MIME Directory Profile for LDAP Schema

Status of this Memo

   This memo provides information for the Internet community. It does
   not specify an Internet standard of any kind. Distribution of this
   memo is unlimited.

Copyright Notice

Abstract

   This document defines a multipurpose internet mail extensions (MIME)
   directory profile for holding a lightweight directory access protocol
   (LDAP) schema. It is intended for communication with the Internet
   schema listing service.

   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 RFC 2119 [4].

1. Overview

   This document defines how a MIME type may be used to transfer a
   single LDAPv3 schema definition.

   A schema for use with LDAPv3 consists of any number of object class,
   attribute type, matching rule and syntax definitions. These concepts
   are defined in the LDAPv3 protocol definition [2]. The schema MAY
   have a numeric OID assigned to it by a schema listing or registration
   service.

   A schema may import definitions from another schema. Schema imports
   are not, however, transitive.

   For example, a schema contains a definition for a "modem" object
   class, which is to be defined as a subclass of the X.521 "device"
   object class. In this case, the schema MUST import the definitions
   of X.521.

2. The "schema-ldap-0" MIME Directory Profile Registration

   This profile is identified by the following registration template
   information.

   To: ietf-mime-direct@imc.org
   Subject: Registration of text/directory MIME profile "schema-ldap-0"

   Profile name: schema-ldap-0

   Profile purpose: To represent a schema defined for use with LDAPv3
   servers.

   Profile types: SOURCE, ldapSchemas, attributeTypes, matchingRules,
   objectClasses, matchingRuleUse, ldapSyntaxes

   Profile special notes:

   The charset parameter MUST be present on the MIME content, and the
   value of this parameter MUST be "utf-8". This ensures that schema
   values can be used in LDAPv3 attribute values without a character set
   translation.

   Neither the "BEGIN" and "END" types nor type grouping are used in
   contents of this profile.

   All of the types in this profile with the exception of ldapSchemas
   may be multi-valued. Each value is present on its own contentline.
   Values may be present in any order, and need not be arranged by type.

   The "SOURCE" type is optional, and if values are present they SHOULD
   be URIs of the "ldap" form. If the URI is of the "ldap" form, the
   object indicated by the URI is a subschema entry. The use of other
   forms are reserved for future applications.

   In this version of the profile, exactly one value of the ldapSchemas
   type MUST be present. (Later versions of the profile may permit
   multiple ldapSchemas values to be present in a content.)

   Implementors should note that there will likely be values of the
   profile types in most contents much longer than 76 bytes. In
   addition, there may be non-ASCII characters and embedded CRLFs inside
   of values, which could require either quoting of the value or use of
   a content transfer encoding.

If a contentline in a particular content contains a "context"
parameter and the value of that parameter is not "ldap", then that
contentline SHOULD be ignored.

Intended usage: COMMON

3. MIME Directory Type Registrations

This document defines all the types, with the exception of "SOURCE"
used in the schema-ldap-0 profile. The "SOURCE" type is defined in
[1]. These types are primarily intended for use in the "schema-
ldap-0" directory profile, although they may be applicable to other
profiles defined in the future.

3.1. ldapSchemas

To: ietf-mime-direct@imc.org
Subject: Registration of text/directory MIME type ldapSchemas

Type name: ldapSchemas

Type purpose: To represent the LDAPv3 attribute "ldapSchemas",
defined in section A.1.

Type encoding: 8bit

Type valuetype: text, encoded according to the BNF of section A.2.

Type special notes: Each value of this type specifies the contents of
an LDAP schema definition. A definition of each object class,
attribute, matching rule, matching rule use and syntax referenced in
a value of ldapSchemas MUST either be defined in one of the schemas
referenced in the "IMPORTS" field, or present in the content
containing this value.

