Use of SRV Records for Locating Email Submission/Access Services

Abstract

   This specification describes how SRV records can be used to locate
   email services.

Status of This Memo

   This is an Internet Standards Track document.

   This document is a product of the Internet Engineering Task Force
   (IETF). It represents the consensus of the IETF community. It has
   received public review and has been approved for publication by the
   Internet Engineering Steering Group (IESG). Further information on
   Internet Standards is available in Section 2 of RFC 5741.

   Information about the current status of this document, any errata,
   and how to provide feedback on it may be obtained at
   http://www.rfc-editor.org/info/rfc6186.

Table of Contents

1. Introduction

   Internet email protocols include SMTP [RFC5321], IMAP [RFC3501], and
   POP3 [RFC1939]. IMAP and POP3 are both message store access
   protocols used by message store user agents (MUAs) to manipulate
   email messages after delivery. [RFC4409] defines a "profile" of the
   SMTP service that is specifically used for message submission. MUAs
   are expected to submit messages to mail submission agents (MSAs)
   using this approach.

   [RFC2782] defines a DNS-based service discovery protocol that has
   been widely adopted as a means of locating particular services within
   a local area network and beyond, using DNS SRV resource records
   (RRs).

   [RFC5321] specifies how to use DNS MX RRs to locate SMTP services for
   a domain. However, MUAs are expected to use the submission protocol
   defined in [RFC4409], which does not use MX records.

   Typically MUAs have required users to enter a fully qualified domain
   name (FQDN) and port information for the services they need. This is
   not ideal as the way in which server configuration information is
   specified can differ from MUA to MUA, and can be confusing to users,
   leading to errors when inputting the details. Alternatively, some
   MUAs have adopted a complex "auto-discovery" process involving
   probing a domain to see what services might be available. A better
   approach to all this would be to require minimal information to be
   entered by a user that would result in automatic configuration of
   appropriate services for that user. The minimal information entered
   would be the user's email address.

This specification defines new SRV service types for the message submission, IMAP, and POP3 services, to enable simple auto-configuration of MUAs. The priority field of the SRV record can also be used to indicate a preference for one message store access protocol over another.

2. Conventions Used in This Document

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 [RFC2119].

Email-related terminology from [RFC5598] is used.

3. SRV Service Labels

3.1. Email Submission

This specification adds one SRV service label for message submission [RFC4409]:

submission: Identifies an MSA using [RFC4409]. Note that this covers connections both with and without Transport Layer Security (TLS) [RFC5246] as defined for SMTP in [RFC3207].

Example: service record

    _submission._tcp   SRV 0 1 587 mail.example.com.

3.2. IMAP

This specification adds two SRV service labels for IMAP [RFC3501]:

_imap: Identifies an IMAP server that MAY advertise the "LOGINDISABLED" capability and MAY require the MUA to use the "STARTTLS" command prior to authentication. Although these two extensions are mandatory-to-implement for both MUAs and IMAP servers, they are not mandatory-to-use by service providers.

_imaps: Identifies an IMAP server where TLS [RFC5246] is initiated directly upon connection to the IMAP server.

Example: service record

    _imap._tcp   SRV 0 1 143 imap.example.com.

   Example: service record

      _imaps._tcp   SRV 0 1 993 imap.example.com.

3.3. POP3

   This specification adds two SRV service labels for POP3 [RFC1939]:

   _pop3: Identifies a POP3 server that MAY require the MUA to use the
      "STLS" extension command [RFC2595] prior to authentication.

   _pop3s: Identifies a POP3 server where TLS [RFC5246] is initiated
      directly upon connection to the POP3 server.

   Example: service record

      _pop3._tcp   SRV 0 1 110 pop3.example.com.

   Example: service record

      _pop3s._tcp   SRV 0 1 995 pop3.example.com.

3.4. Priority for Domain Preferences

   The priority field in the SRV RR allows a domain to indicate that
   some records have a higher preference than others in the DNS query
   results (determined by those records having a lower-numbered priority
   value). Typically, this is used for choosing a record from a set for
   a single service label; however, it is not restricted to choice
   within only one service.

   Often a site will offer both IMAP and POP3 message store access
   services for users. However, the site may have a preference for one
   over the other that they want to convey to the user to ensure that,
   when the user has an MUA capable of using both IMAP and POP3, the
   preferred choice is used.

