RFC 9460 : Service Binding and Parameter Specification via the DNS (SVCB and HTTPS Resource Records)

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 8 avril 2024

Date de publication du RFC : Novembre 2023

https://www.bortzmeyer.org/9460.html

Ces deux nouveaux types d'enregistrement DNS, SVCB et sa variante HTTPS, permettent de donner des informations supplémentaires à un client réseau avant qu'il ne tente de se connecter à un serveur. On peut envoyer ainsi des indications sur les versions des protocoles gérées, des clés cryptographiques ou des noms de serveurs supplémentaires.

Un client d'un service réseau a en effet plein de questions à se poser avant de tenter une connexion. Quelle adresse IP utiliser ? Quel port ? Chiffrement ou pas ? Les anciens mécanismes traitent la question de l'adresse IP (on la trouve par une requête DNS) et celle du port, si on se limite aux ports bien connus (comme 43 pour whois). Mais cela ne dit pas, par exemple, si le serveur HTTP distant accepte ou non HTTP/3 (RFC 9114 [1]). Par contre, cet enregistrement HTTPS de Cloudflare va bien nous dire que ce serveur accepte HTTP/2 et 3 :

```
% dig cloudflare.com HTTPS
...
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 28399
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1
...
;; ANSWER SECTION:
cloudflare.com. 300 IN HTTPS 1 . alpn="h3,h2" ipv4hint=104.16.132.229,104.16.133.229 ipv6hint=2606:4700::6810:84
...
;; WHEN: Mon Apr 08 09:27:01 CEST 2024
;; MSG SIZE  rcvd: 226
```

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc9114.txt

L'idée de base de SVCB (et de HTTPS qui en est dérivé) est donc de fournir à l'avance au client toutes les informations utiles pour se connecter. Le type d'enregistrement SRV (RFC 2782) avait été un pas dans cette direction mais n'a jamais été massivement adopté, en partie parce que HTTP, dans une grosse erreur de conception, ne l'utilisait pas (l'annexe C.1 détaille les différences enter SRV et SVCB/HTTPS).

Bon, en quoi consiste cet enregistrement SVCB ? Il a deux modes de fonctionnement, **alias** et **service**. Le premier mode sert à faire d'un nom une version canonique d'un autre, un peu comme le CNAME mais en étant utilisable à l'apex d'une zone <https://www.bortzmeyer.org/cname-apex.html>. Le second mode sert à indiquer les paramètres techniques de la connexion. Un enregistrement SVCB (ou HTTPS) a trois champs dans ses données :

- `SvcPriority` : quand il vaut zéro, il indique le mode alias. Autrement (par exemple dans le cas ci-dessus), il indique la priorité de ces paramètres.
- `TargetName` : en mode alias, il indique le nom canonique, ou autrement un nom alternatif (pour un service accessible via plusieurs noms). Dans l'exemple Cloudflare ci-desssus, il valait la racine (un point) ce qui indique l'absence de nom alternatif (section 2.5).
- `SvcParams` : une liste de couples {clé,valeur} pour les paramètres de connexion (uniquement en mode service). Dans le cas avec Cloudflare, c'était `alpn="h3,h2" ipv4hint=104.16.132.229,104.16.1` `ipv6hint=2606:4700::6810:84e5,2606:4700::6810:85e5`. (Si vous vous intéressez aux débats à l'IETF, la question de la syntaxe de ces paramètres avait suscité une longue discussion <https://mailarchive.ietf.org/arch/msg/dnsop/fePoVb6vhryjzaMFSx_lzUcqLPk/>.)

Les enregistrements SVCB ont le type 64 (enregistré à l'IANA <https://www.iana.org/assignments/dns-parameters/dns-parameters.xml#dns-parameters-4>) et les HTTPS, qui ont la même syntaxe et le même contenu, mais sont spécifiques à HTTP, ont le 65 (SVCB est générique). Les enregistrements HTTPS (et de futurs enregistrements pour d'autres protocoles) sont dits « compatibles avec SVCB » car ils ont la même syntaxe et la même sémantique.

Notre RFC définit (section 7) une liste de paramètres possibles mais d'autres peuvent être ajoutés dans un registre IANA <https://www.iana.org/assignments/dns-svcb/dns-svcb.xml#dns-svcparamk via la procédure « Examen par un expert » (RFC 8126). Pour l'instant, il y a, entre autres :

- `alpn` : indique l'ALPN (RFC 7301).
- `ech` : il servira à indiquer la clé à utiliser pour chiffrer le SNI.
- `port` : comme son nom l'indique.
- `ipv4hint` et `ipv6hint` : les adresses IP du service.

L'enregistrement peut (cela dépend des protocoles qui l'utilisent, HTTP ne le fait pas) être placé sur un sous-domaine indiquant le service, par exemple `_8765._baz.api.example.com` (section 10.4.5).

Idéalement, un serveur faisant autorité <https://www.bortzmeyer.org/serveur-dns-faisant-autorit html> devrait renvoyer les SVCB et les HTTPS, s'ils sont présents, dans la section additionnelle de la réponse, lorsque le type demandé était une adresse IP. Mais ceux de Cloudflare ne semblent pas le faire actuellement. (PowerDNS le fait <https://doc.powerdns.com/authoritative/guides/svcb.html>.)

