Network Working Group
Request for Comments: 3062
Category: Standards Track

K. Zeilenga
OpenLDAP Foundation

February 2001

LDAP Password Modify Extended 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.

Copyright Notice

Copyright (C) The Internet Society (2001). All Rights Reserved.

Abstract

The integration of the Lightweight Directory Access Protocol (LDAP) and external authentication services has introduced non-DN authentication identities and allowed for non-directory storage of passwords. As such, mechanisms which update the directory (e.g., Modify) cannot be used to change a user’s password. This document describes an LDAP extended operation to allow modification of user passwords which is not dependent upon the form of the authentication identity nor the password storage mechanism used.

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", and "MAY" in this document are to be interpreted as described in RFC 2119.

1. Background and Intent of Use

Lightweight Directory Access Protocol (LDAP) [RFC2251] is designed to support an number of authentication mechanisms including simple user name/password pairs. Traditionally, LDAP users where identified by the Distinguished Name [RFC2253] of a directory entry and this entry contained a userPassword [RFC2256] attribute containing one or more passwords.

The protocol does not mandate that passwords associated with a user be stored in the directory server. The server may use any attribute suitable for password storage (e.g., userPassword), or use non-directory storage.

The integration [RFC2829] of application neutral SASL [RFC2222] services which support simple username/password mechanisms (such as DIGEST-MD5) has introduced non-LDAP DN authentication identity forms and made storage of passwords the responsibility of the SASL service provider.

LDAP update operations are designed to act upon attributes of an entry within the directory. LDAP update operations cannot be used to modify a user's password when the user is not represented by a DN, does not have a entry, or when that password used by the server is not stored as an attribute of an entry. An alternative mechanism is needed.

This document describes an LDAP Extended Operation intended to allow directory clients to update user passwords. The user may or may not be associated with a directory entry. The user may or may not be represented as an LDAP DN. The user's password may or may not be stored in the directory.

The operation SHOULD NOT be used without adequate security protection as the operation affords no privacy or integrity protect itself. This operation SHALL NOT be used anonymously.

2. Password Modify Request and Response

The Password Modify operation is an LDAPv3 Extended Operation [RFC2251, Section 4.12] and is identified by the OBJECT IDENTIFIER passwdModifyOID. This section details the syntax of the protocol request and response.

```
passwdModifyOID OBJECT IDENTIFIER ::= 1.3.6.1.4.1.4203.1.11.1

PasswdModifyRequestValue ::= SEQUENCE {
  userIdentity    [0]  OCTET STRING OPTIONAL
  oldPasswd       [1]  OCTET STRING OPTIONAL
  newPasswd       [2]  OCTET STRING OPTIONAL }

PasswdModifyResponseValue ::= SEQUENCE {
  genPasswd       [0]     OCTET STRING OPTIONAL }
```

2.1. Password Modify Request

A Password Modify request is an ExtendedRequest with the requestName field containing passwdModifyOID OID and optionally provides a requestValue field. If the requestValue field is provided, it SHALL contain a PasswdModifyRequestValue with one or more fields present.

The userIdentity field, if present, SHALL contain an octet string representation of the user associated with the request. This string may or may not be an LDAPDN [RFC2253]. If no userIdentity field is present, the request acts up upon the password of the user currently associated with the LDAP session.

The oldPasswd field, if present, SHALL contain the user's current password.

The newPasswd field, if present, SHALL contain the desired password for this user.

2.2. Password Modify Response

A Password Modify response is an ExtendedResponse where the responseName field is absent and the response field is optional. The response field, if present, SHALL contain a PasswdModifyResponseValue with genPasswd field present.

The genPasswd field, if present, SHALL contain a generated password for the user.

If an resultCode other than success (0) is indicated in the response, the response field MUST be absent.

3. Operation Requirements

Clients SHOULD NOT submit a Password Modification request without ensuring adequate security safeguards are in place. Servers SHOULD return a non-success resultCode if sufficient security protection are not in place.

Servers SHOULD indicate their support for this extended operation by providing PasswdModifyOID as a value of the supportedExtension attribute type in their root DSE. A server MAY choose to advertise this extension only when the client is authorized and/or has established the necessary security protections to use this operation. Clients SHOULD verify the server implements this extended operation prior to attempting the operation by asserting the supportedExtension attribute contains a value of PasswdModifyOID.

The server SHALL only return success upon successfully changing the user's password. The server SHALL leave the password unmodified and return a non-success resultCode otherwise.

If the server does not recognize provided fields or does not support the combination of fields provided, it SHALL NOT change the user password.

If oldPasswd is present and the provided value cannot be verified or is incorrect, the server SHALL NOT change the user password. If oldPasswd is not present, the server MAY use other policy to determine whether or not to change the password.

The server SHALL NOT generate a password on behalf of the client if the client has provided a newPasswd. In absence of a client provided newPasswd, the server SHALL either generate a password on behalf of the client or return a non-success result code. The server MUST provide the generated password upon success as the value of the genPasswd field.

The server MAY return adminLimitExceeded, busy, confidentialityRequired, operationsError, unavailable, unwillingToPerform, or other non-success resultCode as appropriate to indicate that it was unable to successfully complete the operation.

Servers MAY implement administrative policies which restrict this operation.

4. Security Considerations

This operation is used to modify user passwords. The operation itself does not provide any security protection to ensure integrity and/or confidentiality of the information. Use of this operation is strongly discouraged when privacy protections are not in place to guarantee confidentiality and may result in the disclosure of the password to unauthorized parties. This extension MUST be used with confidentiality protection, such as Start TLS [RFC 2830]. The NULL cipher suite MUST NOT be used.

5. Bibliography

[RFC2219] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2222] Myers, J., "Simple Authentication and Security Layer (SASL)", RFC 2222, October 1997.

[RFC2251] Wahl, M., Howes, T. and S. Kille, "Lightweight Directory Access Protocol (v3)", RFC 2251, December 1997.

[RFC2252] Wahl, M., Coulbeck, A., Howes, T. and S. Kille, "Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions", RFC 2252, December 1997.

[RFC2253] Wahl, M., Kille,S. and T. Howes, "Lightweight Directory Access Protocol (v3): UTF-8 String Representation of Distinguished Names", RFC 2253, December 1997.

[RFC2256] Wahl, M., "A Summary of the X.500(96) User Schema for use with LDAPv3", RFC 2256, December 1997.

[RFC2829] Wahl, M., Alvestrand, H., Hodges, J. and R. Morgan, "Authentication Methods for LDAP", RFC 2829, May 2000.

[RFC2830] Hodges, J., Morgan, R. and M. Wahl, "Lightweight Directory Access Protocol (v3): Extension for Transport Layer Security", RFC 2830, May 2000.

6. Acknowledgment

This document borrows from a number of IETF documents and is based upon input from the IETF LDAPext working group.

7. Author’s Address

Kurt D. Zeilenga
OpenLDAP Foundation

EMail: Kurt@OpenLDAP.org

8. Full Copyright Statement

Copyright (C) The Internet Society (2001). All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.