LDAP "What Failed?" Control
draft-masarati-ldap-whatfailed-00.txt

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/1id-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 May 23, 2009.
Abstract

This document describes the LDAP "What Failed?" control. This control allows DUAs to request, in response to a failed operation request, the object identifier of those extensions that caused the operation to fail.

Table of Contents

1. Background and Intended Use .................................. 3
2. LDAP "What Failed?" Control ................................. 4
   2.1. Control Semantics ...................................... 4
   2.2. Control Request ........................................ 4
   2.3. Control Response ....................................... 5
3. Implementation Notes ........................................... 6
4. Security Considerations ....................................... 7
5. IANA Considerations ........................................... 8
   5.1. Object Identifier Registration .......................... 8
6. Acknowledgments ................................................ 9
7. References ..................................................... 10
   7.1. Normative References .................................. 10
   7.2. Informative References ................................ 10
Author’s Address .................................................. 11
Intellectual Property and Copyright Statements .................. 12
1. Background and Intended Use

The LDAP Protocol [RFC4510] is extensible. Extensions include controls, extended requests and extensions related to other aspects of the protocol, for example those described in [RFC4526], [RFC4529] and more.

Operations may fail for different reasons. The resultCode may help in determining the reason of a failure. The (optional) diagnosticsMessage fields of a LDAPResponse could also be of help. However, according to [RFC4511], implementations MUST NOT rely on the returned values, which are simply intended to be presented as are to human users.

In case of failure related to the inability to process a control marked as critical in a request, the specific resultCode unavailableCriticalExtension is returned. In case of failure related to an unrecognized extendedReq, the generic resultCode protocolError is returned. Failures related to handling other extensions may result in other generic resultCode values.

As a consequence, DUAs may be unable to exactly determine what extension, if any, caused a failure. The "What Failed?" control represents a means for the DSA to inform DUAs about what specific extensions, if any, caused an error notified by the DSA.

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 [RFC2119].
2. LDAP "What Failed?" Control

2.1. Control Semantics

The presence of the "What Failed?" LDAP control in a LDAP request indicates that the DUA, in case of error, wishes to receive detailed information about what extension, if any, caused the error.

The criticality of the control in the request SHOULD be FALSE. According to the semantics of the criticality field as indicated in [RFC4511], this ensures that in case the control is not recognized by the DSA, it does not cause itself an error.

The presence of this control in a request does not guarantee that the DSA will return detailed information about what extensions caused an error. Considering the requirement on the criticality of the control, the DSA MAY simply choose to ignore the control. The DSA MAY hide information about failure in handling an extension to prevent disclosure of other information. The DSA MAY choose to notify an error as soon as it is detected, instead of proceed checking its ability to handle any other extension present in a request.

Implementations may choose to check the validity of extensions, including controls, as soon as they are parsed. As a consequence, a critical control might result in an error before the "What Failed?" control request is parsed. Implementations SHOULD check anyway the presence of this control, unless they detect that the remaining part of the request is malformed. Clients SHOULD NOT rely on any specific ordering of controls handling when requesting the "What Failed?" control.

Servers implementing this technical specification SHOULD publish the object identifier whatFailed-oid (IANA assigned; see Section 5) as a value of the ’supportedControl’ attribute [RFC4512] in their root DSE.

2.2. Control Request

The controlType is whatFailed-oid (IANA assigned; see Section 5); the controlValue MUST be absent; the criticality SHOULD be FALSE.
2.3. Control Response

The controlType is whatFailed-oid (IANA assigned; see Section 5); the controlValue is:

\[
\text{controlValue ::= SET OF oid LDAPOID}
\]

If the set of extension OID is empty, the control is omitted from the response. The criticality MUST be FALSE.
3. Implementation Notes

The "What Failed?" LDAP Control is implemented in OpenLDAP software using the temporary OID 1.3.6.1.4.1.4203.666.5.17 under OpenLDAP’s experimental OID arc.
4. Security Considerations

Implementations MUST take measures to prevent the disclosure of sensible information whenever this may result from disclosing what extension caused an error. This can consist in excluding the OID of specific extensions from the controlValue in the response, or in entirely omitting the control in the response.
5. IANA Considerations

5.1. Object Identifier Registration

It is requested that IANA register upon Standards Action an LDAP Object Identifier for use in this technical specification.

Subject: Request for LDAP OID Registration
Person & email address to contact for further information:
   Pierangelo Masarati <ando@OpenLDAP.org>
Specification: (I-D)
Author/Change Controller: IESG
Comments:
   Identifies the LDAP "What Failed?" Control request and response
6. Acknowledgments
7. References

7.1. Normative References


7.2. Informative References


Author’s Address

Pierangelo Masarati
Politecnico di Milano
Dipartimento di Ingegneria Aerospaziale
via La Masa 34
Milano 20156
IT

Phone: +39 02 2399 8309
Fax: +39 02 2399 8334
Email: ando@OpenLDAP.org
URI: http://www.aero.polimi.it/masarati/