

A String Representation of LDAP Search Filters

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.

1. Abstract

The Lightweight Directory Access Protocol (LDAP) [1] defines a network representation of a search filter transmitted to an LDAP server. Some applications may find it useful to have a common way of representing these search filters in a human-readable form. This document defines a human-readable string format for representing LDAP search filters.

2. LDAP Search Filter Definition

An LDAP search filter is defined in [1] as follows:

```
Filter ::= CHOICE {  
    and                [0] SET OF Filter,  
    or                  [1] SET OF Filter,  
    not                 [2] Filter,  
    equalityMatch        [3] AttributeValueAssertion,  
    substrings           [4] SubstringFilter,  
    greaterOrEqual       [5] AttributeValueAssertion,  
    lessOrEqual          [6] AttributeValueAssertion,  
    present              [7] AttributeType,  
    approxMatch          [8] AttributeValueAssertion  
}
```

```
SubstringFilter ::= SEQUENCE {  
    type      AttributeType,  
    SEQUENCE OF CHOICE {  
        initial    [0] LDAPString,  
        any         [1] LDAPString,  
        final       [2] LDAPString  
    }  
}
```

```
AttributeValueAssertion ::= SEQUENCE {
    attributeType  AttributeType,
    attributeValue  AttributeValue
}
```

```
AttributeType ::= LDAPString
```

```
AttributeValue ::= OCTET STRING
```

```
LDAPString ::= OCTET STRING
```

where the LDAPString above is limited to the IA5 character set. The AttributeType is a string representation of the attribute type name and is defined in [1]. The AttributeValue OCTET STRING has the form defined in [2]. The Filter is encoded for transmission over a network using the Basic Encoding Rules defined in [3], with simplifications described in [1].

3. String Search Filter Definition

The string representation of an LDAP search filter is defined by the following grammar. It uses a prefix format.

```
<filter> ::= '(' <filtercomp> ')'
<filtercomp> ::= <and> | <or> | <not> | <item>
<and> ::= '&' <filterlist>
<or> ::= '|' <filterlist>
<not> ::= '!' <filter>
<filterlist> ::= <filter> | <filter> <filterlist>
<item> ::= <simple> | <present> | <substring>
<simple> ::= <attr> <filtertype> <value>
<filtertype> ::= <equal> | <approx> | <greater> | <less>
<equal> ::= '='
<approx> ::= '~='
<greater> ::= '>='
<less> ::= '<='
<present> ::= <attr> '='
<substring> ::= <attr> '=' <initial> <any> <final>
<initial> ::= NULL | <value>
<any> ::= '*' <starval>
<starval> ::= NULL | <value> '*' <starval>
<final> ::= NULL | <value>
```

<attr> is a string representing an AttributeType, and has the format defined in [1]. <value> is a string representing an AttributeValue, or part of one, and has the form defined in [2]. If a <value> must contain one of the characters '*' or '(' or ')', these characters should be escaped by preceding them with the backslash '\' character.

Note that although both the <substring> and <present> productions can produce the 'attr=*' construct, this construct is used only to denote a presence filter.

4. Examples

This section gives a few examples of search filters written using this notation.

```
(cn=Babs Jensen)
(! (cn=Tim Howes))
(& (objectClass=Person) (| (sn=Jensen) (cn=Babs J*)))
(o=univ*of*mich*)
```

5. Security Considerations

Security considerations are not discussed in this memo.

6. Bibliography

- [1] Yeong, W., Howes, T., and S. Kille, "Lightweight Directory Access Protocol", RFC 1777, March 1995.
- [2] Howes, R., Kille, S., Yeong, W., and C. Robbins, "The String Representation of Standard Attribute Syntaxes", RFC 1778, March 1995.
- [3] Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1). CCITT Recommendation X.209, 1988.

7. Author's Address

Tim Howes
University of Michigan
ITD Research Systems
535 W William St.
Ann Arbor, MI 48103-4943
USA

Phone: +1 313 747-4454
EMail: tim@umich.edu

