

Internet Engineering Task Force
Internet-Draft
Intended status: Standards Track
Expires: December 7, 2011

J. Schoenwaelder
Jacobs University Bremen
T. Tsou
C. Zhou
Huawei Technologies
June 5, 2011

DNS SRV Resource Records for Network Management Protocols
draft-schoenw-opsawg-nm-srv-02

Abstract

This document specifies how to use Domain Name Service (DNS) SRV Resource Records (RRs) to locate network management services.

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/lid-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 December 7, 2011.

Copyright Notice

Copyright (c) 2011 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. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the BSD License.

Table of Contents

| | | |
|-----------------------------|-----------------------------------|-------------------|
| 1. | Introduction | 3 |
| 2. | SRV Service Labels | 3 |
| 2.1. | SYSLOG | 3 |
| 2.2. | SNMP | 4 |
| 2.3. | NETCONF | 4 |
| 3. | Security Considerations | 5 |
| 4. | IANA Considerations | 5 |
| 5. | References | 5 |
| 5.1. | Normative References | 5 |
| 5.2. | Informative References | 6 |
| Appendix A. | Open Issues | 6 |
| | Authors' Addresses | 7 |

1. Introduction

This document specifies how to use Domain Name Service (DNS) SRV Resource Records (RRs) [[RFC2782](#)] to locate network management services. The use of SRV RRs can be useful in network bootstrapping scenarios or in zero-configuration network scenarios (e.g., home networks).

The network management DNS SRV RRs defined in this memo may be used for different purposes:

- o Manageable devices announce their management interfaces using a multicast DNS service. A management system discovers the devices and initiates management interactions with them.
- o Devices discover destinations for event notifications or logging services by looking up (statically) configured SRV RRs in the DNS.

The DNS SRV RRs defined in this memo address some gaps identified for the automated configuration of large IP networks [[I-D.ietf-opsawg-automated-network-configuration](#)].

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](#)].

2. SRV Service Labels

2.1. SYSLOG

The Reliable Delivery of syslog specification [[RFC3195](#)] mentions the usage of DNS SRV RRs to locate SYSLOG collectors. The more recent SYSLOG protocol specification [[RFC5424](#)] and the associated transport mappings ([[RFC5425](#)], [[RFC5426](#)], [[RFC6012](#)]) do not discuss the usage of SRV RRs to locate SYSLOG collectors. This specification takes the

service label definition from [[RFC3195](#)] and makes it applicable to structured SYSLOG as defined in [[RFC5424](#)]:

_syslog Identifies a SYSLOG collector. This SRV RR is primarily for discovery of SYSLOG collectors by SYSLOG originators or relays.

Example: service records

```
_syslog._tcp     SRV 0 1 6514 syslog.example.com.  
_syslog._udp     SRV 0 1 514 syslog.example.com.
```

A SYSLOG originator may need additional information to send SYSLOG messages to a SYSLOG collector. How this information is derived is not specified and implementation dependent.

[2.2.](#) SNMP

The Simple Network Management Protocol (SNMP) [[RFC3410](#)] distinguishes between SNMP entities containing command responder and notification originator applications (traditionally called agents) and SNMP entities containing command generator and/or notification receiver applications (traditionally called managers) [[RFC3411](#)]. This specification defines two new SRV service labels for SNMP:

_snmp Identifies an SNMP entity containing a command responder application. This record is primarily for discovery of SNMP agents that announce their presence using multicast DNS protocols.

_snmp-trap Identifies an SNMP entity containing a notification receiver application. This SRV RR is primarily for discovery of SNMP notification sinks by SNMP notification generator applications.

Example: service records

```
_snmp._udp        SRV 0 1 161 device.example.com.  
_snmp-trap._udp   SRV 0 1 162 nms.example.com.
```

An SNMP engine containing a command generator application needs

additional information to send SNMP messages to a SNMP engine containing a command responder application. How this information is derived is not specified and implementation dependent. Similarly, an SNMP engine containing a notification originator application needs additional information to send SNMP messages to a SNMP engine containing a notification receiver application. How this information is derived is not specified and implementation dependent.

