Network Working Group
Request for Comments: 3671
Category: Standards Track

K. Zeilenga
OpenLDAP Foundation

December 2003

Collective Attributes in the Lightweight Directory Access Protocol (LDAP)

Status of this Memo

Copyright Notice

Abstract

X.500 collective attributes allow common characteristics to be shared between collections of entries. This document summarizes the X.500 information model for collective attributes and describes use of collective attributes in LDAP (Lightweight Directory Access Protocol). This document provides schema definitions for collective attributes for use in LDAP.

1. Introduction

In X.500 [X.500], a collective attribute is "a user attribute whose values are the same for each member of an entry collection" [X.501]. This document details their use in the Lightweight Directory Access Protocol (LDAP) [RFC3377].

1.1. Entry Collections

A collection of entries is a grouping of object and alias entries based upon common properties or shared relationship between the corresponding entries which share certain attributes. An entry collection consists of all entries within scope of a collective attributes subentry [RFC3672]. An entry can belong to several entry collections.

1.2. Collective Attributes

Attributes shared by the entries comprising an entry collection are called collective attributes. Values of collective attributes are visible but not updateable to clients accessing entries within the collection. Collective attributes are updated (i.e., modified) via their associated collective attributes subentry.

When an entry belongs to multiple entry collections, the entry's values of each collective attribute are combined such that independent sources of these values are not manifested to clients.

Entries can specifically exclude a particular collective attribute by listing the attribute as a value of the collectiveExclusions attribute. Like other user attributes, collective attributes are subject to a variety of controls including access, administrative, and content controls.

1.3. Conventions

Schema definitions are provided using LDAPv3 [RFC2251] description formats [RFC2252]. Definitions provided here are formatted (line wrapped) for readability.

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 [RFC2119].

2. System Schema for Collective Attributes

The following operational attributes are used to manage Collective Attributes. LDAP servers [RFC3377] MUST act in accordance with the X.500 Directory Models [X.501] when providing this service.

2.1. collectiveAttributeSubentry

Subentries of this object class are used to administer collective attributes and are referred to as collective attribute subentries.

```
( 2.5.17.2 NAME 'collectiveAttributeSubentry' AUXILIARY )
```

A collective attribute subentry SHOULD contain at least one collective attribute. The collective attributes contained within a collective attribute subentry are available for finding, searching, and comparison at every entry within the scope of the subentry. The collective attributes, however, are administered (e.g., modified) via the subentry.

Implementations of this specification SHOULD support collective attribute subentries in both collectiveAttributeSpecificArea (2.5.23.5) and collectiveAttributeInnerArea (2.5.23.6) administrative areas [RFC3672][X.501].

2.2. collectiveAttributeSubentries

The collectiveAttributeSubentries operational attribute identifies all collective attribute subentries that affect the entry.

```
( 2.5.18.12 NAME 'collectiveAttributeSubentries'
  EQUALITY distinguishedNameMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.12
  USAGE directoryOperation NO-USER-MODIFICATION )
```

2.3. collectiveExclusions

The collectiveExclusions operational attribute allows particular collective attributes to be excluded from an entry. It MAY appear in any entry and MAY have multiple values.

```
( 2.5.18.7 NAME 'collectiveExclusions'
  EQUALITY objectIdentifierMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.38
  USAGE directoryOperation )
```

The descriptor excludeAllCollectiveAttributes is associated with the OID 2.5.18.0. When this descriptor or OID is present as a value of the collectiveExclusions attribute, all collective attributes are excluded from an entry.

3. Collective Attribute Types

A userApplications attribute type can be defined to be COLLECTIVE [RFC2252]. This indicates that the same attribute values will appear in the entries of an entry collection subject to the use of the collectiveExclusions attribute and other administrative controls. These administrative controls MAY include DIT Content Rules, if implemented.

Collective attribute types are commonly defined as subtypes of non-collective attribute types. By convention, collective attributes are named by prefixing the name of their non-collective supertype with "c-". For example, the collective telephone attribute is named c-TelephoneNumber after its non-collective supertype telephoneNumber.

Non-collective attributes types SHALL NOT subtype collective attributes.

Collective attributes SHALL NOT be SINGLE-VALUED. Collective attribute types SHALL NOT appear in the attribute types of an object class definition.

Operational attributes SHALL NOT be defined to be collective.

The remainder of section provides a summary of collective attributes derived from those defined in [X.520]. The SUPerior attribute types are described in [RFC 2256] for use with LDAP.

Implementations of this specification SHOULD support the following collective attributes and MAY support additional collective attributes.

3.1. Collective Locality Name

The c-l attribute type specifies a locality name for a collection of entries.

```
( 2.5.4.7.1 NAME 'c-l'
  SUP l COLLECTIVE )
```

3.2. Collective State or Province Name

The c-st attribute type specifies a state or province name for a collection of entries.

```
( 2.5.4.8.1 NAME 'c-st'
  SUP st COLLECTIVE )
```

3.3. Collective Street Address

The c-street attribute type specifies a street address for a collection of entries.

```
( 2.5.4.9.1 NAME 'c-street'
  SUP street COLLECTIVE )
```

3.4. Collective Organization Name

The c-o attribute type specifies an organization name for a collection of entries.

```
( 2.5.4.10.1 NAME 'c-o'
  SUP o COLLECTIVE )
```

3.5. Collective Organizational Unit Name

The c-ou attribute type specifies an organizational unit name for a collection of entries.

```
( 2.5.4.11.1 NAME 'c-ou'
  SUP ou COLLECTIVE )
```

3.6. Collective Postal Address

The c-PostalAddress attribute type specifies a postal address for a collection of entries.

```
( 2.5.4.16.1 NAME 'c-PostalAddress'
  SUP postalAddress COLLECTIVE )
```

