Defect ID: IV22044

Title: INCORRECT INFORMATION IN "SECURE COMMUNICATION WITH SUPPORTED MIDDLEWARE" SECTION OF TIM 5.1 DOCUMENTATION.

Version: ITIM 5.1

Severity: 4

Problem Description from CMVC:
Error Description :
In the Security book/section of the TIM 5.1 infocenter there is the "Secure communication with supported middleware" section and this contains a couple places of incorrect information shown for setup of SSL connection to TIM's LDAP.

1. In the "**Configuring the IBM Tivoli Identity Manager Server**" section shows following steps:

=======
a. In the /opt/IBM/itim/data directory, edit the enRoleLDAPConnection.properties file.

b. In the properties file, change the 'java.naming.provider.url' property to specify the computer and port on which the directory server is listening. In this example, type the host name and secure port of the machine which has the directory server. For example, type:

```
java.naming.provider.url=test1234:636
```

========

The example java.naming.provider.url value show above of just test1234:636 is not correct, the value needs to have ldaps:// infront of it, so like

```
java.naming.provider.url=ldaps://test1234:636
```

The same type of information is correctly documented in the Appendix B of the "Installation and Configuration Guide" book in the "Running ldapConfig and runConfig with SSL" section.

2. In the "**Testing SSL communication between servers**" section there is incorrect test ldapsearch command listed. Below is what the document shows now.

=========
1. Test that the directory server is listening. In the /opt/IBM/ldap/V6.1/bin directory on the computer that has the directory server, type this command on one line:

```
ldapsearch -p 636 -K /certs/LDAPSERVER_TEST1234.kdb -s base objectclass=* -b dc=com
```

=========

The problem is the "objectclass=*" part needs to be at the end, otherwise as listed now the "-b dc=com" part is not used for actual based, but as attributes to show on the search results. So the example ldapsearch command should be following:

```
ldapsearch -p 636 -K /certs/LDAPSERVER_TEST1234.kdb -s base -b dc=com "objectclass=*"
```

Desired Behavior: The correct information to be listed in the documentation for setup of SSL connection between TIM/WAS and LDAP.

Doc Changes:
Following DOC Changes to be incorporated to ITIM5.1 Infocenter under Identity Manager 5.1 > Security > Secure communication with supported middleware section.

LOCATION_URL:
http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.itim.doc/cpt/cpt_ic_security_ssl_midware.html

In the "**Configuring the IBM Tivoli Identity Manager Server**" section, 1b and 1c.
<Infocenter_Update>

1. On the computer that has the Tivoli Identity Manager Server, edit the property that specifies the LDAP connection. Complete these steps:

   a. In the /opt/IBM/itim/data directory, edit the enRoleLDAPConnection.properties file.

   b. In the properties file, change the *java.naming.provider.url* property to specify the computer and port on which the directory server is listening. In this example, type the host name and secure port of the machine which has the directory server. For example, type:

   ```
   java.naming.provider.url=ldap://test1234:636
   ```

   c. Additionally, Tivoli Identity Manager Server should be indicated to use SSL to communicate to LDAP. This can be done by changing the *java.naming.security.protocol* property to specify SSL communication:

   ```
   java.naming.security.protocol=ssl
   ```

   The other way is to specify the protocol as ldaps instead of ldap in the *java.naming.provider.url* property. For example:

   ```
   java.naming.provider.url=ldaps://test1234:636
   ```

2. Save and close the enRoleLDAPConnection.properties file.

3. Restart the WebSphere® Application Server.

</Infocenter_Update>

In the "**Testing SSL communication between servers"** section, step 1.
<Infocenter_Update>
Test that the directory server is listening. In the /opt/IBM/ldap/V6.1/bin directory on the computer that has the directory server, type this command on one line:

```
      ldapsearch -b dc=com -K /certs/LDAPSERVER_TEST1234.kdb -p 636 -s base
"objectclass=*"
```

The result has entries for the top level schema similar to these:

```
dc=com
objectclass=top
objectclass=domain
dc=com
```

</Infocenter_Update>