Internet Engineering Task Force
Internet-Draft
Updates: 4120 (if approved)
Intended status: Standards Track
Expires: November 17, 2016

N. McCallum
Red Hat, Inc.

May 16, 2016

Kerberos Service Discovery using DNS
draft-mccallum-kitten-krb-service-discovery-02

Abstract

This document proposes defines a new mechanism for discovering Kerberos services using DNS. This new mechanism extends the mechanism already defined in Kerberos V5 [RFC4120] and has four goals. First, reduce the number of DNS queries required to discover a Kerberos KDC. Second, provide DNS administrators more control over client behavior. Third, provide support for discovery of the MS-KKDCP transport. Fourth, define a discovery procedure for Kerberos password services.

Status of This Memo

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

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

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."

This Internet-Draft will expire on November 17, 2016.

Copyright Notice

Table of Contents

1. Introduction

Section 7.2.3 of Kerberos V5 [RFC4120] defines a procedure for discovering a KDC based on DNS SRV records. This method has three drawbacks. First, two DNS queries are required to locate a single service (one for UDP and one for TCP). Second, specifying UDP and TCP in separate records means that the DNS administrator has no control over client preferences for TCP or UDP. Third, any new transports for reaching the KDC (such as MS-KKDCP) will require new records and additional DNS queries.

The Kerberos Password [RFC3244] protocol has no defined procedure for discovery similar to the KDC method described above. Implementations have largely chosen a similar method to section 7.2.3 of Kerberos V5 [RFC4120], inheriting the same drawbacks outlined above.

This RFC defines two new URI DNS records [RFC7553]; one each for KDC and Kerberos Password service discovery.

2. Document Conventions

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. Realm to Domain Translation

This document does not define a new mechanism for translating Kerberos realms to DNS domains. The existing mechanism as defined in section 7.2.3.1 of Kerberos V5 [RFC4120] MUST be followed.

4. Required URI Formats

The following URI formats MUST be supported by clients. These formats indicate support for the standard UDP and TCP transports. The port number is optional. If the port is not specified, the client MUST default to the standard port of the service (Kerberos V5 or Kerberos Password).

udp://host[:port]

tcp://host[:port]

5. Optional URI Formats

The following URI formats MAY be supported by clients.

5.1. MS-KKDCP

These URIs indicate support for the MS-KKDCP [MS-KKDCP] protocol. The port number is optional. If the port is not specified, the client MUST default to the standard port of the transport (HTTP or HTTPS). The path is also optional.

http://host[:port][path]

https://host[:port][path]

6. Kerberos V5 KDC Service Discovery

In order to discover a KDC service location, the client MUST query the following URI DNS [RFC7553] record (REALM indicates the translation of the Kerberos realm to a DNS domain):

_kerberos.REALM

TTL, Class, URI, Priority, Weight and Target have the standard meanings as defined in RFC 2782 [RFC2782] and the URI DNS record type [RFC7553]. Target SHOULD contain one of the URI formats specified in this document.

7. Kerberos Password Service Discovery

In order to discover a password service location, the client MUST query the following URI DNS [RFC7553] record (REALM indicates the translation of the Kerberos realm to a DNS domain):

_kpasswd.REALM

TTL, Class, URI, Priority, Weight and Target have the standard meanings as defined in RFC 2782 [RFC2782] and the URI DNS record type [RFC7553]. Target SHOULD contain one of the URI formats specified in this document.

8. Relationship to Existing Mechanism

If an existing discovery protocol is supported by a client, the client SHOULD perform the URI lookup as defined in this document first. If no URI record is found, the client MAY attempt discovery using another protocol.

9. Normative References

[MS-KKDCP] Microsoft, "[MS-KKDCP]: Kerberos Key Distribution Center (KDC) Proxy Protocol", May 2014, <http://msdn.microsoft.com/en-us/library/hh553774.aspx>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

[RFC2782] Gulbrandsen, A., Vixie, P., and L. Esibov, "A DNS RR for specifying the location of services (DNS SRV)", RFC 2782, DOI 10.17487/RFC2782, February 2000, <http://www.rfc-editor.org/info/rfc2782>.

[RFC3244] Swift, M., Trostle, J., and J. Brezak, "Microsoft Windows 2000 Kerberos Change Password and Set Password Protocols", RFC 3244, DOI 10.17487/RFC3244, February 2002, <http://www.rfc-editor.org/info/rfc3244>.

[RFC4120] Neuman, C., Yu, T., Hartman, S., and K. Raeburn, "The Kerberos Network Authentication Service (V5)", RFC 4120, DOI 10.17487/RFC4120, July 2005, <http://www.rfc-editor.org/info/rfc4120>.

[RFC7553] Faltstrom, P. and O. Kolkman, "The Uniform Resource Identifier (URI) DNS Resource Record", RFC 7553, DOI 10.17487/RFC7553, June 2015, <http://www.rfc-editor.org/info/rfc7553>.

Appendix A. Acknowledgements

Simo Sorce (Red Hat)
Nico Williams (Cryptonector)

Author's Address

Nathaniel McCallum
Red Hat, Inc.
100 East Davie Street
Raleigh, NC 27601
USA

EMail: npmccallum@redhat.com