LDAPEXT Working Group
INTERNET-DRAFT PROPOSAL
Intended Category: Standards Track
Expires: TBD

Alan Lloyd
OpenDirectory

18 September 1998

Service Controls: LDAP-X.500 Alignment
<draft-lloyd-ldap-svcs-00.txt>

1. Status of this Memo

This document is a contribution.

LDAP Service Controls

2. Abstract

This document defines service controls that extend the LDAPv3 [LDAP] operations to provide a simple mechanism by which an LDAP client can select master or replica directory information, control chaining and specify other service requirements when connected to an **X.500 directory service. These service control mechanisms are not** required when LDAP clients are connected to a single(non X.500) LDAP server because, for example, chaining [X.518]is not supported by these servers.
Chaining protocols (DSP in X.500) also permit the extraction of master or replica data from within the X.500 directory system and provide this to the client (via LDAP) without the need for client based LDAP referrals to different servers.

In addition, the controls proposed provide major step in the "control" alignment of LDAP and DAP and their use of X.500. This will permit functional consistency to be achieved in directory enabled applications that use LDAP for access.

In order to distinguish this functionality from LDAP V3 capable systems, an upgrade to LDAP V4 is also proposed.

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 [KEYWORDS].

3. General Approach

The approach taken to implement the features required is to use the LDAP Controls mechanism and define this in an identical manner (as appropriate)as X.511. This field in LDAP has been provided for the very purpose. ie. to enable a LDAP client control directory services in the manner described. The controls already provided in LDAP such as size and time limit have not been included in the specification below. These will be used as per the current LDAP control definitions.

4. Service Controls

This control may be included in the Controls portion of any LDAPv3 message. The controlType is "2.16.840.1.TBD".
LDAP V3 defines the control field as:

```
Control ::= SEQUENCE {
               controlType             LDAPOID,
               criticality             BOOLEAN DEFAULT FALSE,
               controlValue            OCTET STRING OPTIONAL }
```

Where criticality is operationally required to be different for different service controls, a sequence of LDAP control elements can be provided with the critical service controls set in one LDAP Control element and non critical service controls set in another.

The Control Value field is encoded as follows:

```
          ServiceControls ::= SET {
                  Options
           options  ::=                [0]  BIT STRING {
               preferChaining         (0),
               chainingProhibited     (1),
               localScope             (2),
               dontUseCopy            (3),
               dontDereferenceAliases (4),
               subentries             (5),
               copyShallDo            (6),
               partialNameResolution  (7),
               manageDSAIT            (8) } DEFAULT {},
           priority               [1] INTEGER {low (0), medium (1),
                                    high (2)}DEFAULT medium,
           scopeOfReferral        [4]INTEGER
                                    {dmd(0),country(1)}OPTIONAL,
             attributeSizeLimit     [5]INTEGER OPTIONAL,
```

```
            manageDSAITPlaneRef    [6]SEQUENCE {
                                   dsaName Name,
                                agreementID  AgreementID }OPTIONAL }
```

Note: ASN.1 Context tags have kept in alignemnt with X.511.

4.1 Options

The options component contains a number of indications, each of which, if set, asserts the condition suggested. Thus:

a)preferChaining indicates that the preference is that chaining, rather than referrals, be used to provide the service. The Directory is not obliged to follow this preference.

b)chainingProhibited indicates that chaining, and other methods of distributing the request around the Directory, are prohibited.

c)localScope indicates that the operation is to be limited to a local scope. The definition of this option is itself a local matter, for example, within a single DSA/server or a single DMD.

d)dontUseCopy indicates that copied information (as defined in ITU-T Rec. X.518 | ISO/IEC 9594-4)shall not be used to provide the service.

e)dontDereferenceAliases indicates that any alias used to identify the entry affected by an operation is not to be dereferenced.

NOTE 1 This control may be used instead of the LDAP alias controls provided in the LDAP search. However, in order to maintain compatability, the search parameters should be used in preference.

f)subentries indicates that a Search (or List) operation is to access subentries only; normal entries become inaccessible i.e. the Directory behaves as though normal entries do not exist. If this service control is not set, then the operation accesses normal entries only and subentries become inaccessible. The service control is ignored for operations other than Search or List.

NOTE 2 The effects of subentries on access control, schema, and collective attributes are still observed even if subentries are inaccessible.

NOTE 3 If this service control is set, normal entries may still be

specified as the base object of an operation.

NOTE 4 The List operation is not yet supported in LDAP. This will be the subject of another proposal.

g) copyShallDo indicates that if the Directory is able to partly but not fully satisfy a query at a copy of an entry, it shall not chain the query. It is meaningful only if dontUseCopy is not set. If copyShallDo is not set, the Directory will use shadow data only if it is sufficiently complete to allow the operation to be fully satisfied at the copy. A query may be only partially satisfied because some of the requested attributes are missing in the shadow copy, because some of the attribute values for a given attribute are missing in the shadow copy, because the DSA does not hold all context information for the attribute values it does have, or because the DSA holding the shadowed data does not support all of the matching rules on that data. If copyShallDo is set and the Directory is not able to fully satisfy a query, it shall set incompleteEntry in the the returned entry information.

h)partialNameResolution indicates that if the Directory is able to resolve only part of the purported name in a Read or Search operation, i.e. it is about to return a nameError, the entry whose name consists of all resolved RDNs is to be considered the target of the operation and partialName is set to TRUE in the result. This service control is ignored for operations other than Read or Search.