Intended usage: COMMON

3.2. attributeTypes

To: ietf-mime-direct@imc.org
Subject: Registration of text/directory MIME type attributeTypes

Type name: attributeTypes

Type purpose: To represent the LDAPv3 attribute "attributeTypes",
defined in section 5.1.6 of [4].

Type encoding: 8bit

   Type valuetype: text, encoded according to the BNF of
   "AttributeTypeDescription" given in section 4.2 of [4].

   Type special notes: Each value of the type specifies one LDAPv3
   attribute type definition. The syntax and matching rules referenced
   in a value of attributeTypes MUST either be present in this content,
   or defined in one of the schemas referenced in the "IMPORTS" field of
   the ldapSchemas line.

   Intended usage: COMMON

3.3. matchingRules

   To: ietf-mime-direct@imc.org
   Subject: Registration of text/directory MIME type matchingRules

   Type name: matchingRules

   Type purpose: To represent the LDAPv3 attribute "matchingRules",
   defined in section 5.1.8 of [4].

   Type encoding: 8bit

   Type valuetype: text, encoded according to the BNF of
   "MatchingRuleDescription" given in section 4.5 of [4].

   Type special notes: Each value of the type specifies one matching
   rule definition. The syntax reference in a value of matchingRules
   MUST either be present in this content, or defined in one of the
   schemas referenced in the "IMPORTS" field of the ldapSchemas line.

   Intended usage: COMMON

3.4. objectClasses

   To: ietf-mime-direct@imc.org
   Subject: Registration of text/directory MIME type objectClasses

   Type name: objectClasses

   Type purpose: To represent the LDAPv3 attribute "objectClasses",
   defined in section 5.1.7 of [4].

   Type encoding: 8bit

   Type valuetype: text, encoded according to the BNF of
   "ObjectClassDescription" given in section 4.4 of [4].

   Type special notes: Each value of the type specifies one LDAPv3
   object class definition. The attributes and object classes
   referenced in a value of objectClasses MUST either be present in this
   content, or defined in one of the schema referenced in the "IMPORTS"
   field of the ldapSchemas line.

   Intended usage: COMMON

3.5. matchingRuleUse

   To: ietf-mime-direct@imc.org
   Subject: Registration of text/directory MIME type matchingRuleUse

   Type name: matchingRuleUse

   Type purpose: To represent the LDAPv3 attribute "matchingRuleUse",
   defined in section 5.1.9 of [4].

   Type encoding: 8bit

   Type valuetype: text, encoded according to the BNF of
   "MatchingRuleUseDescription" given in section 4.5 of [4].

   Type special notes: Each value of the type specifies a relationship
   between a matching rule and attribute types. The matching rule and
   attribute types referenced in a value of matchingRuleUse MUST either
   be present in this content, or defined in one of the schemas
   referenced in the "IMPORTS" statement of the ldapSchemas line.

   Intended usage: COMMON

3.6. ldapSyntaxes

   To: ietf-mime-direct@imc.org
   Subject: Registration of text/directory MIME type ldapSyntaxes

   Type name: ldapSyntaxes

   Type purpose: To represent the LDAPv3 attribute "ldapSyntaxes",
   defined in section 5.3.1 of [3].

   Type encoding: 8bit

   Type valuetype: text, encoded according to the BNF of
   "SyntaxDescription" given in section 4.3.3 of [3].

Type special notes: Each value of this type specifies a single LDAPv3
attribute value syntax.

