Novell LDAP Proxy 1.0 Linux Readme

October 27, 2011

Novell LDAP Proxy 1.0 is a powerful application that acts as a middleware layer between LDAP clients and LDAP directory servers. The benefits of using this proxy server include enhanced security, scalability, high availability, and direct access control to directory services.

1 Installation

- Section 1.1, "System Requirements," on page 1
- Section 1.2, "Installing the LDAP Proxy," on page 2
- Section 1.3, "Installing NLPManager," on page 2

1.1 System Requirements

The minimum operating system requirements and hardware requirements for installing the LDAP Proxy are as follows:

- Section 1.1.1, "Operating Systems Requirements," on page 1
- Section 1.1.2, "Hardware Requirements," on page 1

1.1.1 Operating Systems Requirements

The LDAP Proxy Server and NLP Manager can be installed on the following 32-bit and 64-bit operating systems:

  - SUSE Linux Enterprise Server (SLES) 10 SP4
  - SLES 11 SP1
  - Red Hat Enterprise Linux (RHEL) 5.6
  - Red Hat Enterprise Linux 6.0

IMPORTANT: Ensure that you install 32-bit LDAP Proxy on a 32-bit platform and 64-bit LDAP Proxy on a 64-bit platform.

1.1.2 Hardware Requirements

In addition to the platform requirements mentioned above, ensure that you have the following resource requirements in order to install and configure the LDAP Proxy Server and the NLP Manager:

- For LDAP Proxy Server:
  - A minimum of 128 MB of RAM
  - A minimum of 30 MB of disk space

- For NLPManager:
  - A minimum of 1 GB RAM
  - A minimum of 256 MB disk space

IMPORTANT: You must install the `libstdc++.so.5` and `libstdc++.so.6` libraries on your system before installing the LDAP Proxy.

1.2 Installing the LDAP Proxy

Use the `nlp-install` command in the `ldapproxy` directory for installing the Novell LDAP Proxy:

```
./nlp-install
```

For more information on installing the Novell LDAP Proxy, refer to the *Novell LDAP Proxy 1.0 Installation Guide* (http://www.novell.com/documentation/ldapproxy/ldapin/index.html?page=/documentation/ldapproxy/ldapin/data/index.html).

1.3 Installing NLPManager

You can download Novell NLPManager from the Novell Downloads (http://download.novell.com/index.jsp).

For more information on installing NLPManager, refer to the *Novell LDAP Proxy 1.0 Administration Guide* (http://www.novell.com/documentation/ldapproxy/admin/data/bookinfo.html).

2 Known Issues

- Section 2.1, “Installation Dependency,” on page 3
- Section 2.2, “Unable to Block Search Selection Attribute,” on page 3
- Section 2.3, “Using SSL Clients,” on page 4
- Section 2.4, “Using a Connection Pool,” on page 4
- Section 2.5, “NLPManager Throws a NullPointerException Error,” on page 4
- Section 2.6, “NLPManager Throws an Application Error,” on page 4
- Section 2.7, “Launching NLPManager on Another Linux System,” on page 4
- Section 2.8, “Handling a Start TLS Extended Request,” on page 4
- Section 2.9, “Starting NLPManager on RHEL,” on page 4
- Section 2.10, “Disabled Policies Are Processed,” on page 5
- Section 2.11, “The Search Base Is Not Modified in the LDAPSearch Response,” on page 5
- Section 2.12, “The Schema Map Policy Does Not Map the Attribute Values,” on page 5
- Section 2.13, “The String Replacement Policy Does Not Replace the Object Identifiers by the Attribute Types,” on page 5
- Section 2.14, “Multiple Actions in a Policy,” on page 5
- Section 2.15, “Configuring a Search Policy for op="show-only" Containers,” on page 6
- Section 2.16, “Listener Issues,” on page 6

2.1 Installation Dependency

To successfully install the LDAP Proxy, you must install `libstdc++.so.5` and `libstdc++.so.6` libraries on your system before the installing proxy.

2.2 Unable to Block Search Selection Attribute

If the proxy is configured to allow a specific search selection attribute, and if this attribute is concatenated with restricted attributes, the search results will also contain the restricted attributes. For example, the following policy node is configured to allow only `cn` as a search selection attribute. In such a case, a search request with the selection attribute `sn` is rejected. However, a search request with the search selection attribute list as `cn  sn` returns the values with `sn`.

```
<policy-connection-route id-policy="multi-value RDNs">
  <rule>
  <conditions>
   <or>
     <if-bind-dn op="equal">cn=john+uid=3517,ou=eng_dept1,o=my_company</if-
bind-dn>
   <if-bind-dn op="equal">uid=3517+cn=john,ou=eng_dept1,o=my_company</if-bind-
dn>
   </or>
  </conditions>
  <actions>
   <do-deny/>
  </actions>
  <actions-default>
   <do-nothing/>
  </actions-default>
 </rule>
</policy-connection-route>
```

```
<policy-search-request id-policy="testing738911" disabled="false">
<description>search restriction operation to test if-srch-selection-attrcase-
ignore equals cn</description>

      <rule>

        <conditions>

          <if-srch-selection-attr op="not-equal"

match="case-ignore">cn</if-srch-selection-attr>

        </conditions>

        <actions>

          <do-deny /></actions>

        <actions-default>

          <do-allow /></actions-default>

      </rule>

    </policy-search-request>
```

2.3 Using SSL Clients

If the connection between the proxy and the back-end server is configured for SSL, the performance of the proxy server could potentially degrade if the number of incoming connections is high.

2.4 Using a Connection Pool

When a connection pool is enabled, the LDAP Proxy sends an anonymous bind request to the back-end server to nullify the connection identity. If the back-end server is not configured for anonymous bind, the connection pool feature does not work.

