Internet Engineering Task Force
Internet-Draft
Intended status: Informational
Expires: September 13, 2012

J. Schoenwaelder
Jacobs University Bremen
T. Tsou
C. Zhou
Huawei Technologies

March 12, 2012

DNS SRV Resource Records for Network Management Protocols
draft-schoenw-opsawg-nm-srv-03

Abstract

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

Status of this Memo

Copyright Notice

Table of Contents

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 [I-D.cheshire-dnsext-multicastdns]. 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. Service Names

IANA maintains the registry for service names and port numbers [RFC6335]. The service names maintained in this registry can be used with DNS SRV records. In addition, these service names can be used for dynamic service discovery as defined in [I-D.cheshire-dnsext-dns-sd].

2.1. SYSLOG

The Reliable Delivery of syslog specification [RFC3195] already 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.

Note that the IANA service names and port number registry defines the following service names and default port numbers:

Name	Port	Proto	Description	Reference
syslog	514	udp	Syslog over UDP	[RFC5426]
syslog-conn	601	tcp	Reliable Syslog Service	[RFC3195]
syslog-conn	601	udp	Reliable Syslog Service	[RFC3195]
syslog-tls	6514	tcp	Syslog over TLS	[RFC5425]
syslog-tls	6514	udp	Syslog over DTLS	[RFC5425]
syslog-tls	6514	dccp	Syslog over DTLS	[RFC5425]

Table 1: SYSLOG Service Names and Port Numbers

[[SYSLOG-Q1: Shall we suggest that implementations MUST or SHOULD use only the syslog service name for discovery? This way, it is not necessary to start a discovery for multiple service names. Of course, we also loose some context information (e.g., that TLS is to be used, which might matter if non-default port numbers are used). --JS]]

[[SYSLOG-Q2: What is the future of Reliable Syslog? Can we expect this to be retired so that we can choose to ignore it? --JS]]

[[SYSLOG-Q3: What to do with SYSLOG over DTLS/DCCP? Section 7 of the multicast service discovery document suggests that applications using transport protocols different from UDP and TCP should all use the _udp protocol label. Its unclear whether this is generally accepted common practice for SRV records or only a specific recommendation for service discovery. --JS]]

[[SYSLOG-Q4: SYSLOG over plain TCP is forthcoming. At the time of this writing, the specification is with the IESG. --JS]]

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. Similarily, 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.

Note that the IANA service names and port number registry defines the following service names and default port numbers:

Name	Port	Proto	Description	Reference
snmp	161	udp	SNMP over UDP	[RFC3430]
snmp	161	tcp	SNMP over TCP	[RFC3417]
snmp-trap	162	udp	SNMP traps over UDP	[RFC3430]
snmp-trap	162	tcp	SNMP traps over TCP	[RFC3417]
snmpssh	5161	tcp	SNMP over SSH	[RFC5592]
snmpssh-trap	5162	tcp	SNMP traps over SSH	[RFC5592]
snmptls	10161	tcp	SNMP over TLS	[RFC6353]
snmpdtls	10161	udp	SNMP over DTLS	[RFC6353]
snmptls-trap	10162	tcp	SNMP traps over TLS	[RFC6353]
snmptls-trap	10162	udp	SNMP traps over DTLS	[RFC6353]

Table 2: SNMP Service Names and Port Numbers

[[SNMP-Q1: Shall we suggest that implementations MUST or SHOULD use only the snmp and snmp-trap service names for discovery? This way, it is not necessary to start a discovery for multiple service names. Of course, we also loose some context information (e.g., that TLS is to be used, which might matter if non-default port numbers are used). --JS]]

2.3. NETCONF

The NECONF protocol [RFC6241] provides mechanisms to install, manipulate, and delete the configuration of network devices. The mandatory to implement transport uses the Secure Shell (SSH) protocol [RFC6242]. 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.

Note that the IANA service names and port number registry defines the following service names and default port numbers:

Name	Port	Proto	Description	Reference
netconf-ssh	830	tcp	NETCONF over SSH	[RFC6242]
netconf-beep	831	tcp	NETCONF over BEEP	[RFC4744]
netconfsoaphttp	832	tcp	NETCONF over SOAP/HTTP	[RFC4743]
netconfsoapbeep	833	tcp	NETCONF over SOAP/BEEP	[RFC4743]
netconf-tls	6513	tcp	NETCONF over TLS	[RFC5539]

Table 3: NETCONF Service Names and Port Numbers

[[NETCONF-Q1: Shall we suggest that implementations MUST or SHOULD use only the netconf service name for discovery? This way, it is not necessary to start a discovery for multiple service names. Of course, we also loose some context information (e.g., that TLS or SSH is to be used, which might matter if non-default port numbers are used). --JS]]

[[NETCONF-Q2: There is discussion to retire NETCONF over SOAP and NETCONF over BEEP which may simplify this a bit. --JS]]

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

[I-D.cheshire-dnsext-dns-sd]
Cheshire, S. and M. Krochmal, "DNS-Based Service Discovery", draft-cheshire-dnsext-dns-sd-11 (work in progress), December 2011.

[I-D.cheshire-dnsext-multicastdns]
Cheshire, S. and M. Krochmal, "Multicast DNS", draft-cheshire-dnsext-multicastdns-15 (work in progress), December 2011.

[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.

[RFC3195] New, D. and M. Rose, "Reliable Delivery for syslog", RFC 3195, November 2001.

[RFC3417] Presuhn, R., "Transport Mappings for the Simple Network Management Protocol (SNMP)", STD 62, RFC 3417, December 2002.

[RFC3430] Schoenwaelder, J., "Simple Network Management Protocol Over Transmission Control Protocol Transport Mapping", RFC 3430, December 2002.

[RFC4033] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "DNS Security Introduction and Requirements", RFC 4033, March 2005.

[RFC4743] Goddard, T., "Using NETCONF over the Simple Object Access Protocol (SOAP)", RFC 4743, December 2006.

[RFC4744] Lear, E. and K. Crozier, "Using the NETCONF Protocol over the Blocks Extensible Exchange Protocol (BEEP)", RFC 4744, 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.

[RFC5539] Badra, M., "NETCONF over Transport Layer Security (TLS)", RFC 5539, May 2009.

[RFC5592] Harrington, D., Salowey, J., and W. Hardaker, "Secure Shell Transport Model for the Simple Network Management Protocol (SNMP)", RFC 5592, June 2009.

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

[RFC6241] Enns, R., Bjorklund, M., Schoenwaelder, J., and A. Bierman, "Network Configuration Protocol (NETCONF)", RFC 6241, June 2011.

[RFC6242] Wasserman, M., "Using the NETCONF Protocol over Secure Shell (SSH)", RFC 6242, June 2011.

[RFC6335] Cotton, M., Eggert, L., Touch, J., Westerlund, M., and S. Cheshire, "Internet Assigned Numbers Authority (IANA) Procedures for the Management of the Service Name and Transport Protocol Port Number Registry", BCP 165, RFC 6335, August 2011.

[RFC6353] Hardaker, W., "Transport Layer Security (TLS) Transport Model for the Simple Network Management Protocol (SNMP)", RFC 6353, July 2011.

5.2. Informative References

[I-D.ietf-opsawg-automated-network-configuration] Tsou, 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-03 (work in progress), March 2012.

[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-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.

2. 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.

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