Tuning LDAP to Improve Searches in Communications Services Clients

Sun Java™ Enterprise System Technical Note

Sun Microsystems, Inc.
4150 Network Circle
Santa Clara, CA 95054
U.S.A.

Part No: 819–5201

060206@13215

Tuning LDAP to Improve Searches in Communications Services Clients

All the client products that are released with Sun Java™ System Communications Services allow users to search the corporate directory and their own address books. While search does work, some LDAP tuning might improve the user experience. This technical note provides some tips for improving searches in the Sun Java System Communications Express and Sun Java System Connector for Microsoft Outlook client products.

This technical note contains the following sections:

Technical Note Revision History

Version	Date	Description of Changes
1.0	February 2006	Initial release of this technical note.

Setting up International Searches

Whether you use Communications Express or Connector for Microsoft Outlook, your search in your personal contacts or the public address book for a particular string is a locale-specific operation. For example, a French user searching for "Gaelle" expects to get back entries containing the string "Gaelle" but also any entry containing the string "Gaëlle."

The various rules driving the way entries are presented to a user based on locale are called *collation rules* or *collation order*. The collation order provides language and cultural-specific information about how the characters of a given language are to be sorted. These rules identify the sequence of the letters in the alphabet, how to compare letters with accents to letters without accents, and characters that can be ignored when comparing strings. The collation order also takes into account culture-specific information about a language, such as the direction in which the language is read (left to right, right to left, or up and down).

The Sun Java System Directory Server supports a large variety of locales and collation rules (See "Identifying Supported Locales" in the *Sun Java System Directory Server 5 2005Q1 Administration Reference*). Depending on your user base, you first need to choose the locale for your environment. In the example below, we use the English (US) locale (OID = 1.3.6.1.4.1.42.2.27.9.4.34.1).

To specify which locale to use when performing a search, use the matching rule filter syntax, described in "Searching an Internationalized Directory" in the *Sun Java System Directory Server 5 2005Q1 Administration Reference*. This syntax lets you specify the locale as well as the type of search (equality, substring, and so on).

The following filter will perform a substring comparison (.6) on the CN attribute, using the English (US) collation rules (1.3.6.1.4.1.42.2.27.9.4.34.1). The filter looks at the CN for strings starting with `Gae`:

```
cn:1.3.6.1.4.1.42.2.27.9.4.34.1.6:=Gae*
```

Updating the Indexes for International Searches

During an LDAP search, most performance problems occur because indexes are not present or are not properly configured. By default, the Directory Server is configured so that lookups issued by Communications Express or by Connector for Microsoft Outlook are indexed and should return in a reasonable amount of time. Nevertheless, the Directory Server is not set up for international searches. you must alter the existing indexes so that they take into account the collation rules that have been chosen. How to alter the indexes is described in the "Managing Indexes" section in the *Sun Java System Directory Server 5 2005Q1 Administration Guide*.

For example, the CN attribute is indexed by default in the `userRoot` suffix:

```
ldapsearch -D "cn=Directory manager" -b
"cn=cn,cn=index,cn=userRoot,cn=ldbm database,cn=plugins,cn=config"
"objectclass=*"
cn=cn,cn=index,cn=userRoot,cn=ldbm database,cn=plugins,cn=config
objectClass=top objectClass=nsIndex
cn=cn
nsSystemIndex=false
nsIndexType=pres
nsIndexType=eq
nsIndexType=sub
```

To enable the indexes for international searches using the English (US) collation rules, add one `nsMatchingRule` attribute with the English (US) OID. The clients perform substring searches, so add the substring suffix (`.6`) to the OID :

```
ldapmodify -D "cn=Directory manager"
dn: cn=cn,cn=index,cn=userRoot,cn=ldbm database,cn=plugins,cn=config
changetype: modify
add: nsMatchingRule
nsMatchingRule: 1.3.6.1.4.1.42.2.27.9.4.34.1.6
```

Note – Do not add a space, tab, or other non-visible characters at the beginning or at the end of the value.

The `nsMatchingRule` attribute is a multivalued attribute. Different types of searches for the same OID, or different OIDs can be added.