For the connection pool to work, anonymous bind must be enabled at the back-end server.

2.5 NLPManager Throws a NullPointerException Error

In certain cases, in NLPManager, when you try to close multiple instances of the *Listeners*, *Backend servers*, or *Backend Server Groups* tabs in the editor pane, the application throws the NullPointerException error. It is safe to ignore this exception because it does not cause any loss of functionality.

2.6 NLPManager Throws an Application Error

In certain cases, NLPManager throws an application error when you launch and close the application for the first time. This error is displayed in the *Error Log* tab when you launch the application again. The error does not occur subsequently and does not not affect the functionality of the application. You can either delete the error from the error log or ignore it.

2.7 Launching NLPManager on Another Linux System

NLPManager throws an application error message indicating `Error Line : org.eclipse.swt.SWTError: No more handles [gtk_init_check() failed]`when you try to log in to another Linux system and launch NLPManager without the -X option. This is an informational error that can be ignored.

However, you must always use the -X option while logging in to another Linux system where NLPManager is installed.

2.8 Handling a Start TLS Extended Request

When the LDAP Proxy receives a Start TLS extended request, it forwards the request to the back-end server. Any Start TLS error from the back-end server is ignored.

2.9 Starting NLPManager on RHEL

When you try to start NLPManager on RHEL, an error message indicating “`Cannot restore segment prot after reloc: Permission denied.` appears.

This is caused by the SeLinux security extension. SeLinux is active in the newer distributions of Linux with 2.6. kernels. It changes some default system behavior, including the shared library loading.

To temporarily disable enforcement on a running system, run the following command:

```
/usr/sbin/setenforce 0
```

To permanently disable enforcement during a system startup:

Set `SELINUX=disabled` at `/etc/selinux/config` and reboot.

2.10 Disabled Policies Are Processed

The LDAP Proxy processes disabled policies without checking their disabled status.

2.11 The Search Base Is Not Modified in the LDAPSearch Response

The Search Request policy does not change the requested search base in the LDAP search response.

To modify the search base, use the Replace String policy.

2.12 The Schema Map Policy Does Not Map the Attribute Values

The Schema Map policy maps only the DN and the attribute names of the attributes it is mapping.

2.13 The String Replacement Policy Does Not Replace the Object Identifiers by the Attribute Types

The String Replacement policy does not map the object identifiers with the corresponding attribute types.

To resolve this issue, configure a different replacement pattern in the String Replacement policy.

For example, to replace `o=organization` with `o=example`, you can add an extra pattern with object identifiers. For example, you can change `2.5.4.10=organization` to `2.5.4.10=example`.

```
<replace>
     <from>o=organization</from>
     <to>o=example</to>
</replace>
<replace>
     <from>2.5.4.10=organization</from>
     <to>2.5.4.10=example</to>
</replace>
```

2.14 Multiple Actions in a Policy

You should not configure a policy with more than one action at a time. For example, if you configure a Search Request policy with the do-modify-search and do-restrict-view actions and then restart the LDAP Proxy, the first action is overwritten by the second action.

2.15 Configuring a Search Policy for op="show-only" Containers

The filter is not replaced if a search policy is configured for op="show-only" containers. The Replace String policy does not use the filter that is internally created by the Restrict View to query the LDAP server. The attribute values in the filter created by the Restrict View policy are not replaced.

To work around this issue, configure the Restrict View policy to consume the actual DNs present in the LDAP server.

2.16 Listener Issues

- Section 2.16.1, “Using the Same Listener Name in the NLPManager,” on page 6
- Section 2.16.2, “Using an Empty Listener Name,” on page 6

2.16.1 Using the Same Listener Name in the NLPManager

In the NLPManager, the LDAP Proxy does not check for the existing listener names. It allows users to use the same name for more than one listener.

2.16.2 Using an Empty Listener Name

The LDAP Proxy allows empty listener names. If you specify a name for a listener that was saved earlier with an empty name, the new value is not accepted. The listener name field remains empty.

To work around this issue, manually add the listener name value in the configuration file.

3 Additional Documentation

- Section 3.1, “NLP Manager,” on page 6
- Section 3.2, “Certificate Server,” on page 6
- Section 3.3, “NICI 2.7.6,” on page 6

3.1 NLP Manager

For information on NLPManager, refer to the *Novell LDAP Proxy 1.0 Administration Guide* (http://www.novell.com/documentation/ldapproxy/admin/data/bookinfo.html).

3.2 Certificate Server

For Certificate Server information, refer to the Certificate Server online documentation (http://www.novell.com/documentation/crt33/index.html).

3.3 NICI 2.7.6

For NICI information, refer to the NICI online documentation (http://www.novell.com/documentation/nici27x/index.html).

4 Legal Notices

Novell, Inc. makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, Novell, Inc. makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. reserves the right to make changes to any and all parts of Novell software, at any time, without any obligation to notify any person or entity of such changes.

Any products or technical information provided under this Agreement may be subject to U.S. export controls and the trade laws of other countries. You agree to comply with all export control regulations and to obtain any required licenses or classification to export, re-export, or import deliverables. You agree not to export or re-export to entities on the current U.S. export exclusion lists or to any embargoed or terrorist countries as specified in the U.S. export laws. You agree to not use deliverables for prohibited nuclear, missile, or chemical biological weaponry end uses. Please refer to the Novell International Trade Services Web page (http://www.novell.com/info/exports/) for more information on exporting Novell software. Novell assumes no responsibility for your failure to obtain any necessary export approvals.

For Novell trademarks, see the Novell Trademark and Service Mark list (http://www.novell.com/company/legal/trademarks/tmlist.html).

All third-party trademarks are the property of their respective owners.