   To aid with this choice, sites SHOULD offer both sets of IMAP (_imap
   and/or _imaps) and POP3 (_pop3 and/or _pop3s) SRV records in their
   DNS and set the priority for those sets of records such that the
   "preferred" service has a lower-numbered priority value than the
   other. When an MUA supports both IMAP and POP3, it SHOULD retrieve
   records for both services and then use the service with the lowest
   priority value. If the priority is the same for both services, MUAs
   are free to choose whichever one is appropriate. When considering
   multiple records for different protocols at the same priority but
   with different weights, the client MUST first select the protocol it

intends to use, then perform the weight selection algorithm given in
[RFC2782] on the records associated with the selected protocol.

Example: service records for both IMAP and POP3, with IMAP having a
lower-numbered priority value (0) than POP3 (10), indicating to the
MUA that IMAP is preferred over POP3, when the MUA can support either
service.

```
_imap._tcp      SRV  0 1 143 imap.example.com.
_pop3._tcp      SRV 10 1 110 pop3.example.com.
```

In addition, with SRV RRs it is possible to indicate that a
particular service is not supported at all at a particular domain by
setting the target of an SRV RR to ".". If such records are present,
clients MUST assume that the specified service is not available, and
instead make use of the other SRV RRs for the purposes of determining
the domain preference.

Example: service records for IMAP and POP3 with both TLS and non-TLS
service types are present. Both IMAP and POP3 non-TLS service types
are marked as not available. IMAP (with TLS) has a lower-numbered
priority value 0 than POP3 (with TLS) at priority 10, indicating to
the MUA that IMAP is preferred over POP3, when the MUA can support
either service, and only the TLS versions of the services are
available.

```
_imap._tcp      SRV  0 0 0   .
_imaps._tcp     SRV  0 1 993 imap.example.com.
_pop3._tcp      SRV  0 0 0   .
_pop3s._tcp     SRV 10 1 995 pop3.example.com.
```

4. Guidance for MUAs

By using SRV records as above, MUAs need initially only to prompt the
user for their email address [RFC5322]. The "local-part" and
"domain" portions are then extracted from the email address by the
MUA. The MUA uses the "domain" portion as the service domain to
perform SRV lookups for the services it wants to configure. If the
SRV lookup is successful, the target FQDN and port for the service
can be determined and used to complete MUA configuration. If an SRV
record is not found, the MUA will need to prompt the user to enter
the FQDN and port information directly, or use some other heuristic.
In the case of multiple SRV records returned for a particular
service, the MUA MUST use the priority and weight fields in the
record to determine which one to use (as per [RFC2782]).

MUAs that support both POP3 and IMAP use the procedure in Section 3.4
to choose between each service when both are offered.

   Subsequent to configuration, the MUA will connect to the service.
   When using "imaps" or "pop3s" services, a TLS [RFC5246] negotiation
   is done immediately upon connection. With "imap", "pop3", and
   "submission" services, the "STARTTLS", "STLS", and "STARTTLS"
   commands respectively are used to initiate a protected connection
   using TLS [RFC5246]. When using TLS in this way, MUAs SHOULD use the
   TLS Server Name Indication [RFC6066]. Certificate verification MUST
   use the procedure outlined in Section 6 of [RFC6125] in regard to
   verification with an SRV RR as the starting point.

   Once a suitable connection has been made, and any required protection
   set up, the MUA will typically need to authenticate with the IMAP,
   POP3, or SMTP (submission) server. The details of that are governed
   by the specific protocols themselves, though often times a "user
   identifier" is required for some form of user/password
   authentication. When a user identifier is required, MUAs MUST first
   use the full email address provided by the user, and if that results
   in an authentication failure, SHOULD fall back to using the "local-
   part" extracted from the email address. This is in line with the
   guidance outlined in Section 5. If both these user identifiers
   result in authentication failure, the MUA SHOULD prompt the user for
   a valid identifier.

   Once a successful connection and authentication have been done, MUAs
   SHOULD cache the service details (hostname, port, user identity) that
   were successfully used, and reuse those when connecting again at a
   later time.

   If a subsequent connection attempt fails, or authentication fails,
   MUAs SHOULD re-try the SRV lookup to "refresh" the cached data for
   the same protocol the client had chosen earlier; i.e., this means
   that the client MUST NOT change from IMAP service to POP3 (or vice
   versa) due to changes in the corresponding SRV priorities without
   user interaction.