Run the `db2index.pl` script located under *server-root*`/slapd-instance`:

```
perl db2index.pl -D "cn=Directory Manager" -w \
secret -n userRoot -t cn
```

This script runs online and might take some time to finish. Alternatively, reinitialize the suffix. See "Reinitializing a Suffix" in the *Sun Java System Directory Server 5 2005Q1 Administration Guide*.

Use console to add the `nsMatchingRule` attribute (see the "Managing Indexes" section in the *Sun Java System Directory Server 5 2005Q1 Administration Guide*).

See the following sections for the indexes that need to be modified. Ensure that no non-indexed searches are performed by looking at the Directory Server access log file and for a `notes=U` in the search results.

Setting up the Search Filter in Communications Express

You must change the search filter used by Communications Express to accommodate the matching rule syntax through the collation rule parameters specified in the `db_config.properties` file. The file resides under *deployed-path*`/WEB-INF/ldappstore` for personal store and *deployed-path*`/WEB-INF/corp-dir` for corporate directory.

The parameters are:

```
# Collation Rule
# Uncomment below to apply collation rule
#
# collation_rule=en-US
```

```
#
# Search Fields for which collation rule should be applied.
# The fields provided here should be disambiguator formatted fields
# e.g. entry/displayname, person/givenname etc.
# Uncomment below to supply the comma-separated fields
#
# search_fields=entry/displayname
```

Uncomment the `collation_rule` and `search_fields` parameters to enable the collation rule. In order to specify a separate set of field or fields in the search, change the value of `search_fields` to the desired values. The `collation_rule` can contain either the language tag or the OID corresponding to that language (in the example 1.3.6.1.4.1.42.2.27.9.4.34.1) without the suffix specifying the type of search. The Web Container instance needs to be started after making the change.

Index the following attributes on the LDAP Server for international search against Communications Express:

- `cn` (under the `ou=people/ou=groups` suffix)
- `displayname` (under the `o=piServerDb` suffix)

Allowing Anonymous Access to the Corporate Directory

The Connector for Microsoft Outlook can be configured to bind using a DN and password or to bind as anonymous. To enable anonymous access to the corporate directory, add an Access Control Instruction (ACI) at the root level of the `ou=people/ou=group` sub-trees.

For example, if the root level is `dc=red,dc=sesta,dc=com`, add the following ACI:

```
ldapmodify -D "cn=Directory manager"
dn: dc=red,dc=sesta,dc=com
changetype: modify
add: aci
aci: (targetattr != "userPassword")
  (version 3.0;acl "Anonymous access";
  allow (read,compare,search)
  (userdn = "ldap:///anyone");)
```

For more information about ACI issues and limitations with Connector for Microsoft Outlook see *Avoiding ACI Problems with Outlook Connector*

Allowing Directory Browsing

New in this release, Connector for Microsoft Outlook 7 2005Q4 allows the end user to browse directories. When the user brings up the address book page, the user sees the first 10 entries in the directory. The user can scroll up and down or type a few characters and see the results automatically refreshed. This is a change from previous versions of Connector for Microsoft Outlook where the user was only able to search for one particular user.

To enable this feature while keeping good performance, the connector relies on two LDAP control extensions called Virtual List View (VLV) and Server Side Sorting of Search Results (RFC 2891). The following `ldapsearch` example returns the list of supported controls:

```
ldapsearch -s base "objectclass=*" supportedControl
supportedControl=2.16.840.1.113730.3.4.2
supportedControl=2.16.840.1.113730.3.4.3
supportedControl=2.16.840.1.113730.3.4.4
supportedControl=2.16.840.1.113730.3.4.5
supportedControl=1.2.840.113556.1.4.473  ------> Server Side Sort Control
supportedControl=2.16.840.1.113730.3.4.9 ------> VLV Control
supportedControl=2.16.840.1.113730.3.4.16
supportedControl=2.16.840.1.113730.3.4.15
supportedControl=2.16.840.1.113730.3.4.17
supportedControl=2.16.840.1.113730.3.4.19
supportedControl=1.3.6.1.4.1.42.2.27.9.5.2
supportedControl=1.3.6.1.4.1.42.2.27.9.5.6
supportedControl=2.16.840.1.113730.3.4.14
supportedControl=1.3.6.1.4.1.1466.29539.12
supportedControl=2.16.840.1.113730.3.4.12
supportedControl=2.16.840.1.113730.3.4.18
supportedControl=2.16.840.1.113730.3.4.13
```

