Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: May 21, 2007

M. Wahl
Informed Control Inc.

November 17, 2006

LDAP Administrator Address Attribute
draft-wahl-ldap-adminaddr-04

Status of this Memo

Copyright Notice

Abstract

Organizations with multiple or outsourced directory servers need the ability for administrators to determine who is responsible for a particular directory server. This document defines an attribute with contact information for a directory server's responsible party, conceptually similar to the 'sysContact' object of SNMP, which can be retrieved from the directory server using the Lightweight Directory Access Protocol.

1. Introduction

This document defines an attribute type, administratorsAddress, for use in LDAP [1] directory deployments.

The values of this this attribute are used to provide contact information of the responsible party for an LDAP server, or of the responsible party for a naming context within a LDAP server.

This attribute is intended to be used by management tools that are LDAP clients. For example, a management tool for checking the state of a replication or referral topology might use this attribute to send email to the manager of a particular server when it detects an error.

(This attribute type was originally defined in the mid-1990s for inclusion in the LDAPv3 data model, but was omitted from the LDAPv3 root DSE specification as there was only one implementation of a server supporting that attribute at that time.)

The words "MUST", "SHOULD" and "MAY" are used as defined in RFC 2119 [2].

Please send comments to the author at mark.wahl@informed-control.com.

2. The administratorsAddress attribute

The attribute type is defined as follows (with lines wrapped for readability):

```
( 1.3.6.1.4.1.1466.101.120.1 NAME 'administratorsAddress'
 SYNTAX 1.3.6.1.4.1.1466.115.121.1.26
 USAGE directoryOperation )
```

Attributes of this type can contain one or more values, and each value is a URI [3]. Each URI is encoded using the IA5 string syntax [4].

Unlike the labeledURI attribute [6], these values do not have a label.

In existing practice, this URI can be of the 'mailto:' form identifying a personal or role email address, such as "mailto:helpdesk@example.com".

To obtain the responsible party for a directory server, the attribute is read from the root DSE, using a baseObject search requesting this attribute by returned, as described in RFC 4512 [5].

To obtain the responsible party for a naming context, the attribute is read from the entry at the base of the naming context, using a baseObject search requesting this attribute be returned. Note that these addresses need not be the same as that of the directory server administrator, or of a data administrator.

This document only specifies how a client can read this attribute. Some servers MAY support updating this attribute over protocol, subject to access control. Other servers might instead provide this value read only, if it is configured through the server's out-of-band management interface, such as in a configuration file.

3. Security Considerations

The server's access control policy SHOULD allow this information to be visible to a suitable administrator in the same organization. Since one use of this attribute is to find who is responsible if the server is not making authentication decisions properly, a directory server configuration SHOULD cause the attribute in the root DSE, if present, to be able to be returned in a search response to all users who are permitted to access the directory server. The administrator SHOULD choose addresses for use in this attribute that are already publicly known within the organization, and SHOULD NOT encode passwords or other secret information within the URIs.

4. IANA Considerations

The LDAP Parameter registration for this attribute has already been reviewed by the Directorate and processed by IANA. This attribute object identifier is registered as follows:

Descriptor: administratorsAddress

Object Identifier: 1.3.6.1.4.1.1466.101.120.1

Person & email address to contact for further information:
Mark Wahl <Mark.Wahl@informed-control.com>

Usage: attribute type

Author/Change Controller: Mark Wahl

5. Acknowledgments

The contents of this document is based on earlier work of the ASID Working Group of the IETF. The contributions of its members is greatly appreciated.

6. References

6.1. Normative References

[1] Zeilenga, K., "Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map", RFC 4510, June 2006.

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

[3] Berners-Lee, T., "Uniform Resource Identifier (URI): Generic Syntax", RFC 1738, STD 66, January 2005.

[4] Legg, S., "Lightweight Directory Access Protocol (LDAP): Syntaxes and Matching Rules", RFC 4517, June 2006.

[5] Zeilenga, K., "Lightweight Directory Access Protocol (LDAP): Directory Information Models", RFC 4512, June 2006.

6.2. Informative References

[6] Smith, M., "Definition of an X.500 Attribute Type and Object Class to Hold Uniform Resource Identifiers (URIs)", RFC 2079.

Appendix A. Copyright

Author's Address

Mark Wahl
Informed Control Inc.
PO Box 90626
Austin, TX 78709
US

Email: mark.wahl@informed-control.com

Full Copyright Statement

Intellectual Property

Acknowledgment

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