NETWORK WORKING GROUP
Internet-Draft
Expires: July 27, 2008

N. Williams
Sun

January 24, 2008

GSS-API Domain-Based Service Names Mapping for the Kerberos V GSS Mechanism

draft-ietf-kitten-krb5-gssapi-domain-based-names-05.txt

Status of this Memo

Copyright Notice

Abstract

This document describes the mapping of GSS-API domainname-based service principal names onto Kerberos V principal names.

Table of Contents

1. 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].

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

In accordance with [I-D.ietf-kitten-gssapi-domain-based-names] 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 NT-SRV-HST-DOMAIN (integral value to be assigned, possibly after WGLC?) but MAY use NT-UNKNOWN instead.

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 [I-D.ietf-kitten-gssapi-domain-based-names].

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

[I-D.ietf-kitten-gssapi-domain-based-names]
Williams, N. and A. Melnikov, "GSS-API Internationalization and Domain-Based Service Names and Name Type", draft-ietf-kitten-gssapi-domain-based-names-05 (work in progress), December 2007.

[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.

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

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).