[2.3.](#) NETCONF

The NETCONF protocol [[RFC4741](#)] provides mechanisms to install, manipulate, and delete the configuration of network devices. The mandatory to implement transport uses the Secure Shell (SSH) protocol [[RFC4742](#)]. SSH sessions are initiated by the NETCONF client. This specification adds a new SRV service label for NETCONF:

`_netconf` Identifies a NETCONF server. This record is primarily for discovery of NETCONF servers that announce their presence using multicast DNS protocols.

Example: service records

`_netconf._tcp SRV 0 1 830 device.example.com.`

A NETCONF client needs additional information in order to establish a session with a NETCONF server. How this information is derived is not specified and implementation dependent.

[3.](#) Security Considerations

The security considerations spelled out in the DNS SRV specification [[RFC2782](#)] apply. In general, the usage of DNSSEC [[RFC4033](#)] is recommended in environments where DNS cannot be trusted.

The usage of multicast DNS protocols to discover network management services potentially introduces new security risks since such protocols usually assume cooperating participants. In an environment

where antagonistic participants exists, it is necessary to deploy additional security mechanism such as DNSSEC to securely discover network management services.

[4.](#) IANA Considerations

TBD

[5.](#) References

[5.1.](#) Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.
- [RFC2782] Gulbrandsen, A., Vixie, P., and L. Esibov, "A DNS RR for specifying the location of services (DNS SRV)", [RFC 2782](#), February 2000.
- [RFC4033] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "DNS Security Introduction and Requirements", [RFC 4033](#), March 2005.
- [RFC4741] Enns, R., "NETCONF Configuration Protocol", [RFC 4741](#),

December 2006.

- [RFC4742] Wasserman, M. and T. Goddard, "Using the NETCONF Configuration Protocol over Secure SHell (SSH)", [RFC 4742](#), December 2006.
- [RFC5424] Gerhards, R., "The Syslog Protocol", [RFC 5424](#), March 2009.
- [RFC5425] Miao, F., Ma, Y., and J. Salowey, "Transport Layer Security (TLS) Transport Mapping for Syslog", [RFC 5425](#), March 2009.
- [RFC5426] Okmianski, A., "Transmission of Syslog Messages over UDP", [RFC 5426](#), March 2009.

- [RFC6012] Salowey, J., Petch, T., Gerhards, R., and H. Feng, "Datagram Transport Layer Security (DTLS) Transport Mapping for Syslog", [RFC 6012](#), October 2010.

[5.2.](#) Informative References

- [I-D.ietf-opsawg-automated-network-configuration] ZOU), T., Schoenwaelder, J., Shi, Y., Taylor, T., and G. Yang, "Problem Statement for the Automated Configuration of Large IP Networks", [draft-ietf-opsawg-automated-network-configuration-01](#) (work in progress), May 2011.
- [RFC3195] New, D. and M. Rose, "Reliable Delivery for syslog", [RFC 3195](#), November 2001.
- [RFC3410] Case, J., Mundy, R., Partain, D., and B. Stewart, "Introduction and Applicability Statements for Internet-Standard Management Framework", [RFC 3410](#), December 2002.
- [RFC3411] Harrington, D., Presuhn, R., and B. Wijnen, "An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks", STD 62, [RFC 3411](#), December 2002.

[Appendix A.](#) Open Issues

1. [draft-gudmundsson-dns-srv-iana-registry-04](#) proposes a template for registering SRV names. We may have to use this format in case this I-D moves forward.

2. [draft-hallambaker-esrv-01](#) proposes a RRs to store additional information in so called General Service Description (GSRV) and Extended Service Description (ESRV) records (e.g., which security protocol to use). This is traditionally done using TXT records.
3. [draft-gudmundsson-dnsexst-srv-clarify-02](#) clarifies service names and their usage.

4. [draft-kwatsen-reverse-ssh-00](#) proposes a mechanism which allows an SSH server to establish the TCP connection to an SSH client; if this moves forward NETCONF servers may want to discover NETCONF clients.
5. Add support for NTP? (DHC has an option to configure IP address of NTP servers.)

Authors' Addresses

Juergen Schoenwaelder
Jacobs University Bremen
Campus Ring 1
Bremen 28759
Germany

Email: j.schoenwaelder@jacobs-university.de

Tina Tsou
Huawei Technologies
Bantian, Longgang District
Shenzhen 518129
P.R. China

Email: tena@huawei.com

Cathy Zhou
Huawei Technologies
Bantian, Longgang District
Shenzhen 518129
P.R. China

Email: cathyzhou@huawei.com