Internet Engineering Task Force (IETF)
Request for Comments: 6111
Updates: 4120
Category: Standards Track
ISSN: 2070-1721

L. Zhu
Microsoft Corporation

April 2011

Additional Kerberos Naming Constraints

Abstract

This document defines new naming constraints for well-known Kerberos principal names and well-known Kerberos realm names.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc6111.

Table of Contents

1. Introduction

Occasionally, protocol designers need to designate a Kerberos principal name or a Kerberos realm name to have a special meaning other than identifying a particular instance. An example is that the anonymous principal name and the anonymous realm name are defined for the Kerberos anonymity support [RFC6112]. This anonymity name pair conveys no more meaning than that the client’s identity is not disclosed. In the case of the anonymity support, it is critical that deployed Kerberos implementations that do not support anonymity fail the authentication if the anonymity name pair is used; therefore, no access is granted accidentally to a principal who’s name happens to match with that of the anonymous identity.

However, Kerberos, as defined in [RFC4120], does not have such reserved names. As such, protocol designers have resolved to use names that are exceedingly unlikely to have been used to avoid collision. Even if a registry were set up to avoid collision of new implementations, there is no guarantee for deployed implementations preventing accidental reuse of names that can lead to access being granted unexpectedly.

The Kerberos realm name in [RFC4120] has a reserved name space although no specific name is defined and the criticality of unknown reserved realm names is not specified.

This document remedies these issues by defining well-known Kerberos names and the protocol behavior when a well-known name is used but not supported.

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. Definitions

In this section, well-known names are defined for both the Kerberos principal name and the Kerberos realm name.

3.1. Well-Known Kerberos Principal Names

A new name type KRB_NT_WELLKNOWN is defined for well-known principal names. The Kerberos principal name is defined in Section 6.2 of [RFC4120].

```
KRB_NT_WELLKNOWN                11
```

A well-known principal name MUST have at least two or more KerberosString components, and the first component MUST be the string literal "WELLKNOWN".

If a well-known principal name is used as the client principal name or the server principal name but not supported, the Authentication Service (AS) [RFC4120] and the application server MUST reject the authentication attempt. Similarly, the Ticket Granting Service (TGS) [RFC4120] MAY reject the authentication attempt if a well-known principal name is used as the client principal name but not supported, and SHOULD reject the authentication attempt if a well-known principal name is used as the server principal name but not supported. These rules were designed to allow incremental updates and ease migration. More specifically, if a well-known principal is accepted in one realm, it is desirable to allow the cross-realm Ticket Granting Ticket (TGT) to work when not all of the realms in the cross-realm authentication path are updated; if the server principal with an identically named well-known name was created before the Key Distribution Center (KDC) is updated, it might be acceptable to allow authentication to work within a reasonably limited time window. However, unless otherwise specified, if a well-

known principal name is used but not supported in any other places of Kerberos messages, authentication MUST fail. The error code is KRB_AP_ERR_PRINCIPAL_UNKNOWN, and there is no accompanying error data defined in this document for this error.

```
KRB_AP_ERR_PRINCIPAL_UNKNOWN      82
     -- A well-known Kerberos principal name is used but not
     -- supported.
```

3.2. Well-Known Kerberos Realm Names

Section 6.1 of [RFC4120] defines the "other" style of realm name, a new realm type WELLKNOWN is defined as a name of type "other", with the NAMETYPE part filled in with the string literal "WELLKNOWN".

```
other: WELLKNOWN:realm-name
```

This name type is designated for well-known Kerberos realms.

The AS and the application server MUST reject the authentication attempt if a well-known realm name is used as the client realm or the server realm but not supported. The TGS [RFC4120] MAY reject the authentication attempt if a well-known realm name is used as the client realm but not supported, and it SHOULD reject the authentication attempt if a well-known realm name is used as the server realm but not supported. Unless otherwise specified, if a well-known realm name is used but not supported in any other places of Kerberos messages, authentication MUST fail. The error code is KRB_AP_ERR_REALM_UNKNOWN, and there is no accompanying error data defined in this document for this error.

```
KRB_AP_ERR_REALM_UNKNOWN          83
     -- A well-known Kerberos realm name is used but not
     -- supported.
```

Unless otherwise specified, all principal names involving a well-known realm name are reserved, and if a reserved principal name is used but not supported, and if the authentication is rejected, the error code MUST be KRB_AP_ERR_PRINCIPAL_RESERVED.

```
KRB_AP_ERR_PRINCIPAL_RESERVED     84
     -- A reserved Kerberos principal name is used but not
     -- supported.
```

There is no accompanying error data defined in this document for this error.

According to Section 3.3.3.2 of [RFC4120], the TGS MUST add the name of the previous realm into the transited field of the returned ticket. Typically, well-known realms are defined to carry special meanings, and they are not used to refer to intermediate realms in the client's authentication path. Consequently, unless otherwise specified, the TGS MUST NOT encode a well-known Kerberos realm name into the transited field [RFC4120] of a ticket, and parties checking the transited realm path MUST reject a transited realm path that includes a well-known realm. In the case of KDCs checking the transited realm path, this means that the TRANSITED-POLICY-CHECKED flag MUST NOT be set in the resulting ticket. Aside from the hierarchical meaning of a null subfield, the DOMAIN-X500-COMPRESS encoding for transited realms [RFC4120] treats realm names as strings, although it is optimized for domain style and X.500 realm names; hence, the DOMAIN-X500-COMPRESS encoding can be used when the client realm or the server realm is reserved or when a reserved realm is in the transited field. However, if the client's realm is a well-known realm, the abbreviation forms [RFC4120] that build on the preceding name cannot be used at the start of the transited encoding. The null-subfield form (e.g., encoding ending with ",") [RFC4120] could not be used next to a well-known realm, including potentially at the beginning and end where the client and server realm names, respectively, are filled in.

4. Security Considerations

It is possible to have a name collision with well-known names because Kerberos, as defined in [RFC4120], does not reserve names that have special meanings; accidental reuse of names MUST be avoided. If a well-known name is not supported, authentication MUST fail as specified in Section 3. Otherwise, access can be granted unintentionally, resulting in a security weakness. Consider, for example, a KDC that supports this specification but not the anonymous authentication described in [RFC6112]. Assume further that the KDC allows a principal to be created named identically to the anonymous principal. If that principal were created and given access to resources, then anonymous users might inadvertently gain access to those resources if the KDC supports anonymous authentication at some future time. Similar issues may occur with other well-known names. By requiring that KDCs reject authentication with unknown well-known names, we minimize these concerns.

If a well-known name was created before the KDC is updated to conform to this specification, it SHOULD be renamed. The provisioning code that manages account creation MUST be updated to disallow creation of principals with unsupported well-known names.

5. Acknowledgements

The initial document was mostly based on the author's conversation with Clifford Newman and Sam Hartman.

Jeffrey Hutzelman, Ken Raeburn, and Stephen Hanna provided helpful suggestions for improvements to early revisions of this document.

6. IANA Considerations

This document provides the framework for defining well-known Kerberos names and Kerberos realms. Two new IANA registries have been created to contain well-known Kerberos principal names and Kerberos realm names that are defined based on this document. The evaluation policy for each is "Specification Required", as specified in [RFC5226].

7. References

7.1. Normative References

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

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

[RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 5226, May 2008.

7.2. Informative References

[RFC6112] Zhu, L., Leach, P., and S. Hartman, "Anonymity Support for Kerberos", RFC 6112, April 2011.

Author's Address

Larry Zhu
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052
US

EMail: lzhu@microsoft.com