Network Working Group
Request for Comments: 5179
Category: Standards Track

N. Williams
Sun

May 2008

Generic Security Service Application Program Interface (GSS-API) Domain-Based Service Names Mapping for the Kerberos V GSS Mechanism

Status of This Memo

Abstract

This document describes the mapping of Generic Security Service Application Program Interface (GSS-API) domain-name-based service principal names onto Kerberos V principal names.

Table of Contents

1. Domain-Based Names for the Kerberos V GSS-API Mechanism

In accordance with [RFC5178], this document provides the mechanism-specific details needed to implement GSS-API [RFC2743] domain-based service names with the Kerberos V GSS-API mechanism [RFC4121].

GSS_C_NT_DOMAINBASED_SERVICE name SHOULD be mapped to Kerberos V principal names as follows:

- the <service> name becomes the first (0th) component of the Kerberos V principal name;
- the <hostname> becomes the second component of the Kerberos V principal name;
- the <domain> name becomes the third component of the Kerberos V principal name;
- the realm of the resulting principal name is that which corresponds to the domain name, treated as a hostname.

The same name canonicalization considerations and methods as used elsewhere in the Kerberos V GSS-API mechanism [RFC4121] and Kerberos V [RFC4120] in general apply here.

Implementations SHOULD use a Kerberos V name-type of NTT-SRVT-HST-DOMAIN (which has the value 12) but MAY use NT-UNKNOWN instead.

2. Conventions Used in This Document

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 [RFC2119].

3. Internationalization Considerations

It is unclear, at this time, how best to address internationalization of Kerberos V domain-based principal names. This is because the Kerberos V core protocol internationalization project is incomplete.

However, clearly the best way to interoperate when using Kerberos V domain-based principal names is to use ACE-encoded internationalized domain names [RFC3490] for the hostname and domain name slots of a Kerberos V domain-based principal name. Therefore Kerberos V GSS-API mechanism implementations MUST do just that.

4. Examples

- The domain-based name, of generic form, "ldap@foo.example@ds1.foo.example" may map to a Kerberos V principal name like: "ldap/ds1.foo.example/foo.example@FOO.EXAMPLE"

- The domain-based name, of generic form, "kadmin@foo.example@kdc1.foo.example" may map to a Kerberos V principal name like: "kadmin/kdc1.foo.example/foo.example@FOO.EXAMPLE"

5. Security Considerations

See [RFC5178].

It is important for the security of protocols using the Kerberos V GSS-API mechanism and domain-based names, that the realm of domain-based principal names be derived from the hostname, rather than the domain name slots of the input domain-based name string.

6. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2743] Linn, J., "Generic Security Service Application Program Interface Version 2, Update 1", RFC 2743, January 2000.

[RFC3490] Faltstrom, P., Hoffman, P., and A. Costello, "Internationalizing Domain Names in Applications (IDNA)", RFC 3490, March 2003.

[RFC4120] Neuman, C., Yu, T., Hartman, S., and K. Raeburn, "The Kerberos Network Authentication Service (V5)", RFC 4120, July 2005.

[RFC4121] Zhu, L., Jaganathan, K., and S. Hartman, "The Kerberos Version 5 Generic Security Service Application Program Interface (GSS-API) Mechanism: Version 2", RFC 4121, July 2005.

[RFC5178] Williams, N. and A. Melnikov, "Generic Security Service Application Program Interface (GSS-API) Internationalization and Domain-Based Service Names and Name Type", RFC 5178, May 2008.

Author's Address

Nicolas Williams
Sun Microsystems
5300 Riata Trace Ct.
Austin, TX 78727
US

EMail: Nicolas.Williams@sun.com

Full Copyright Statement

Intellectual Property