octets pour la chaîne d'interrogation, "_foobar._tcp.example.com."
130 octets pour 4 RR SRV, de 20 octets chacun plus les longueurs de "new-fast-box", "old-slow-box", "server" et "sysadmins-box" - "example.com" dans la section d'interrogation est mis ici entre guillemets et n'a pas à être compté à nouveau.
75 octets pour 3 RR NS, de 15 octets chacun plus les longueurs de "server", "ns1.ip-provider.net." et "ns2" – ici encore, "ip-provider.net." est mis entre guillemets et ne doit être compté qu'une seule fois.
120 octets pour les 6 enregistrements d'adresse (en supposant seulement IPv4) mentionnés par les RR SRV et NS.

Considérations relatives à l'IANA

L'IANA a alloué la valeur de type de RR de 33 au RR de SRV. Aucun autre service de l'IANA n'est exigé par le présent document.

Changements par rapport à la RFC 2052

Le présent document rend obsolète la RFC 2052. Le changement majeur par rapport à la version précédente, expérimentale, de cette spécification est que maintenant les étiquettes de protocole et de service sont précédées d'un souligné, pour diminuer la probabilité d'une collision accidentelle avec un nom similaire utilisé pour des besoins sans rapport avec celui-ci. À côté de cela, les changements sont seulement destinés à améliorer la clarté et l'exhaustivité du document. Le présent document précise particulièrement l'utilisation du champ Poids des enregistrements de SRV.

Considérations pour la sécurité

Les auteurs estiment que ce RR ne cause aucun nouveau problème de sécurité. Certains problèmes deviennent cependant plus visibles.

- La capacité à spécifier les accès sur la base d'une granularité plus fine change évidemment la façon dont un routeur filtre les paquets. Il devient impossible de bloquer l'accès des clients internes à des services externes spécifiques, légèrement plus difficile de bloquer l'accès des utilisateurs internes à des services non autorisés, et plus important que le personnel de fonctionnement du routeur et du DNS de coopérer.

- Un site ne peut pas empêcher que ses hôtes soient référencés comme serveurs. Cela pourrait conduire à des dénis de service.

- Avec SRV, des usurpateurs du DNS peuvent fournir de faux numéros d'accès, ainsi que des noms et adresses d'hôte. Parce que cette faiblesse existe déjà avec les noms et adresses, ce n'est pas une nouvelle faiblesse, simplement une faiblesse légèrement augmentée, avec peu d'effet pratique.

Références

STD 2 J. Reynolds et J. Postel, "Numéros alloués", STD 2, RFC 1700, octobre 1994.

RFC 1034 P. Mockapetris, "Noms de domaines - concepts et facilités", STD 13, RFC 1034, novembre 1987.

RFC 1035 P. Mockapetris, "Noms de domaines – mise en œuvre et spécification", STD 13, RFC 1035, novembre 1987.

RFC 974 C. Partridge, "L'acheminement de la messagerie et le système des domaines", STD 14, RFC 974, janvier 1986.

BCP 14 S. Bradner, "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence", BCP 14, RFC 2119, mars 1997.

RFC 2181 R. Elz et R. Bush, "Précisions sur la spécification du DNS", RFC 2181, juillet 1997.

RFC 2219 M. Hamilton et R. Wright, "Utilisation des alias du DNS pour les services réseau", BCP 17, RFC 2219, octobre 1997.

ARM M. Armijo, L. Esibov et P. Leach, "Découverte des services LDAP avec le DNS", Travail en cours.

KDC-DNS K. Hornstein et J. Altman, "Distribution de KDC Kerberos et d'informations de domaine avec le DNS", Travail en cours.

Remerciements

L'algorithme utilisé pour choisir entre les RR SRV pondérés d'égale priorité est adapté de celui fourni par Dan Bernstein.

Adresse des auteurs

Arnt Gulbrandsen
Troll Tech
Waldemar Thranes gate 98B
N-0175 Oslo, Norway
Fax : +47 22806380
téléphone : +47 22806390
mél : arnt@troll.no

Paul Vixie
Internet Software Consortium
950 Charter Street
Redwood City, CA 94063
téléphone : +1 650 779 7001

Levon Esibov
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052
mél : levone@microsoft.com

Déclaration de copyright

Remerciement

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