Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: November 3, 2007

E. Lear
Cisco Systems GmbH
May 2, 2007

syslog URIs
draft-lear-ietf-syslog-uri-00.txt

Status of this Memo

Copyright Notice

Abstract

syslog specifies both a logging format and a set of protocols to communicate that format over. This memo specifies a set of URIs that administrators and configuration systems may use to inform syslog senders of their collectors or relays and protocols.

1. Introduction

The syslog protocol [1] has been used as a logging mechanism for close to three decades, in one form or another. Its reach has extended from UNIX mail systems to printers to routers to many different devices. In many cases the logging configuration is as simple as an IP address. This configuration may be in a file, specified by an administrator on a device console, or perhaps retrieved by a device through a configuration protocol, such as DHCP [8].

With the formal specification of the syslog transport protocols for UDP [3], TLS [2], and BEEP [4], a simple means is needed to provide a concise way to tell systems which host and which protocol to use as either a collector or relay. Universal Resource Identifiers (URIs) [5] provide a flexible and concise means to accomplish this task.

This memo specifies three such URIs. They are "syslog.udp", "syslog.tls", and "syslog.beep;". A description of each URI scheme follows in the next section. It is recommended that future syslog transports include an appropriate URI scheme that begins with "syslog.".

syslog terminology used in this draft is taken from [1].

2. syslog URI Scheme Registrations and Description

Each section below consists of a completed template from RFC 4395 [6].

2.1. syslog.udp Schema Registration

URI scheme name

syslog.udp

Status

Permanent

Syntax

The following syntax makes use of Augmented BNF (ABNF) [7] and the definitions found in RFC 3986.

```
syslog-udp-uri = "syslog.udp:" host [ ":" port ]
```

URI semantics

This URI is used to specify a syslog collector or relay running over a specific UDP port. syslog senders will make a connection to the host and transmit any appropriate logging as prescribed by the sender's configuration.

Encoding Considerations

As only a host and a port number are provided, encoding of these portions of the URI are specified in [5].

Applications/protocols that use this URI scheme name

syslog senders will primarily make use of this URI to configure themselves. The syslog protocol is specified in [1]. UDP transport of syslog is specified in [3].

Interoperability considerations

None

Security Considerations

[3] discusses the underlying concerns of syslog over udp. Additionally, as URIs tend to be portable, some additional concern should be given to protecting the host in a syslog.udp URI from unauthorized access.

Contact

The author section of this document.

Author/Change Control

The author of this scheme is the same as in the author section of this document. Change control is vested with the IESG.

References

Please see the References section of this document.

2.2. syslog.tls Schema Registration

URI scheme name

syslog.tls

Status

Permanent

Syntax

The following syntax makes use of ABNF and the definitions found in RFC 3986.

```
 syslog-tls-uri = "syslog.tls:" host [ ":" port ]
```

URI semantics

This URI is used to specify a syslog collector or relay running over TLS. syslog senders will make a connection to the host, initiate TLS, and transmit any appropriate logging as prescribed by the sender's configuration over the encrypted channel.

Encoding Considerations

As only a host and a port number are provided, encoding of these portions of the URI are specified in [5].

Applications/protocols that use this URI scheme name

syslog senders will primarily make use of this URI to configure themselves. The syslog protocol is specified in [1]. TLS transport of syslog is specified in [2].

Interoperability considerations

None

Security Considerations

[2] discusses issues and concerns of using syslog over TLS. Additionally, as URIs tend to be portable, some additional concern should be given to protecting the host in a syslog.tls URI from unauthorized access.

Contact

The author section of this document.

Author/Change Control

The author of this scheme is the same as in the author section of this document. Change control is vested with the IESG.

References

Please see the References section of this document.

2.3. syslog.beep Schema Registration

URI scheme name

syslog.beep

Status

Permanent

Syntax

The following syntax makes use of ABNF and the definitions found in RFC 3986.

```
syslog-beep-uri = "syslog.beep:" host [ ":" port ]
```

URI semantics

This URI is used to specify a syslog collector or relay running over BEEP. syslog senders will make a TCP connection to the host, utilize an appropriate BEEP profile for syslog, and transmit any appropriate logging as prescribed by the sender's configuration over the BEEP channel.

Encoding Considerations

As only a host and a port number are provided, encoding of these portions of the URI are specified in [5].

Applications/protocols that use this URI scheme name

syslog senders will primarily make use of this URI to configure themselves. The syslog protocol is specified in [4]. BEEP transport of syslog is specified in [4].

Interoperability considerations

None

Security Considerations

[4] discusses issues and concerns of using syslog over BEEP. Additionally, as URIs tend to be portable, some additional concern should be given to protecting the host in a syslog.beep URI from unauthorized access.

Contact

The author section of this document.

Author/Change Control

The author of this scheme is the same as in the author section of this document. Change control is vested with the IESG.

References

Please see the References section of this document.

3. Operational Considerations

Use of a URI to configure the syslog service requires some thought about potential circular dependencies. For instance, if a domain name is used to configure the service, the URI cannot be resolved if name service is unavailable. Implementers are reminded to obey the rules set forth in Section 3.2.2 of [5]. Administrators must balance the requirements of flexible management against the need for logging resiliency, when making use of these URIs. In some cases devices may be able to store messages locally until they are able to resolve the address of a collector or relay. In other cases, logging information may be time critical.

4. Security Considerations

Please see the above sections as well as the underlying protocol documents for security considerations. Use of this URI to configure devices should be considered in the same light as other potentially sensitive configuration information. The underlying content being logged may or may not warrant additional protections, depending on environment and circumstances.

5. IANA Considerations

The IANA is requested to register the profiles in Section 2.

6. References

6.1. Normative References

[1] Gerhards, R., "The syslog Protocol", draft-ietf-syslog-protocol-19 (work in progress), November 2006.

[2] Miao, F. and M. Yuzhi, "TLS Transport Mapping for Syslog", draft-ietf-syslog-transport-tls-07 (work in progress), April 2007.

[3] Okmianski, A., "Transmission of syslog messages over UDP", draft-ietf-syslog-transport-udp-09 (work in progress), March 2007.

[4] Lear, E., "Reliable Delivery for syslog", draft-lear-ietf-syslog-rfc3195bis-00 (work in progress), February 2007.

[5] Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax", STD 66, RFC 3986, January 2005.

[6] Hansen, T., Hardie, T., and L. Masinter, "Guidelines and Registration Procedures for New URI Schemes", BCP 115, RFC 4395, February 2006.

[7] Crocker, D., Ed. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", RFC 4234, October 2005.

6.2. Informational References

[8] Droms, R., "Dynamic Host Configuration Protocol", RFC 2131, March 1997.

Appendix A. Changes

This seciton to be removed prior to publication.
o 00 Initial Revision.

Author's Address

Eliot Lear
Cisco Systems GmbH
Glatt-com
Glattzentrum, ZH CH-8301
Switzerland

Phone: +41 1 878 7525
Email: lear@cisco.com

Full Copyright Statement

Intellectual Property

Acknowledgments

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA). This document was produced using xml2rfc v1.32 (of http://xml.resource.org/) from a source in RFC-2629 XML format.