Si vous vous intéressez aux questions opérationnelles, et que vous voulez mettre des enregistrements SVCB/HTTPS dans votre zone, la section 10 du RFC est faite pour vous. J'ai des enregistrements HTTPS pour ce blog :

```
# Un alias à l'apex (la priorité 0 indique le mode alias)
% dig +short +nodnssec bortzmeyer.org HTTPS
0 www.bortzmeyer.org.

# J'ai HTTP/2 (mais pas encore HTTP/3)
% dig +short +nodnssec www.bortzmeyer.org HTTPS
1 . alpn="h2"
```

Pour cela, j'ai mis dans le fichier de zone :

```
; Enregistrements SVCB (HTTPS).

; HTTP/2 (mais pas encore - au 2024-04-08 - de HTTP/3)
www IN HTTPS 1 . alpn="h2"

; alias
@ IN HTTPS 0 www.bortzmeyer.org.
```

Les clients HTTP récents, qui gèrent SVCB/HTTPS vont alors se connecter directement en HTTP/2 à `https://www.bortzmeyer.org/` même si l'utilisateur demandait originellement `http://bortzmeyer.org/` (le type d'enregistrement HTTPS, comme son nom l'indique, sert aussi à annoncer qu'on accepte HTTPS, ce qui permettra d'abandonner HSTS). Les clients HTTP plus anciens, évidemment, ne connaissent pas le système SVCB/HTTPS et il faut donc garder une configuration pour eux (par exemple des adresses IP à l'apex). Il y a aussi les autres méthodes, comme le `Alt-Svc:` du RFC 7838. La section 9.3 du RFC décrit le comportement attendu lorsque les différentes méthodes coexistent.

Faites attention toutefois, lorsque vous mettez ce type d'enregistrements dans votre zone, je ne connais pas encore d'outils de test permettant de vérifier la syntaxe des enregistrements, encore moins leur correspondance avec la réalité (par exemple, SSLLabs <`https://www.ssllabs.com/ssltest/`> ne semble pas le faire). C'est un problème général de la signalisation sur l'Internet, quand on signale (notamment via le DNS) les capacités d'un serveur : le logiciel client doit de toute façon être prêt à tout, car il ne peut jamais être sûr que le signal est conforme aux faits.

En parlant d'anciens logiciels (clients et serveurs), vous pouvez trouver une liste de mises en œuvre de SVCB/HTTPS <`https://github.com/MikeBishop/dns-alt-svc/blob/main/svcb-implementations.md`>. Attention, elle est incomplète et pas à jour. Notez qu'il y a parfois des contraintes particulières, ainsi, il semble que Firefox ne demande des enregistrements HTTPS <`https://bugzilla.mozilla.org/show_bug.cgi?id=1721132`> que s'il utilise DoH. iOS envoie des requêtes HTTPS depuis iOS 14, publié en septembre 2020, ce qui avait étonné, à l'époque <`https://mailman.nanog.org/pipermail/nanog/2020-September/209823.html`>.

En parlant de Firefox, s'il est assez récent, et s'il est configuré pour faire du DoH, vous pouvez tester le SVCB/HTTPS en allant dans `about:networking#dnslookuptool`. En entrant un nom de domaine, le champ « RR HTTP » doit renvoyer l'enregistrement HTTPS.

Avec un tcpdump récent, voici le trafic DNS utilisant le nouvel enregistrement DNS, qu'on peut observer sur un serveur faisant autorité pour `bortzmeyer.org` :

```
09:49:23.354974 IP6 2a04....31362 > 2001:4b98:dc0:41:216:3eff:fe27:3d3f.53: 13024% [1au] HTTPS? www.bortzmeyer.o
09:52:06.094314 IP6 2a00....56551 > 2001:4b98:dc0:41:216:3eff:fe27:3d3f.53: 40948% [1au] HTTPS? wWw.bOrTZmEyER.O
10:06:21.501437 IP6 2400....11624 > 2001:4b98:dc0:41:216:3eff:fe27:3d3f.53: 59956 [1au] HTTPS? doh.bortzmeyer.fr
10:06:21.999608 IP6 2400....36887 > 2001:4b98:dc0:41:216:3eff:fe27:3d3f.53: 17231 [1au] HTTPS? radia.bortzmeyer.
10:25:53.947096 IP6 2001....54476 > 2001:4b98:dc0:41:216:3eff:fe27:3d3f.53: 26123% [1au] HTTPS? www.bortzmeyer.o
```

Si votre tcpdump est plus ancien, vous verrez Type65 au lieu de HTTPS.

Sinon, si vous aimez les bricolages (et celui-ci sera de moins en moins utile avec le temps, au fur et à mesure que les serveurs géreront ce type), pour fabriquer les enregistrements, vous pouvez utiliser cet outil <`https://github.com/massar/misc/tree/master/type65_https`>, qui va fabriquer la forme binaire, directement chargeable par les serveurs faisant autorité :

```
% perl type65_https.pl 'example.net HTTPS 1 . alpn="h3,h2" ipv4hint="192.0.2.42" ipv6hint="2001:db8::42"'
example.net. TYPE65 ( \# 41 000100000100060268330268320004000
04c000022a0006001020010db8000000 000000000000000042 )
```

(Il faut un `Net::DNS` récent sinon « *"unknown type "HTTPS" at /usr/share/perl5/Net/DNS/RR.pm line 671. in new Net::DNS::RR(www.bortzmeyer.org HTTPS 1 . alpn="h2") at type65_https.pl line 30."* ».)

Quelques articles pas mal :

— *"Simple HTTPS Records"* <https://kalfeher.com/https-records-simple/> par Kal Feher.
— *"Use of HTTPS Resource Records"* <https://netmeister.org/blog/https-rrs.html> avec le résultat de mesures sur le déploiement effectif.
— Autres mesures dans le monde, l'article *"Deciphering the Digital Veil : Exploring the Ecosystem of DNS HTTPS Resource Records"* <https://arxiv.org/abs/2403.15672>.