INTERNET-DRAFT
draft-legg-ldap-admin-03.txt
Intended Category: Standards Track

S. Legg
eB2Bcom

September 3, 2007

Lightweight Directory Access Protocol (LDAP): Directory Administrative Model

Status of This Memo

Abstract

This document adapts the X.500 directory administrative model for use by the Lightweight Directory Access Protocol (LDAP). The administrative model partitions the Directory Information Tree (DIT) for various aspects of directory data administration, e.g., subschema, access control, and collective attributes. The generic framework that applies to every aspect of administration is described in this document. The definitions that apply for a specific aspect of administration, e.g., access control administration, are described

in other documents.

Table of Contents

1. Introduction

This document adapts the X.500 directory administrative model [X.501] for use by the Lightweight Directory Access Protocol (LDAP) [LDAP]. The administrative model partitions the Directory Information Tree (DIT) for various aspects of directory data administration, e.g., subschema, access control, and collective attributes. This document provides the definitions for the generic parts of the administrative model that apply to every aspect of directory data administration.

Sections 3 to 7, in conjunction with [SUBENTRY], describe the means by which administrative authority is aportioned and exercised in the DIT.

Aspects of administration that conform to the administrative model described in this document, e.g., access control administration [ACA] and collective attribute administration [COLLECT], are detailed elsewhere.

This document is derived from, and duplicates substantial portions of, Sections 4 and 8 of X.501 [X.501].

2. Conventions

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 BCP 14, RFC 2119 [BCP14].

3. Administrative Areas

An administrative area is a subtree of the DIT considered from the perspective of administration. The root entry of the subtree is an administrative point. An administrative point is represented by an entry holding an administrativeRole attribute [SUBENTRY]. The values of this attribute identify the kind of administrative point.

4. Autonomous Administrative Areas

The DIT may be partitioned into one or more non-overlapping subtrees termed autonomous administrative areas. It is expected that the entries in an autonomous administrative area are all administered by the same administrative authority.

An administrative authority may be responsible for several autonomous administrative areas in separated parts of the DIT but it SHOULD NOT arbitrarily partition the collection of entries under its control into autonomous administrative areas (thus creating adjacent autonomous areas administered by the same authority).

The root entry of an autonomous administrative area's subtree is called an autonomous administrative point. An autonomous administrative area extends from its autonomous administrative point downwards until another autonomous administrative point is encountered, at which point another autonomous administrative area begins.

5. Specific Administrative Areas

Entries in an administrative area may be considered in terms of a specific administrative function. When viewed in this context, an administrative area is termed a specific administrative area.

Examples of specific administrative areas are subschema specific administrative areas, access control specific areas, and collective attribute specific areas.

An autonomous administrative area may be considered as implicitly defining a single specific administrative area for each specific aspect of administration. In this case, there is a precise correspondence between each such specific administrative area and the autonomous administrative area.

Alternatively, for each specific aspect of administration, the autonomous administrative area may be partitioned into non-overlapping specific administrative areas.

If so partitioned for a particular aspect of administration, each entry of the autonomous administrative area is contained in one and

only one specific administrative area for that aspect, i.e., specific administrative areas do not overlap.

The root entry of a specific administrative area's subtree is called a specific administrative point. A specific administrative area extends from its specific administrative point downwards until another specific administrative point of the same administrative aspect is encountered, at which point another specific administrative area begins. Specific administrative areas are always bounded by the autonomous administrative area they partition.

Where an autonomous administrative area is not partitioned for a specific aspect of administration, the specific administrative area for that aspect coincides with the autonomous administrative area. In this case, the autonomous administrative point is also the specific administrative point for this aspect of administration. A particular administrative point may be the root of an autonomous administrative area and may be the root of one or more specific administrative areas for different aspects of administration.

It is not necessary for an administrative point to represent each specific aspect of administrative authority. For example, there might be an administrative point, subordinate to the root of the autonomous administrative area, that is used for access control purposes only.

6. Inner Administrative Areas

For some aspects of administration, e.g., access control or collective attributes, inner administrative areas may be defined within the specific administrative areas, to allow a limited form of delegation, or for administrative or operational convenience.

An inner administrative area may be nested within another inner administrative area. The rules for nested inner areas are defined as part of the definition of the specific administrative aspect for which they are allowed.

The root entry of an inner administrative area's subtree is called an inner administrative point. An inner administrative area (within a specific administrative area) extends from its inner administrative point downwards until a specific administrative point of the same administrative aspect is encountered. An inner administrative area is bounded by the specific administrative area within which it is defined.

7. Administrative Entries

An entry located at an administrative point is an administrative entry. Administrative entries MAY have subentries [SUBENTRY] as immediate subordinates. The administrative entry and its associated subentries are used to control the entries encompassed by the associated administrative area. Where inner administrative areas are used, the scopes of these areas may overlap. Therefore, for each specific aspect of administrative authority, a definition is required of the method of combination of administrative information when it is possible for entries to be included in more than one subtree or subtree refinement associated with an inner area defined for that aspect.

8. Security Considerations

This document defines a generic framework for employing policy of various kinds, e.g., access controls, to entries in the DIT. Such policy can only be correctly enforced at a directory server holding a replica of a portion of the DIT if the administrative entries for administrative areas that overlap the portion of the DIT being replicated, and the subentries of those administrative entries relevant to any aspect of policy that is required to be enforced at the replica, are included in the replicated information.

Administrative entries and subentries SHOULD be protected from unauthorized examination or changes by appropriate access controls.

9. Acknowledgements

This document is derived from, and duplicates substantial portions of, Sections 4 and 8 of X.501 [X.501].

10. References

10.1. Normative References

[BCP14] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[SUBENTRY] Zeilenga, K. and S. Legg, "Subentries in the Lightweight Directory Access Protocol (LDAP)", RFC 3672, December 2003.

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

10.2. Informative References

[COLLECT] Zeilenga, K., "Collective Attributes in the Lightweight Directory Access Protocol (LDAP)", RFC 3671, December 2003.

[ACA] Legg, S., "Lightweight Directory Access Protocol (LDAP): Access Control Administration", draft-legg-ldap-acm-admin-xx.txt, a work in progress, June 2004.

[X.501] ITU-T Recommendation X.501 (08/05) | ISO/IEC 9594-2:2005, Information technology - Open Systems Interconnection - The Directory: Models.

IANA Considerations

This document has no actions for IANA.

Author's Address

Dr. Steven Legg
eB2Bcom
Suite 1, 85-87 Charles Street
Kew, Victoria 3101
AUSTRALIA

Phone: +61 3 9851 8630
Fax: +61 3 9851 8601
EMail: steven.legg@eb2bcom.com

Full Copyright Statement

Intellectual Property

Note to the RFC Editor: the remainder of this document is to be removed before final publication.

Changes in Draft 00

This document reproduces Section 4 from draft-legg-ldap-acm-admin-00.txt as a standalone document. All changes made are purely editorial. No technical changes have been introduced.

Changes in Draft 01

RFC 3377 replaces RFC 2251 as the reference for LDAP.

Changes in Draft 02

The document has been reformatted in line with current practice.

Changes in Draft 03

RFC 4510 replaces RFC 3377 as the reference for LDAP.