Internet Engineering Task Force (IETF)
Request for Comments: 6171
Category: Standards Track
ISSN: 2070-1721

K. Zeilenga
Isode Limited

March 2011

The Lightweight Directory Access Protocol (LDAP) Don't Use Copy Control

Abstract

This document defines the Lightweight Directory Access Protocol (LDAP) Don't Use Copy control extension, which allows a client to specify that copied information should not be used in providing service. This control is based upon the X.511 dontUseCopy service control option.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc6171.

1. Background and Intended Usage

This document defines the Lightweight Directory Access Protocol (LDAP) [RFC4510] Don’t Use Copy control extension. The control may be attached to request messages to indicate that copied (replicated or cached) information [X.500] is not be used in providing service. This control is based upon the X.511 [X.511] dontUseCopy service control option.

The Don’t Use Copy control is intended to be used where the client requires the service be provided using original (master) information [X.500]. In absence of this control, the server is free to make use of copied (i.e., non-authoritative) information in providing the requested service.

For instance, a client might desire to have an authoritative answer to a question of whether or not a particular user is a member of a group. To ask this question of a server, the client might issue a compare request [RFC4511], with the Don’t Use Copy control, where the entry parameter is the Distinguished Name (DN) of the group, the ava.attributeDesc is ’member’, and the ava.assertionValue is the DN of the user in question. If the server has access to the original (master) information directly or through chaining, it performs the operation against the original (master) information and returns compareTrue or compareFalse (or an error). If the server does not have access to the original information, the server is obligated to either return a referral or an error.

It is not intended that this control be used generally (e.g., for all LDAP interrogation operations) but only as required to ensure proper directory application behavior. In general, directory applications ought to designed to use copied information well.

2. Terminology

DSA stands for Directory System Agent (or server).
DSE stands for DSA-Specific Entry.

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 RFC 2119 [RFC2119].

3. The Don’t Use Copy Control

The Don’t Use Copy control is an LDAP Control [RFC4511] whose controlType is 1.3.6.1.1.22 and controlValue is absent. The criticality MUST be TRUE. There is no corresponding response control.

The control is appropriate for LDAP interrogation operations, including Compare and Search operations [RFC4511]. It is inappropriate for all other operations, including Abandon, Bind, Delete, Modify, ModifyDN, StartTLS, and Unbind operations [RFC4511].

When the control is attached to an LDAP request, the requested operation MUST NOT be performed on copied information. That is, the requested operation MUST be performed on original information.

If original (master) information for the target or base object of the operation is not available (either locally or through chaining), the server MUST either return a referral directing the client to a server believed to be better able to service the request or return an appropriate result code (e.g., unwillingToPerform).

It is noted that a referral, if returned, is not necessarily to the server holding the original (master) information. It is also noted that an authoritative answer to the question might not be available to the client for any number of reasons.

Where the client chases a referral to a server (as referenced by an LDAP URL) in the server response in order to obtain an authoritative response, the client MUST provide the dontUseCopy control with the interrogation request it makes to the referred to server. While LDAP allows return of other kinds of URIs, the syntax and semantics of other kinds of URIs are left to future specifications. The particulars of how to act upon other kinds of URIs are also left to future specifications.

Servers implementing this technical specification SHOULD publish the object identifier 1.3.6.1.1.22 as a value of the ’supportedControl’ attribute [RFC4512] in their root DSE. A server MAY choose to advertise this extension only when the client is authorized to use it.

4. Security Considerations

This control is intended to be provided where providing service using copied information might lead to unexpected application behavior.

Use of the Don’t Use Copy control may permit an attacker to perform or amplify a denial-of-service attack by causing additional server resources to be employed, such as when the server chooses to chain the request instead of returning a referral. Servers capable of such chaining can mitigate this threat by limiting chaining to a particular group of authenticated entities.

LDAP is frequently used for storage and distribution of security-sensitive information, including access control and security policy information. Failure to use the Don’t Use Copy control may thus permit an attacker to gain unauthorized access by allowing reliance on stale data.

5. IANA Considerations

5.1. Object Identifier

IANA has assigned an LDAP Object Identifier [RFC4520] to identify the LDAP Don’t Use Copy Control defined in this document.

```
Subject: Request for LDAP Object Identifier Registration
Person & email address to contact for further information:
    Kurt Zeilenga <Kurt.Zeilenga@Isode.COM>
Specification: RFC 6171
Author/Change Controller: IESG
Comments:
    Identifies the LDAP Don’t Use Copy Control
```

5.2. LDAP Protocol Mechanism

IANA has registered this protocol mechanism [RFC4520] as follows.

Subject: Request for LDAP Protocol Mechanism Registration
Object Identifier: 1.3.6.1.1.22
Description: Don’t Use Copy Control
Person & email address to contact for further information:
Kurt Zeilenga <Kurt.Zeilenga@Isode.COM>
Usage: Control
Specification: RFC 6171
Author/Change Controller: IESG
Comments: none

6. Acknowledgements

The author thanks Ben Campbell, Phillip Hallam-Baker, and Ted Hardie for providing review and specific suggestions.

7. References

7.1. Normative References

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

[RFC4510] Zeilenga, K., Ed., "Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map", RFC 4510, June 2006.

[RFC4511] Sermersheim, J., Ed., "Lightweight Directory Access Protocol (LDAP): The Protocol", RFC 4511, June 2006.

[RFC4512] Zeilenga, K., Ed., "Lightweight Directory Access Protocol (LDAP): Directory Information Models", RFC 4512, June 2006.

7.2. Informative References

[X.500] International Telecommunication Union - Telecommunication Standardization Sector, "The Directory -- Overview of concepts, models and services," X.500(1993) (also ISO/IEC 9594-1:1994).

[X.511] International Telecommunication Union - Telecommunication Standardization Sector, "The Directory: Abstract Service Definition", X.511(1993) (also ISO/IEC 9594-3:1993).

[RFC4520] Zeilenga, K., "Internet Assigned Numbers Authority (IANA) Considerations for the Lightweight Directory Access Protocol (LDAP)", BCP 64, RFC 4520, June 2006.

Author’s Address

Kurt D. Zeilenga
Isode Limited

EMail: Kurt.Zeilenga@Isode.COM