                 Lightweight Directory Access Protocol (LDAP)
                            "Who am I?" Operation

Status of This Memo

   This document specifies an Internet standards track protocol for the
   Internet community, and requests discussion and suggestions for
   improvements. Please refer to the current edition of the "Internet
   Official Protocol Standards" (STD 1) for the standardization state
   and status of this protocol. Distribution of this memo is unlimited.

Abstract

   This specification provides a mechanism for Lightweight Directory
   Access Protocol (LDAP) clients to obtain the authorization identity
   the server has associated with the user or application entity. This
   mechanism is specified as an LDAP extended operation called the LDAP
   "Who am I?" operation.

1. Background and Intent of Use

   This specification describes a Lightweight Directory Access Protocol
   (LDAP) [RFC4510] operation that clients can use to obtain the primary
   authorization identity, in its primary form, that the server has
   associated with the user or application entity. The operation is
   called the "Who am I?" operation.

   This specification is intended to replace the existing Authorization
   Identity Controls [RFC3829] mechanism, which uses Bind request and
   response controls to request and return the authorization identity.
   Bind controls are not protected by security layers established by the
   Bind operation that includes them. While it is possible to establish
   security layers using StartTLS [RFC4511][RFC4513] prior to the Bind
   operation, it is often desirable to use security layers established
   by the Bind operation. An extended operation sent after a Bind
   operation is protected by the security layers established by the Bind
   operation.

There are other cases where it is desirable to request the
authorization identity that the server associated with the client
separately from the Bind operation. For example, the "Who am I?"
operation can be augmented with a Proxied Authorization Control
[RFC4370] to determine the authorization identity that the server
associates with the identity asserted in the Proxied Authorization
Control. The "Who am I?" operation can also be used prior to the
Bind operation.

Servers often associate multiple authorization identities with the
client, and each authorization identity may be represented by
multiple authzId [RFC4513] strings. This operation requests and
returns the authzId that the server considers primary. In the
specification, the term "the authorization identity" and "the
authzId" are generally to be read as "the primary authorization
identity" and the "the primary authzId", respectively.

1.1. Conventions Used in This Document

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. The "Who am I?" Operation

The "Who am I?" operation is defined as an LDAP Extended Operation
[RFC4511] identified by the whoamiOID Object Identifier (OID). This
section details the syntax of the operation's whoami request and
response messages.

       whoamiOID ::= "1.3.6.1.4.1.4203.1.11.3"

2.1. The whoami Request

The whoami request is an ExtendedRequest with a requestName field
containing the whoamiOID OID and an absent requestValue field. For
example, a whoami request could be encoded as the sequence of octets
(in hex):

     30 1e 02 01 02 77 19 80 17 31 2e 33 2e 36 2e 31
     2e 34 2e 31 2e 34 32 30 33 2e 31 2e 31 31 2e 33

2.2. The whoami Response

The whoami response is an ExtendedResponse where the responseName
field is absent and the response field, if present, is empty or an
authzId [RFC4513]. For example, a whoami response returning the
authzId "u:xxyyz@EXAMPLE.NET" (in response to the example request)
would be encoded as the sequence of octets (in hex):

```
30 21 02 01 02 78 1c 0a  01 00 04 00 04 00 8b 13
75 3a 78 78 79 79 7a 40  45 58 41 4d 50 4c 45 2e
4e 45 54
```

3. Operational Semantics

The "Who am I?" operation provides a mechanism, a whoami Request, for
the client to request that the server return the authorization
identity it currently associates with the client. It also provides a
mechanism, a whoami Response, for the server to respond to that
request.

Servers indicate their support for this extended operation by
providing a whoamiOID object identifier as a value of the
'supportedExtension' attribute type in their root DSE. The server
SHOULD advertise this extension only when the client is willing and
able to perform this operation.

If the server is willing and able to provide the authorization
identity it associates with the client, the server SHALL return a
whoami Response with a success resultCode. If the server is treating
the client as an anonymous entity, the response field is present but
empty. Otherwise, the server provides the authzId [RFC4513]
representing the authorization identity it currently associates with
the client in the response field.

