Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: 21 June 2026

J. Khan
DXC Technology

18 December 2025

LDAP Bind Response Extension for Returning DN and Attributes
draft-khan-ldap-bind-return-dn-00

Abstract

This document proposes an extension to the LDAP Bind operation to optionally return the authenticated subject's Distinguished Name (DN) and selected attributes. The goal is to reduce the number of client-server round trips required to obtain user identity information after authentication.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

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."

This Internet-Draft will expire on 21 June 2026.

Table of Contents

1. Introduction 2
2. Motivation 2
3. Specification 2
3.1. Bind Request Control 3
3.2. Bind Response Augmentation 3
3.3. Control Value and Encoding 3
4. Examples 3
4.1. Current Workflow (RFC 4511 behavior) 4
4.2. Proposed Workflow (with this extension) 4
4.3. Attribute Selection Example 4
5. Advantages 4
6. Security Considerations 4
7. IANA Considerations 5
8. Relationship to Existing RFCs 5
9. Conclusion 6
Appendix A. Change Log 6
Author's Address 6

1. Introduction

In current LDAP practice, a client must perform at least two operations to authenticate and retrieve the DN of the subject:

1. Bind Request: The client authenticates using a DN and credentials.

2. Search Request: The client issues a search query to retrieve the DN and attributes of the authenticated subject.

This two-step process introduces unnecessary latency and complexity. By allowing the Bind response itself to return the DN and optionally attributes, the number of calls is reduced, improving efficiency for applications that need immediate access to identity information.

2. Motivation

Many modern applications, including single sign-on (SSO) systems and microservices, require immediate access to user identity attributes after authentication. The current LDAP model requires a follow-up search operation, which adds latency and complexity. This extension simplifies client logic and reduces round trips.

3. Specification

3.1. Bind Request Control

This document defines a new optional LDAP control for the Bind request:

* Control OID: 1.3.6.1.4.1.xxx.yyy.zzz (to be assigned)

* Criticality: OPTIONAL

* Control Value: An ASN.1-encoded sequence of attribute descriptions requested by the client. If the sequence is empty or absent, the server SHALL return only the DN.

3.2. Bind Response Augmentation

If the server supports this extension and the Bind operation succeeds, the Bind response SHALL include an attached response control carrying:

* The Distinguished Name (DN) of the authenticated (authorization) identity.

* The requested attributes, subject to applicable access control and privacy policies.

* Attributes not permitted by policy SHALL be omitted; the server MAY include per-attribute error indicators within the control value.

If the Bind fails, the server SHALL NOT include this response control.

3.3. Control Value and Encoding

The request and response control values are defined using ASN.1:

```
RequestControlValue ::= SEQUENCE OF AttributeDescription
ResponseControlValue ::= SEQUENCE {
    authzDN      LDAPDN,
    attributes   SEQUENCE OF PartialAttribute OPTIONAL
}
```

Where AttributeDescription, LDAPDN, and PartialAttribute are as defined in RFC 4511. Servers SHOULD preserve attribute ordering requested by the client where feasible.

4. Examples

4.1. Current Workflow (RFC 4511 behavior)

```
Client                          Server
------                          ------
Bind Request  ----------------->
                                Bind Response (success)
Search Request ---------------->
                                Search Response (dn + attributes)
```

4.2. Proposed Workflow (with this extension)

```
Client                          Server
------                          ------
Bind Request (with control) -->
                                Bind Response (dn + attributes)
```

4.3. Attribute Selection Example

Request control value: ["givenName", "mail"]

Bind Response control value:

authzDN: uid=jdoe,ou=People,dc=example,dc=com
  attributes: givenName: John mail: jdoe@example.com

5. Advantages

* Reduced number of calls: Authentication and identity retrieval in a single step.

* Lower latency: Fewer round trips between client and server.

* Simplified client logic: No need for a follow-up search.

* Clearer authorization identity handling: DN returned alongside selected attributes.

6. Security Considerations

* Access Control: Servers MUST enforce authorization and access control policies prior to returning any attribute in the Bind response control.

* Sensitive Data: Sensitive attributes (e.g., userPassword, secrets, tokens) MUST NOT be returned.

* Privacy: Servers SHOULD minimize data returned by default and honor least privilege.

* Integrity and Confidentiality: Use of StartTLS or LDAPS is RECOMMENDED to protect Bind credentials and returned attributes.

* Auditing: Servers SHOULD log the use of this control, subject to privacy law and organizational policy.

* Downgrade/Capability: Clients MUST NOT assume support; they SHOULD fall back to a search when the server does not advertise or honor the control.

7. IANA Considerations

IANA is requested to assign a new LDAP control OID under the appropriate IANA registry. The descriptive name is:

LDAP Bind Response Extension for Returning DN and Attributes

The control is suitable for Standards Track registration.

8. Relationship to Existing RFCs

This document defines an LDAP control that extends the Bind operation specified in RFC 4511 (“Lightweight Directory Access Protocol (LDAP): The Protocol”). RFC 4511 defines the Bind request and response as an authentication mechanism, with the Bind response limited to success or failure indicators. It does not provide a mechanism for returning the Distinguished Name (DN) or attributes of the authenticated subject.

The closest related work is RFC 3829 (“Lightweight Directory Access Protocol (LDAP) Authorization Identity Request and Response Controls”), which introduces a control allowing a client to request the authorization identity established by the Bind. RFC 3829 enables a client to confirm the identity string (such as a DN or other identifier) but does not return arbitrary attributes of the subject entry.

This document differs from RFC 3829 in that it allows the Bind response to return not only the DN but also selected attributes of the authenticated subject, subject to access control policies. Thus, this proposal complements RFC 3829 by extending the Bind operation to cover attribute retrieval, reducing the need for a subsequent search operation.

9. Conclusion

This document proposes an LDAP Bind extension that returns the DN and optionally attributes of the authenticated subject. By collapsing authentication and identity retrieval into a single operation, the protocol reduces overhead and improves efficiency for client applications.

Appendix A. Change Log

draft-khan-ldap-bind-return-dn-00
- Initial version of the document.
- Defined Bind request/response extension and ASN.1 control values.
- Added Motivation and Examples, including ASCII workflow diagrams.
- Added Security and IANA considerations.
- Added Relationship to Existing RFCs (RFC 4511 and RFC 3829).
- Added Change Log appendix.

Author’s Address

J. Khan
DXC Technology
Vancouver, BC, Canada