

Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: March 9, 2008

M. Wahl
Informed Control Inc.
September 6, 2007

LDAP Administrators Address Attribute
draft-wahl-ldap-adminaddr-05

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with [Section 6 of BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/lid-abstracts.txt>.

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

This Internet-Draft will expire on March 9, 2008.

Copyright Notice

Copyright (C) The IETF Trust (2007).

Internet-Draft LDAP Administrators Address Attribute September 2007

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.

Internet-Draft LDAP Administrators Address Attribute September 2007

1. Introduction

This document defines an attribute type, `administratorsAddress`, for use in LDAP [\[1\]](#) directory deployments.

The values of attributes of this attribute type are used to provide contact information of the responsible party for an LDAP server, or of the responsible party for a naming context (or other directory administrative division) 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.

Internet-Draft LDAP Administrators Address Attribute September 2007

[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'  
  EQUALITY caseExactIA5Match  
  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 the attribute of this type be 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 the attribute of this type be returned. Note that these addresses need not be the same as that of the

directory server administrator, or of a data administrator.

An attribute of this type MAY be present in other entries and subentries in a directory information tree. For example, an attribute might be present in a collective attribute subentry. (Collective attribute subentries are defined in [RFC 3671](#) [7] and [RFC 3672](#) [8]).

A client SHOULD treat values of this attribute type which do not contain a valid URI as non-resolvable.

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

Generally, the information provided by this attribute in a particular organization's directory service is intended to be visible to all the directory service administrators and to all the administrators of directory-enabled applications in the organization. Since one use of this attribute is to find who is responsible for a directory server that is not making authentication decisions properly, in some deployments it might be appropriate to allow any user, including anonymous (unauthenticated) users, to read the values of an attribute of this type from the root DSE. Thus, it is good practice that the email addresses chosen for use in this attribute avoid revealing personal information. Applications setting values of this attribute SHOULD NOT encode passwords or other secret information within the URIs, and MUST allow the administrator to choose not to provide a value for this attribute.

[4.](#) IANA Considerations

The LDAP Parameter registration for this attribute type has already been reviewed by the Directorate and processed by IANA. This attribute type 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

[5.](#) Changes from previous versions

In an earlier Internet-Draft of the ASID working group, the `administratorsAddress` attribute was defined to only be present in the root DSE, the definition did not specify an equality matching rule and had usage "dSAOperation", and the values of the attribute were limited to being URLs of the mailto form.

[6.](#) 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.

[7.](#) References

[7.1.](#) 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.

[7.2.](#) Informative References

- [6] Smith, M., "Definition of an X.500 Attribute Type and Object Class to Hold Uniform Resource Identifiers (URIs)", [RFC 2079](#).
- [7] Zeilenga, K., "Collective Attributes in the Lightweight Directory Access Protocol (LDAP)", [RFC 3671](#).
- [8] Zeilenga, K. and S. Legg, "Subentries in the Lightweight Directory Access Protocol (LDAP)", [RFC 3672](#).

Internet-Draft LDAP Administrators Address Attribute September 2007

[Appendix A](#). Copyright

Copyright (C) The Internet Society 2007. This document is subject to the rights, licenses and restrictions contained in [BCP 78](#), and except as set forth therein, the authors retain all their rights. This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Internet-Draft LDAP Administrators Address Attribute September 2007

Author's Address

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

Email: mark.wahl@informed-control.com

Internet-Draft LDAP Administrators Address Attribute September 2007

Full Copyright Statement

Copyright (C) The IETF Trust (2007).

This document is subject to the rights, licenses and restrictions contained in [BCP 78](#), and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY, THE IETF TRUST AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

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).