Internet Engineering Task Force
Internet-Draft
Updates: 4120 (if approved)
Intended status: Standards Track
Expires: March 27, 2017

N. McCallum
M. Rogers
Red Hat, Inc.

September 23, 2016

Kerberos Service Discovery using DNS
draft-mccallum-kitten-krb-service-discovery-03

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 March 27, 2017.

Copyright Notice

Table of Contents

1. Introduction 2
2. Document Conventions 3
3. Realm to Domain Translation 3
4. Required URI Format 3
4.1. Scheme 3
4.2. Flags 3
4.2.1. Master Flag 4
4.3. Transport 4
4.4. Residual 4
5. Kerberos V5 KDC Service Discovery 4
6. Kerberos Password Service Discovery 4
7. Kerberos Admin Service Discovery 5
8. Relationship to Existing Mechanism 5
9. IANA Considerations 5
9.1. Kerberos Server Discovery Flags 5
9.1.1. Registration Template 5
9.1.2. Initial Registry Contents 6
9.2. Kerberos Server Discovery Transport Types 6
9.2.1. Registration Template 6
9.2.2. Initial Registry Contents 6
10. Appendix 7
10.1. URI Format Examples 7
11. Normative References 7
Appendix A. Acknowledgements 9
Authors' Addresses 9

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 three new URI DNS records [RFC7553]; one each for KDC, Kerberos Password, and Kerberos Admin 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 Format

The following URI format MUST be supported by clients.

The URI format is comprised of text fields delimited by a colon (":") character.

krb5srv:[flags]:transport:residual

See the Appendix for examples.

4.1. Scheme

This field identifies the URI scheme. Its value MUST be the string "krb5srv".

4.2. Flags

This field contains a sequence of zero or more case-insensitive characters used individually to convey server attributes or feature support (eg. "XYZ" indicates support for features X, Y, and Z.) for the purpose of organizing the lookup results.

This field MUST be present even when no flags are provided, appearing as two colons seperating the scheme and transport fields (eg. "krb5srv::tcp:host").

Flags are not considered critical, therefore flags that are not used or unknown to the implementation SHOULD be ignored.

4.2.1. Master Flag

The "m" flag signifies that the discovered server is a master server. The client SHOULD consider this server as one that would immediately see password changes and use it as a fallback for incorrect password errors.

4.3. Transport

This field contains a string to indicate the transport method to use when contacting the host specified in the URI.

4.4. Residual

This field contains information specific to the transport. It may contain sub-fields where such are defined in the transport specification.

5. 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.

6. 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.

7. Kerberos Admin Service Discovery

In order to discover an admin 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-adm.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. IANA Considerations

This document establishes two registries with the following procedure, in accordance with [RFC5226]:

Registry entries are to be evaluated using the Specification Required method. All specifications must be be published prior to entry inclusion in the registry. There will be a three-week review period by Designated Experts on the kitten@ietf.org mailing list. Prior to the end of the review, the Designated Experts must approve or deny the request. This decision is to be conveyed to both the IANA and the list, and should include reasonably detailed explanation in the case of a denial as well as whether the request can be resubmitted.

9.1. Kerberos Server Discovery Flags

This section species the IANA "Kerberos Server Discovery Flags" registry. This registry records the value and description for each flag.

9.1.1. Registration Template

Value: A single unique ASCII character that identifies the entry, excluding the colon character (":") since it is used as a field delimiter in the scheme outlined in this document.

Description: A brief description of the meaning of the value when it appears in the flags field.

Reference: A reference to the details of the flag.

9.1.2. Initial Registry Contents

- Value: m
- Description: The target is a master server.
- Reference: TBD

9.2. Kerberos Server Discovery Transport Types

This section specifies the IANA "Kerberos Server Discovery Transport Types" registry. This registry records the value, description, residual format, case-sensitive residual elements, default ports, and a reference for each type.

9.2.1. Registration Template

Value: A unique value to identify the transport type within the transport field.

Description: The name or description of the transport type.

Residual Format: The format of the residual field that specifies the discovered target URL. Optional parts of the URL are enclosed in brackets.

Case Sensitive: If any part of the residual format is case-sensitive, it is specified here.

Default KDC Port: A number in the range of 1-65535 as the port used to contact the target URL when no port is specified and the lookup result is for a Kerberos server.

Default Admin Service Port: A number in the range of 1-65535 as the port used to contact the target URL when no port is specified and the lookup result is for a Kerberos Admin server.

Default Password Service Port: A number in the range of 1-65535 as the port used to contact the target URL when no port is specified and the lookup result is for a Kerberos Password server.

Reference: A reference to the details of the transport type.

9.2.2. Initial Registry Contents

- Value: "udp"
- Description: User Datagram Protocol
- Residual Format: "host[:port]"
- Case Sensitive: None
- Default KDC Port: 88
- Default Admin Service Port: 749
- Default Password Service Port: 464
- Reference: [RFC0768]

- Value: "tcp"
- Description: Transport Control Protocol
- Residual Format: "host[:port]"
- Case Sensitive: None
- Default KDC Port: 88
- Default Admin Service Port: 749
- Default Password Service Port: 464
- Reference: [RFC0793]

- Value: "kkdcp"
- Description: Kerberos Key Distribution Center Proxy Protocol
- Residual Format: https://host[:port][/path]
- Case Sensitive: [/path]
- Default KDC Port: 443
- Default Admin Service Port: 443
- Default Password Service Port: 443
- Reference: [MS-KKDCP]

10. Appendix

10.1. URI Format Examples

- krb5srv:m:kkdcp:https://kdc.example.com:8080/path
- krb5srv:m:udp:kdc.example.com
- krb5srv::kkdcp:https://kdc2.example.com/path
- krb5srv::tcp:192.168.1.20:1000

11. 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>.

[RFC0768] Postel, J., "User Datagram Protocol", STD 6, RFC 768, DOI 10.17487/RFC0768, August 1980, <http://www.rfc-editor.org/info/rfc768>.

[RFC0793] Postel, J., "Transmission Control Protocol", STD 7, RFC 793, DOI 10.17487/RFC0793, September 1981, <http://www.rfc-editor.org/info/rfc793>.

[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>.

[RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 5226, DOI 10.17487/RFC5226, May 2008, <http://www.rfc-editor.org/info/rfc5226>.

[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)

Authors' Addresses

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

EMail: npmccallum@redhat.com

Matt Rogers
Red Hat, Inc.
100 East Davie Street
Raleigh, NC 27601
USA

EMail: mrogers@redhat.com