Network Working Group
Request for Comments: 3494
Obsoletes: 1484, 1485, 1487, 1488, 1777, 1778, 1779, 1781, 2559
Category: Informational

K. Zeilenga
OpenLDAP Foundation

March 2003

Lightweight Directory Access Protocol version 2 (LDAPv2) to Historic Status

Status of this Memo

Copyright Notice

Abstract

This document recommends the retirement of version 2 of the Lightweight Directory Access Protocol (LDAPv2) and other dependent specifications, and discusses the reasons for doing so. This document recommends RFC 1777, 1778, 1779, 1781, and 2559 (as well as documents they superseded) be moved to Historic status.

Lightweight Directory Access Protocol, version 2

LDAPv2 (Lightweight Directory Access Protocol, version 2) [RFC1777][RFC1778][RFC1779] is an Internet Protocol used to access X.500-based directory services. This document recommends that LDAPv2 and other dependent specifications be retired. Specifically, this document recommends RFC 1777, 1778, 1779, 1781, and 2559 (as well as documents they superseded) be moved to Historic status. The reasons for taking this action are discussed below.

LDAPv2 was published in 1995 as a Draft Standard. Since its publication, a number of inadequacies in the specification have been discovered. LDAPv3 [RFC3377] was published in 1997 as a Proposed Standard to resolve these inadequacies. While LDAPv3 is currently being revised [LDAPbis], it is clearly technically superior to LDAPv2.

The LDAPv2 specification is not generally adhered to; that is, an independently developed implementation of the specification would not interoperate with existing implementations, as existing

implementations use syntaxes and semantics different than those prescribed by the specification. Below are two examples.

1) Existing LDAPv2 implementations do not commonly restrict textual values to IA5 (ASCII) and T.61 (Teletex) as required by RFC 1777 and RFC 1778. Some existing implementations use ISO 8859-1, others use UCS-2, others use UTF-8, and some use the current local character set.

2) RFC 1777 requires use of the textual string associated with AttributeType in the X.500 Directory standards. However, existing implementations use the NAME associated with the AttributeType in the LDAPv3 schema [RFC2252]. That is, LDAPv2 requires the organization name attribute be named "organizationName", not "o".

In addition, LDAPv2 does not provide adequate security features for use on the Internet. LDAPv2 does not provide any mechanism for data integrity or confidentiality. LDAPv2 does not support modern authentication mechanisms such as those based on DIGEST-MD5, Kerberos V, and X.509 public keys.

Dependent Specifications

Since the publication of RFC 1777, 1778, and 1779, there have been additional standard track RFCs published that are dependent on these technical specifications, including:

"Using the OSI Directory to Achieve User Friendly Naming" [RFC1781]

and

"Internet X.509 Public Key Infrastructure Operational Protocols - LDAPv2" [RFC2559].

RFC 1781 is a technical specification for "User Friendly Naming" which replies on particular syntaxes described in RFC 1779. RFC 2253, which replaced RFC 1779, eliminated support for the "User Friendly Naming" syntaxes. RFC 1781 is currently a Proposed Standard.

RFC 2559 is primarily an applicability statement for using LDAPv2 in providing Public Key Infrastructure. It depends on RFC 1777 and updates RFC 1778. If LDAPv2 is moved to Historic status, so must this document. RFC 2559 is currently a Proposed Standard.

Security Considerations

LDAPv2 does not provide adequate security mechanisms for general use on the Internet. LDAPv3 offers far superior security mechanisms, including support for strong authentication and data confidentiality services. Moving LDAPv2 to Historic may improve the security of the Internet by encouraging implementation and use of LDAPv3.

Recommendations

Developers should not implement LDAPv2 per RFC 1777, as such would result in an implementation that will not interoperate with existing LDAPv2 implementations. Developers should implement LDAPv3 instead.

Deployers should recognize that significant interoperability issues exist between current LDAPv2 implementations. LDAPv3 is clearly technically superior to LDAPv2 and hence should be used instead.

It is recommended that RFC 1777, RFC 1778, RFC 1779, RFC 1781, and RFC 2559 be moved to Historic status.

The previously superseded specifications RFC 1484, 1485, 1487, and 1488 (by RFC 1781, 1779, 1777, and 1778, respectively) should also be moved to Historic status.

Acknowledgment

The author would like to thank the designers of LDAPv2 for their contribution to the Internet community.

Normative References

[RFC1777] Yeong, W., Howes, T. and S. Kille, "Lightweight Directory Access Protocol", RFC 1777, March 1995.

[RFC1778] Howes, T., Kille, S., Yeong, W. and C. Robbins, "The String Representation of Standard Attribute Syntaxes", RFC 1778, March 1995.

[RFC1779] Kille, S., "A String Representation of Distinguished Names", RFC 1779, March 1995.

[RFC1781] Kille, S., "Using the OSI Directory to Achieve User Friendly Naming", RFC 1781, March 1995.

[RFC2559] Boeyen, S., Howes, T. and P. Richard, "Internet X.509 Public Key Infrastructure Operational Protocols - LDAPv2", RFC 2559, April 1999.

Informative References

[LDAPbis] IETF LDAP Revision (v3) Working Group (LDAPbis), <http://www.ietf.org/html-charters/ldapbis-charter.html>.

[RFC3377] Hodges, J. and R. Morgan, "Lightweight Directory Access Protocol (v3): Technical Specification", RFC 3377, September 2002.

[RFC2252] Wahl, M., Coulbeck, A., Howes, T. and S. Kille, "Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions", RFC 2252, December 1997.

[RFC2253] Wahl, M., Kille, S. and T. Howes, "Lightweight Directory Access Protocol (v3): UTF-8 String Representation of Distinguished Names", RFC 2253, December 1997.

Author’s Address

Kurt D. Zeilenga
OpenLDAP Foundation

EMail: Kurt@OpenLDAP.org

Full Copyright Statement

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.