5. Guidance for Service Providers

   Service providers wanting to offer IMAP, POP3, or SMTP (submission)
   services that can be configured by MUAs using SRV records need to
   follow certain guidelines to ensure proper operation.

   a. IMAP, POP3, and SMTP (submission) servers SHOULD be configured to
       allow authentication with email addresses or email local-parts.
       In the former case, the email addresses MUST NOT conflict with
       other forms of permitted user login name. In the latter case,
       the email local-parts need to be unique across the server and
       MUST NOT conflict with any login name on the server.

   b. If the service provider uses TLS [RFC5246], the service provider
       MUST ensure a certificate is installed that can be verified by
       MUAs using the procedure outlined in Section 6 of [RFC6125] in
       regard to verification with an SRV RR as the starting point. If
       the service provider hosts multiple domains on the same IP
       address, then the service provider MUST enable support for the
       TLS Server Name Indication [RFC6066].

   c. Install the appropriate SRV records for the offered services.

6. Security Considerations

   If a user has explicitly requested a connection with a transport
   layer security mechanism (user interfaces sometimes present this
   choice as a "use SSL" or "secure connection" checkbox), the MUA MUST
   successfully negotiate transport layer security prior to sending an
   authentication command. For example, the MUA MAY do this with
   "imaps", "pop3s", "imap" with "STARTTLS", or "pop3" with "STLS".
   Service providers MAY offer any subset of these four options for the
   mail service.

   A malicious attacker with access to the DNS server data, or able to
   get spoofed answers cached in a recursive resolver, can potentially
   cause MUAs to connect to any IMAP, POP3, or submission server chosen
   by the attacker. In the absence of a secure DNS option, MUAs SHOULD
   check that the target FQDN returned in the SRV record matches the
   original service domain that was queried. If the target FQDN is not
   in the queried domain, MUAs SHOULD verify with the user that the SRV
   target FQDN is suitable for use before executing any connections to
   the host. Alternatively, if TLS [RFC5246] is being used for the
   email service, MUAs MUST use the procedure outlined in Section 6 of
   [RFC6125] to verify the service.

   Implementations of TLS [RFC5246] typically support multiple versions
   of the protocol as well as the older Secure Sockets Layer (SSL)
   protocol. Because of known security vulnerabilities, email clients
   and email servers MUST NOT request, offer, or use SSL 2.0. See
   Appendix E.2 of [RFC5246] for further details.

7. Acknowledgments

   Thanks to Tony Finch, Ned Freed, Alfred Hoenes, Suresh Krishnan,
   Alexey Melnikov, Chris Newman, and Phil Pennock for feedback and
   suggestions. Some of this work is based on a previously drafted
   document by John Klensin and Eric Hall.

8. References

8.1. Normative References

   [RFC1939] Myers, J. and M. Rose, "Post Office Protocol - Version 3",
              STD 53, RFC 1939, May 1996.

   [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate
              Requirement Levels", BCP 14, RFC 2119, March 1997.

   [RFC2595] Newman, C., "Using TLS with IMAP, POP3 and ACAP",
              RFC 2595, June 1999.

   [RFC2782] Gulbrandsen, A., Vixie, P., and L. Esibov, "A DNS RR for
              specifying the location of services (DNS SRV)", RFC 2782,
              February 2000.

   [RFC3207] Hoffman, P., "SMTP Service Extension for Secure SMTP over
              Transport Layer Security", RFC 3207, February 2002.

   [RFC3501] Crispin, M., "INTERNET MESSAGE ACCESS PROTOCOL - VERSION
              4rev1", RFC 3501, March 2003.

   [RFC4409] Gellens, R. and J. Klensin, "Message Submission for Mail",
              RFC 4409, April 2006.

   [RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security
              (TLS) Protocol Version 1.2", RFC 5246, August 2008.

   [RFC5321] Klensin, J., "Simple Mail Transfer Protocol", RFC 5321,
              October 2008.

   [RFC5322] Resnick, P., Ed., "Internet Message Format", RFC 5322,
              October 2008.

   [RFC6066] Eastlake, D., "Transport Layer Security (TLS) Extensions:
              Extension Definitions", RFC 6066, January 2011.

   [RFC6125] Saint-Andre, P. and J. Hodges, "Representation and
              Verification of Domain-Based Application Service Identity
              within Internet Public Key Infrastructure Using X.509
              (PKIX) Certificates in the Context of Transport Layer
              Security (TLS)", RFC 6125, March 2011.

8.2. Informative References

   [RFC5598] Crocker, D., "Internet Mail Architecture", RFC 5598,
              July 2009.

Author's Address

   Cyrus Daboo
   Apple Inc.
   1 Infinite Loop
   Cupertino, CA 95014
   USA

   EMail: cyrus@daboo.name
   URI: http://www.apple.com/