If the server is unwilling or unable to provide the authorization
identity it associates with the client, the server SHALL return a
whoami Response with an appropriate non-success resultCode (such as
operationsError, protocolError, confidentialityRequired,
insufficientAccessRights, busy, unavailable, unwillingToPerform, or
other) and an absent response field.

As described in [RFC4511] and [RFC4513], an LDAP session has an
"anonymous" association until the client has been successfully
authenticated using the Bind operation. Clients MUST NOT invoke the
"Who am I?" operation while any Bind operation is in progress,
including between two Bind requests made as part of a multi-stage

Bind operation. Where a whoami Request is received in violation of
this absolute prohibition, the server should return a whoami Response
with an operationsError resultCode.

4. Extending the "Who am I?" Operation with Controls

Future specifications may extend the "Who am I?" operation using the
control mechanism [RFC4511]. When extended by controls, the "Who am
I?" operation requests and returns the authorization identity the
server associates with the client in a particular context indicated
by the controls.

4.1. Proxied Authorization Control

The Proxied Authorization Control [RFC4370] is used by clients to
request that the operation it is attached to operate under the
authorization of an assumed identity. The client provides the
identity to assume in the Proxied Authorization request control. If
the client is authorized to assume the requested identity, the server
executes the operation as if the requested identity had issued the
operation.

As servers often map the asserted authzId to another identity
[RFC4513], it is desirable to request that the server provide the
authzId it associates with the assumed identity.

When a Proxied Authorization Control is be attached to the "Who am
I?" operation, the operation requests the return of the authzId the
server associates with the identity asserted in the Proxied
Authorization Control. The authorizationDenied (123) result code is
used to indicate that the server does not allow the client to assume
the asserted identity.

5. Security Considerations

Identities associated with users may be sensitive information. When
they are, security layers [RFC4511][RFC4513] should be established to
protect this information. This mechanism is specifically designed to
allow security layers established by a Bind operation to protect the
integrity and/or confidentiality of the authorization identity.

Servers may place access control or other restrictions upon the use
of this operation. As stated in Section 3, the server SHOULD
advertise this extension when it is willing and able to perform the
operation.

As with any other extended operations, general LDAP security
considerations [RFC4510] apply.

6. IANA Considerations

   The OID 1.3.6.1.4.1.4203.1.11.3 is used to identify the LDAP "Who am
   I?" extended operation. This OID was assigned [ASSIGN] by the
   OpenLDAP Foundation, under its IANA-assigned private enterprise
   allocation [PRIVATE], for use in this specification.

   Registration of this protocol mechanism [RFC4520] has been completed
   by the IANA.

   Subject: Request for LDAP Protocol Mechanism Registration
   Object Identifier: 1.3.6.1.4.1.4203.1.11.3
   Description: Who am I?
   Person & email address to contact for further information:
       Kurt Zeilenga <kurt@openldap.org>
   Usage: Extended Operation
   Specification: RFC 4532
   Author/Change Controller: IESG
   Comments: none

7. Acknowledgement

   This document borrows from prior work in this area, including
   "Authentication Response Control" [RFC3829] by Rob Weltman, Mark
   Smith, and Mark Wahl.

   The LDAP "Who am I?" operation takes it's name from the UNIX
   whoami(1) command. The whoami(1) command displays the effective user
   ID.

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.

   [RFC4370] Weltman, R., "Lightweight Directory Access Protocol (LDAP)
             Proxied Authorization Control", RFC 4370, February 2006.

   [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.

   [RFC4513] Harrison, R., Ed., "Lightweight Directory Access Protocol
             (LDAP): Authentication Methods and Security Mechanisms",
             RFC 4513, June 2006.

8.2. Informative References

   [RFC3829] Weltman, R., Smith, M., and M. Wahl, "Lightweight Directory
             Access Protocol (LDAP) Authorization Identity Request and
             Response Controls", RFC 3829, July 2004.

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

   [ASSIGN] OpenLDAP Foundation, "OpenLDAP OID Delegations",
             http://www.openldap.org/foundation/oid-delegate.txt.

   [PRIVATE] IANA, "Private Enterprise Numbers",
             http://www.iana.org/assignments/enterprise-numbers.

Author's Address

   Kurt D. Zeilenga
   OpenLDAP Foundation

   EMail: Kurt@OpenLDAP.org

Full Copyright Statement

Intellectual Property

Acknowledgement