The Sun Java System Directory Server supports both controls. Nevertheless, the VLV control is by default only available to authenticated users:

```
ldapsearch -D "cn=Directory Manager" -b \
"oid=2.16.840.1.113730.3.4.9,cn=features,cn=config" \
"objectclass=*" aci

oid=2.16.840.1.113730.3.4.9,cn=features,cn=config
aci=(targetattr != "aci")(version 3.0; acl "VLV Request Control"; \
allow( read, search, compare, proxy ) userdn = "ldap:///all";)
```

To grant anonymous access to the VLV control, add the corresponding ACI:

```
ldapmodify -D "cn=Directory Manager"
dn: oid=2.16.840.1.113730.3.4.9,cn=features,cn=config
changetype: modify
add: aci
aci: (targetattr !="aci")\
```

```
(version 3.0; acl "VLV Request Control"; allow (compare,read,search) \
userdn = "ldap:///anyone"; )
```

To improve the performance of searches requiring VLV plus Sort, create a Browsing Index in the Directory Server (as described in "Managing Browsing Indexing" in the *Sun Java System Directory Server 5 2005Q1 Administration Guide*). Each Browsing Index is specific to one base DN, search filter, scope, and sorting attribute. The VLV settings can be tuned on the client side using the deployment configuration tool.

In that particular case, create a Browsing Index for a base dn equal to `dc=red,dc=sesta,dc=com`, a filter equal to `(&(mail=*)(cn=*))`, using a sort on the `cn` attribute. The Browsing Index information is added into the configuration containing the base `dn` (in this case `userRoot`):

```
ldapmodify -D "cn=Directory Manager"
dn: cn=Browsing red.sesta.com,cn=userRoot,
cn=ldbm database,cn=plugins,cn=config
changetype: add
objectClass: top
objectClass: vlvSearch
cn: Browsing red.sesta.com
vlvbase: dc=red,dc=sesta,dc=com
vlvscope: 2
vlvfilter: (&(mail=*)(cn=*))
aci: (targetattr="*")
(version 3.0; acl "VLV for Anonymous";
allow (read,search,compare)
userdn="ldap:///anyone";)
dn: cn=Sort by cn, cn=Browsing red.sesta.com,cn=userRoot,
cn=ldbm database,cn=plugins,cn=config
changetype: add
objectClass: top
objectClass: vlvIndex
cn: Sort by cn
vlvSort: cn
```

Next run the `vlvindex` command located under *serverroot*`/slapd-`*instance*:

```
./vlvindex -n userRoot -T "Sort by cn"
```

Accessing Sun Resources Online

The docs.sun.com[SM] web site enables you to access Sun technical documentation online. You can browse the docs.sun.com archive or search for a specific book title or subject. Books are available as online files in PDF and HTML formats. Both formats are readable by assistive technologies for users with disabilities.

To access the following Sun resources, go to `http://www.sun.com`:

- Downloads of Sun products
- Services and solutions
- Support (including patches and updates)
- Training
- Research
- Communities (for example, Sun Developer Network)

Third-Party Web Site References

Third-party URLs are referenced in this document and provide additional, related information.

Note – Sun is not responsible for the availability of third-party web sites mentioned in this document. Sun does not endorse and is not responsible or liable for any content, advertising, products, or other materials that are available on or through such sites or resources. Sun will not be responsible or liable for any actual or alleged damage or loss caused or alleged to be caused by or in connection with use of or reliance on any such content, goods, or services that are available on or through such sites or resources.

Sun Welcomes Your Comments

Sun is interested in improving its documentation and welcomes your comments and suggestions. To share your comments, go to `http://docs.sun.com` and click Send Comments. In the online form, provide the full document title and part number. The part number is a 7-digit or 9-digit number that can be found on the book's title page or in the document's URL. For example, the part number of this book is 819-5201-10.