Note 5 If this service control is set, the purported name is a context prefix entry to which access is denied, and the requestor has access to the superior entry, then the existence of the context prefix entry will be indirectly disclosed to the requestor even if DiscloseOnError permission to the entry is denied.

NOTE 6 The Read operation is not yet supported in LDAP. This will be the subject of another proposal.

4.2 Priority

The priority (low, medium, or high) at which the service is to be provided. Note that this is not a guaranteed service in that the Directory, as a whole, does not implement queuing. There is no relationship implied with the use of priorities in underlying layers.

4.3 Scope of Referral

The scopeOfReferral indicates the scope to which a referral returned by a DSA should be relevant. Depending on whether the values dmd or

country are selected, only referrals to other DSAs within the selected scope shall be returned. This applies to the referrals in both a Referral error and the unexplored parameter of List and Search results.

NOTE 1 The List operation is not yet supported in LDAP. This will be the subject of another proposal.

4.4 Attribute Size Limit

The attributeSizeLimit indicates the largest size of any attribute (i.e. the type and all its values) that is included in returned entry information. If an attribute exceeds this limit, all of its values are omitted from the returned entry information and incompleteEntry is set in the returned entry information. The size of an attribute is taken to be its size in octets in the local concrete syntax of the DSA holding the data. Because of different ways applications store the data, the limit is imprecise. If this parameter is not specified, no limit is implied.

NOTE 1 Attribute values returned as part of an entry's Distinguished Name are exempt from this limit.

4.5 ManageDSAITPlaneRef

The manageDSAITPlaneRef indicates that the operation has been requested by an administrative user so that a specific replication plane of the DSA Information Tree is managed. The manageDSAITPlaneRef service control is ignored if the manageDSAIT option is not set. The plane is identified by the dsaName component which is the name of the supplying DSA and the agreementID component which contains the shadowing agreement identifier.

It is noted that LDAP servers may have some functionality for managing their DITs. This control is used where the administrative client wishes to manage an X.500 system via LDAP (subject to authorisation and access controls, and in addition manage LDAP servers using the standard LDAP server approaches.

5. Service Combinations

Certain combinations of priority, timeLimit, and sizeLimit may result in conflicts. For example, a short time limit could conflict with low priority; a high size limit could conflict with a low time limit, etc.

6. Compliance

Upon receiving this control, a server that supports it MUST process this as a standard LDAPv3 operation.

Compliance to the support of the above controls will be specified in the respective Server or Client profiles or X.500/DAP/LDAP ISPs.

7. Security Considerations

In some situations, it may be important to prevent general exposure of information from directory services which support these controls. Therefore,servers (DSAs) that implement the mechanism described in this document SHOULD provide a means to enforce use authentication and access control on the entries and control information returned and possibly prevent the selection of these controls via pre configured default values.

8. Associated Proposals

This proposal accompanies a proposal to align the service control aspects of LDAP V3 and X.511.
draft-lloyd-ldap-list-read-00.txt

9. Acknowledgements

This document is an update to RFC 2251, by Mark. Wahl, ,Tim Howes, and Steve Kille. Design ideas included in this document are based on those provided in the X.500 ISO/ITU specifications. The contributions of individuals in these working groups is gratefully acknowledged.

10. Copyright

TBS

11. Bibliography

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

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

[X.208] CCITT Recommendation X.208: Specification of Abstract Syntax Notation One (ASN.1), 1988.

[X.501] ITU-T Recommendation X.501: Information Technology - Open Systems Interconnection - The Directory: Models, 1993.

[X.509] ITU-T Recommendation X.509 (1997 E): Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, June 1997.

[X.511] ITU-T Recommendation X.511: Information Technology - Open Systems Interconnection - The Directory: Abstract Service Definition(DAP), 1993/7.

[X.518] ITU-T Recommendation X.511: Information Technology - Open Systems Interconnection - The Directory: Procedures for Distributed Operations(DSP),1993

[X.520] ITU-T Recommendation X.520: Information Technology - Open Systems Interconnection - The Directory: Selected Attribute Types, 1993.

[X.521] ITU-T Recommendation X.520: Information Technology - Open Systems Interconnection - The Directory: Selected Object Classes, 1993.

[X.525] ITU-T Recommendation X.511: Information Technology - Open Systems Interconnection - The Directory: Replication (DISP), 1993.

9. Author's Addresses

Alan Lloyd
OpenDirectory Pty Ltd.
266 Maroondah Highway
Mooroolbark
Melbourne Vic 3138
Australia
+61 3 9727 8900
mobile + 61 416 536 749
alan.lloyd@opendirectory.com.au