Intended usage: COMMON

3. Example

```
From: Whomever@wherever.com
To: Someone@somewhere.com
Subject: schema information
MIME-Version: 1.0
Message-Id: <ids1@wherever.com>
Content-Type: text/directory; profile="schema-ldap-0";charset="utf-8"
Content-Transfer-Encoding: Quoted-Printable
ldapSchemas: ( 1.2.3.4 NAME 'bogus schema' CLASSES ( top $ thing ) =
ATTRIBUTES ( objectClass $ name ) SYNTAXES ( =
1.3.6.1.4.1.1466.115.121.1.38 $ 1.3.6.1.4.1.1466.115.121.1.15 ) )
attributeTypes: ( 2.5.4.0 NAME 'objectClass' SYNTAX =
1.3.6.1.4.1.1466.115.121.1.38 )
objectClasses: ( 2.5.6.0 NAME 'top' ABSTRACT MUST objectClass )
attributeTypes: ( 2.5.4.41 NAME 'name' SYNTAX =
1.3.6.1.4.1.1466.115.121.1.15{32768} )
objectClasses: ( 2.5.6.999 NAME 'thing' MUST name )
ldapSyntaxes: ( 1.3.6.1.4.1.1466.115.121.1.15 DESC 'String' )
ldapSyntaxes: ( 1.3.6.1.4.1.1466.115.121.1.38 DESC 'OID' )
```

4. Security Considerations

A MIME body part containing an text/directory of the schema-ldap-0
profile may be incorporated in a digitally signed MIME content, which
can be used to verify that the body part has not been modified in
transit. When the signer has been certified by a trusted third party
service, it may also be possible to verify the origin of the content.

5. Bibliography

   [1] Howes, T., Smith, M. and F. Dawson, "A MIME Content-Type for
       Directory Information", RFC 2425, September 1998.

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

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

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

6. Author's Address

Mark Wahl
Sun Microsystems, Inc.
8911 Capital of Texas Hwy Suite 4140
Austin, TX 78759
USA

EMail: Mark.Wahl@sun.com

Appendix A

   This appendix defines two new attributes which could be present in an
   subschema entry. These attributes could be added to a future
   revision of the LDAP attribute definition [3].

A.1. ldapSchemas attribute type definition

       (1.3.6.1.4.1.1466.101.120.17 NAME 'ldapSchemas'
         SYNTAX 1.3.6.1.4.1.1466.115.121.1.56 USAGE directoryOperation)

   Each value of the ldapSchemas attribute defines one schema. Its
   syntax, given in section A.2, contains the elements needed for an
   LDAPv3 server to correctly process operations which use the
   definitions from this syntax.

A.2. LDAP Schema Definition syntax definition

       (1.3.6.1.4.1.1466.115.121.1.56 DESC 'LDAP Schema Definition')

   Values in this syntax are represented according to the following BNF:

      LdapSchema = "(" whsp
        numericoid whsp
        ["NAME" qdescrs]
        ["OBSOLETE" whsp]
        ["IMPORTS" oids]
        ["CLASSES" oids]
        ["ATTRIBUTES" oids]
        ["MATCHING-RULES" oids]
        ["SYNTAXES" oids]
        whsp ")"

   The numericoid field uniquely identifies the schema. A new OID
   should be assigned if any of the fields of the schema change. It is
   not possible to import definitions from a schema until an OID has
   been assigned to it.

   The "NAME" field contains optional human-readable labels for the
   schema.

   The "OBSOLETE" field is present if the schema is obsolete.

   The "IMPORTS" field lists the OIDs of other schemas which are to be
   incorporated by reference into this schema. It is an error to have
   an attribute type or object class defined in a schema with the same
   name but a different OID as an attribute type or object class in an

imported schema. It is also an error to import from two schema
definitions in which there are attribute types or object classes with
the same names but different OIDs.

The "CLASSES" field lists the OIDs of object classes defined in this
schema. A schema need not contain any object class definitions. A
schema must not contain two object class definitions of the same name
but with different OIDs.

The "ATTRIBUTES" field lists the OIDs of attribute types defined in
this schema. A schema need not contain any object class definitions.
A schema must not contain two attribute type definitions of the same
name but with different OIDs.

The "MATCHING-RULES" field lists the OIDs of matching rules defined
in this schema. A schema need not contain any matching rules.

The "SYNTAXES" field lists the OIDs of syntaxes defined in this
schema. A schema need not contain any syntaxes.

Full Copyright Statement

Acknowledgement