3.7. Collective Postal Code

The c-PostalCode attribute type specifies a postal code for a collection of entries.

```
( 2.5.4.17.1 NAME 'c-PostalCode'
  SUP postalCode COLLECTIVE )
```

3.8. Collective Post Office Box

The c-PostOfficeBox attribute type specifies a post office box for a collection of entries.

```
( 2.5.4.18.1 NAME 'c-PostOfficeBox'
  SUP postOfficeBox COLLECTIVE )
```

3.9. Collective Physical Delivery Office Name

The c-PhysicalDeliveryOfficeName attribute type specifies a physical delivery office name for a collection of entries.

```
( 2.5.4.19.1 NAME 'c-PhysicalDeliveryOfficeName'
  SUP physicalDeliveryOfficeName COLLECTIVE )
```

3.10. Collective Telephone Number

The c-TelephoneNumber attribute type specifies a telephone number for a collection of entries.

```
( 2.5.4.20.1 NAME 'c-TelephoneNumber'
  SUP telephoneNumber COLLECTIVE )
```

3.11. Collective Telex Number

The c-TelexNumber attribute type specifies a telex number for a collection of entries.

```
( 2.5.4.21.1 NAME 'c-TelexNumber'
  SUP telexNumber COLLECTIVE )
```

3.13. Collective Facsimile Telephone Number

The c-FacsimileTelephoneNumber attribute type specifies a facsimile telephone number for a collection of entries.

```
( 2.5.4.23.1 NAME 'c-FacsimileTelephoneNumber'

SUP facsimileTelephoneNumber COLLECTIVE )
```

3.14. Collective International ISDN Number

The c-InternationalISDNNumber attribute type specifies an international ISDN number for a collection of entries.

```
( 2.5.4.25.1 NAME 'c-InternationalISDNNumber'
  SUP internationalISDNNumber COLLECTIVE )
```

4. Security Considerations

Collective attributes, like other attributes, are subject to access control restrictions and other administrative policy. Generally speaking, collective attributes accessed via an entry in a collection are governed by rules restricting access to attributes of that entry. And collective attributes access via a subentry are governed by rules restricting access to attributes of that subentry. However, as LDAP does not have a standard access model, the particulars of each server's access control system may differ.

General LDAP security considerations [RFC3377] also apply.

5. IANA Considerations

The IANA has registered the LDAP descriptors [RFC3383] defined in this technical specification. The following registration template is suggested:

```
Subject: Request for LDAP Descriptor Registration
Descriptor see comments
Object Identifier: see comment
Person & email address to contact for further information:
     Kurt Zeilenga <kurt@OpenLDAP.org>
Usage: see comment
Specification: RFC3671
Author/Change Controller: IESG
Comments:
```

NAME	Type	OID
c-FacsimileTelephoneNumber	A	2.5.4.23.1
c-InternationalISDNNumber	A	2.5.4.25.1
c-PhysicalDeliveryOffice	A	2.5.4.19.1
c-PostOfficeBox	A	2.5.4.18.1
c-PostalAddress	A	2.5.4.16.1
c-PostalCode	A	2.5.4.17.1
c-TelephoneNumber	A	2.5.4.20.1
c-TelexNumber	A	2.5.4.21.1
c-l	A	2.5.4.7.1
c-o	A	2.5.4.10.1
c-ou	A	2.5.4.11.1
c-st	A	2.5.4.8.1
c-street	A	2.5.4.9.1
collectiveAttributeSubentries	A	2.5.18.12
collectiveAttributeSubentry	O	2.5.17.2
collectiveExclusions	A	2.5.18.7

where Type A is Attribute and Type O is ObjectClass.

The Object Identifiers used in this document were assigned by the ISO/IEC Joint Technical Committee 1 - Subcommittee 6 to identify elements of X.500 schema [X.520]. This document make no OID assignments, it only provides LDAP schema descriptions with existing elements of X.500 schema.

6. Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any intellectual property 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; neither does it represent that it has made any effort to identify any such rights. Information on the IETF's procedures with respect to rights in standards-track and standards-related documentation can be found in BCP-11. Copies of claims of rights made available for publication 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 implementors or users of this specification can be obtained from the IETF Secretariat.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights which may cover technology that may be required to practice this standard. Please address the information to the IETF Executive Director.

7. Acknowledgments

This document is based upon the ITU Recommendations for the Directory [X.501][X.520].

8. References

8.1. Normative References

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

[RFC2251] Wahl, M., Howes, T. and S. Kille, "Lightweight Directory Access Protocol (v3)", RFC 2251, December 1997.

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

[RFC2256] Wahl, M., "A Summary of the X.500(96) User Schema for use with LDAPv3", RFC 2256, December 1997.

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

[RFC3383] Zeilenga, K., "Internet Assigned Numbers Authority (IANA) Considerations for the Lightweight Directory Access Protocol (LDAP)", BCP 64, RFC 3383, September 2002.

[RFC3672] Zeilenga, K. and S. Legg, "Subentries in Lightweight Directory Access Protocol (LDAP)", RFC 3672, December 2003.

[X.501] "The Directory: Models", ITU-T Recommendation X.501, 1993.

8.2. Informative References

[X.500] "The Directory: Overview of Concepts, Models", ITU-T Recommendation X.500, 1993.

[X.520] "The Directory: Selected Attribute Types", ITU-T Recommendation X.520, 1993.

9. Author's Address

Kurt D. Zeilenga
OpenLDAP Foundation

EMail: Kurt@OpenLDAP.org

10. Full Copyright Statement

Acknowledgement

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