DNS SRV Records for HTTP
draft-jennings-http-srv-03

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on August 28, 2009.

Copyright Notice

Copyright (c) 2009 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document.

This document may contain material from IETF Documents or IETF Contributions published or made publicly available before November 10, 2008. The person(s) controlling the copyright in some of this document
material may not have granted the IETF Trust the right to allow modifications of such material outside the IETF Standards Process. Without obtaining an adequate license from the person(s) controlling the copyright in such materials, this document may not be modified outside the IETF Standards Process, and derivative works of it may not be created outside the IETF Standards Process, except to format it for publication as an RFC or to translate it into languages other than English.

Abstract

This document specifies a new URI scheme called http+srv which uses a DNS SRV lookup to locate a HTTP server. The http+srv scheme operates in the same way as an http scheme but instead of the normal DNS lookup that a http scheme would use, it first tries an DNS SRV lookup. This memo also defines a https+srv scheme that operates in the same way as an https URI but uses DNS SRV lookups.

The draft is being discussed on the apps-discuss@ietf.org list.

Legal

This documents and the information contained therein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY, THE IETF TRUST AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION THEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

1. Introduction

Web services often define APIs where software running on machine in a data center acts as an HTTP client and performs some http transactions to another HTTP server. For example, a portal such as Facebook can act as a http client and call specific HTTP-based APIs on other http servers. The reality of current networks is a large portion of the hosts have NATed addresses and often can not run on port 80. This is likely to become more common with the deployment of Carrier Grade NAT. DNS SRV records allow a DNS lookup of a name like www.example.com to provide both a port and the IP addresses of the HTTP server.

This specification defines two new URI schemes, http+srv, and https+srv which are like http and https respectively. When a http client uses one of theses schemes to locate a web server, it starts by doing
a DNS SRV record lookup and if one is found, uses that result. If no SRV record is found, it falls back to a DNS address (A or AAAA) record. The specification does not update or modify HTTP in any way.

It is not expected that most web browsers would support these schemes for generic web use. It would instead be used for particular applications using HTTP such as specific web APIs. These APIs would be defined to require the use of this specification. In this situation, the end user’s web browser might not do the SRV lookup when it browsed to the portal web pages, but the HTTP calls that the portal made out to other sites to generate the content would use this mechanism. As such architectures become more common, DNS SRV would allow many servers that are just providing an API to run on ports other than 80 even though main portal sites may still be running on the well known ports. Eventually, web browsers may end up supporting these SRV lookups, as the implementation is trivial and has very little downside.

This technique is useful where users wish to run a web server behind a NAT but cannot control which port the NAT will allocate for the service. It is also useful where several users want to run different web servers on the same machine. A third use case for HTTP SRV is a situation in which all requests should be sent to a primary server, but if that server is down, then requests should fall back to an alternative server.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

3. Mechanisms

Applications compliant with this specification MUST perform an SRV lookup as specified in [RFC2782] when resolving the host portion of a http+srv or https+srv URI. As defined in the IANA port numbers registry, the service names used are _http and _https respectively. As described in RFC 2782, if no SRV record is present, the resolution will fall back on using other DNS records that would be used by a http scheme as defined in HTTP[RFC2616]. The rest of the http+srv URI is processed in the same way as an http URI in RFC 2616 while the rest of a https+srv scheme URI is processed the same way as a https URI as defined in [RFC2818].
4. Example

In the following example, the client will do a lookup on the URI, which finds the SRV record that then points at the A record that points at the IP address.

URI: https+srv://example.com
DNS SRV RR: _https._tcp.example.com. SRV 1 0 8080 host1.example.com.
DNS A RR:    host1.example.com.       A   192.0.2.88

Figure 1

In this case the client would form a TCP connection to 192.0.2.88:8080 then start TLS over that connection. Note that the certificate in the TLS handshake would be matched to example.com as that was the names used in the URI and it would not be matched to host1.example.com.

5. IANA Considerations

This specification registers two provisional URI schemes.

5.1. http+srv URI scheme

URI scheme name:

http+srv

Status:

provisional

URI scheme syntax:

Identical to http URI as defined in RFC 2616 but using the 'http+srv' protocol identifier in place of the 'http' protocol identifier

URI scheme semantics:

See draft-jennings-http-uri

Encoding considerations:
No special considerations

Applications/protocols that use this URI scheme name:

Applications which need to lookup http servers using DNS SRV

Interoperability considerations.:

None known

Security considerations.:

Same as http URI. See RFC 2616

Contact.:

Cullen Jennings <fluffy@cisco.com>

Author/Change controller.:

Cullen Jennings <fluffy@cisco.com>

References.:

draft-jennings-http-srv

RFC 3986

RFC 2616

5.2. https+srv URI scheme

URI scheme name:

https+srv

Status:

provisional

URI scheme syntax:

Identical to http URI as defined in RFC 2818 but using the 'https+srv' protocol identifier in place of the 'https' protocol identifier
URI scheme semantics:

See draft-jennings-http-uri

Encoding considerations:

No special considerations

Applications/protocols that use this URI scheme name:

Applications which need to lookup http servers using DNS SRV

Interoperability considerations.:

None known

Security considerations.:

Same as https URI. See RFC 2818

Contact.:

Cullen Jennings <fluffy@cisco.com>

Author/Change controller.:

Cullen Jennings <fluffy@cisco.com>

References.:

draft-jennings-http-srv

RFC 3986

RFC 2818

6. Security Considerations

This introduces no new security considerations beyond the common usage of HTTP. It is analogous to DNS CNAME records that redirect address records.

7. Acknowledgements

Variants of this idea has been proposed by many people, including Mark Andrews and Thor Kottelin in an internet draft in 2000. Some
text came from various documents by Ted Hardie. Thanks to good feedback from many people including Ted Hardie, Mr. Moonesamy, Cyrus Daboo, Stefanos Harhalakis, Ray Bellis, John Klensin, and Eran Hammer-Lahav.

8. Normative References


Author’s Address

Cullen Jennings
Cisco Systems
170 West Tasman Drive
Mailstop SJC-30
San Jose, CA  95134
USA

Phone: +1 408 902-3341
Email: fluffy@cisco.com