Network Working Group
Request for Comments: 4528
Category: Standards Track

K. Zeilenga
OpenLDAP Foundation

June 2006

Lightweight Directory Access Protocol (LDAP) Assertion Control

Status of This Memo

Copyright Notice

Abstract

This document defines the Lightweight Directory Access Protocol (LDAP) Assertion Control, which allows a client to specify that a directory operation should only be processed if an assertion applied to the target entry of the operation is true. It can be used to construct "test and set", "test and clear", and other conditional operations.

Table of Contents

1. Overview

This document defines the Lightweight Directory Access Protocol (LDAP) [RFC4510] assertion control. The assertion control allows the client to specify a condition that must be true for the operation to be processed normally. Otherwise, the operation is not performed. For instance, the control can be used with the Modify operation [RFC4511] to perform atomic "test and set" and "test and clear" operations.

The control may be attached to any update operation to support conditional addition, deletion, modification, and renaming of the target object. The asserted condition is evaluated as an integral part the operation.

The control may also be used with the search operation. Here, the assertion is applied to the base object of the search before searching for objects that match the search scope and filter.

The control may also be used with the compare operation. Here, it extends the compare operation to allow a more complex assertion.

2. Terminology

Protocol elements are described using ASN.1 [X.680] with implicit tags. The term "BER-encoded" means the element is to be encoded using the Basic Encoding Rules [X.690] under the restrictions detailed in Section 5.1 of [RFC4511].

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

In this document, the key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" are to be interpreted as described in BCP 14 [RFC2119].

3. The Assertion Control

The assertion control is an LDAP Control [RFC4511] whose controlType is 1.3.6.1.1.12 and whose controlValue is a BER-encoded Filter [Protocol, Section 4.5.1]. The criticality may be TRUE or FALSE. There is no corresponding response control.

The control is appropriate for both LDAP interrogation and update operations [RFC4511], including Add, Compare, Delete, Modify, ModifyDN (rename), and Search. It is inappropriate for Abandon, Bind, Unbind, and StartTLS operations.

When the control is attached to an LDAP request, the processing of the request is conditional on the evaluation of the Filter as applied against the target of the operation. If the Filter evaluates to TRUE, then the request is processed normally. If the Filter evaluates to FALSE or Undefined, then assertionFailed (122) resultCode is returned, and no further processing is performed.

For Add, Compare, and ModifyDN operations, the target is indicated by the entry field in the request. For Modify operations, the target is indicated by the object field. For Delete operations, the target is indicated by the DelRequest type. For Compare operations and all update operations, the evaluation of the assertion MUST be performed as an integral part of the operation. That is, the evaluation of the assertion and the normal processing of the operation SHALL be done as one atomic action.

For Search operations, the target is indicated by the baseObject field, and the evaluation is done after "finding" but before "searching" [RFC4511]. Hence, no entries or continuations references are returned if the assertion fails.

Servers implementing this technical specification SHOULD publish the object identifier 1.3.6.1.1.12 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.

Other documents may specify how this control applies to other LDAP operations. In doing so, they must state how the target entry is determined.

4. Security Considerations

The filter may, like other components of the request, contain sensitive information. When it does, this information should be appropriately protected.

As with any general assertion mechanism, the mechanism can be used to determine directory content. Hence, this mechanism SHOULD be subject to appropriate access controls.

Some assertions may be very complex, requiring significant time and resources to evaluate. Hence, this mechanism SHOULD be subject to appropriate administrative controls.

Security considerations for the base operations [RFC4511] extended by this control, as well as general LDAP security considerations [RFC4510], generally apply to implementation and use of this extension.

5. IANA Considerations

5.1. Object Identifier

The IANA has assigned an LDAP Object Identifier [RFC4520] to identify the LDAP Assertion Control defined in this document.

```
Subject: Request for LDAP Object Identifier Registration
Person & email address to contact for further information:
    Kurt Zeilenga <kurt@OpenLDAP.org>
Specification: RFC 4528
Author/Change Controller: IESG
Comments:
    Identifies the LDAP Assertion Control
```

5.2. LDAP Protocol Mechanism

Registration of this protocol mechanism [RFC4520] is requested.

```
Subject: Request for LDAP Protocol Mechanism Registration
Object Identifier: 1.3.6.1.1.12
Description: Assertion Control
Person & email address to contact for further information:
    Kurt Zeilenga <kurt@openldap.org>
Usage: Control
Specification: RFC 4528
Author/Change Controller: IESG
Comments: none
```

5.3. LDAP Result Code

The IANA has assigned an LDAP Result Code [RFC4520] called 'assertionFailed' (122).

```
Subject: LDAP Result Code Registration
Person & email address to contact for further information:
    Kurt Zeilenga <kurt@OpenLDAP.org>
Result Code Name: assertionFailed
Specification: RFC 4528
Author/Change Controller: IESG
Comments:  none
```

6. Acknowledgements

The assertion control concept is attributed to Morteza Ansari.

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., "Lightweight Directory Access Protocol (LDAP): Directory Information Models", RFC 4512, June 2006.

[X.680] International Telecommunication Union - Telecommunication Standardization Sector, "Abstract Syntax Notation One (ASN.1) - Specification of Basic Notation", X.680(2002) (also ISO/IEC 8824-1:2002).

[X.690] International Telecommunication Union - Telecommunication Standardization Sector, "Specification of ASN.1 encoding rules: Basic Encoding Rules (BER), Canonical Encoding Rules (CER), and Distinguished Encoding Rules (DER)", X.690(2002) (also ISO/IEC 8825-1:2002).

7.2. Informative References

[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
OpenLDAP Foundation

EMail: Kurt@OpenLDAP.org

Full Copyright Statement

Intellectual Property

Acknowledgement

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