Lab E - Exercise 1: Communicate using SSL

Overview

In this exercise you will configure your TIBCO EMS server to listen for SSL connections. For this initial exercise, you will set the server identity using the following digital certificates:

- server identity file = /opt/tibco/soa/ems/8.2/samples/certs/server.cert.pem
- server certificate key file = /opt/tibco/soa/ems/8.2/samples/certs/server.key.pem
- server certificate key password = password

You will then develop and test two processes to publish and subscribe in SSL mode.

Steps

1. Configure EMS to accept SSL connections.

- Shutdown the EMS Server (*Applications* > *TIBCO* > *EMS* > ***TIBCO EMS Server - Stop***)
- Make a copy **tibemsd.conf**
    - In File Browser, navigate to `/opt/tibco/soa/config/tibco/cfgmgmt/ems/`**`data`**
    - Right-click on **tibemsd.conf** file and select **Copy**
    - Use *Edit* > ***Paste*** to copy the file in the same folder
    - Rename the copy to **`tibemsdSSL.conf`**
- Open **tibemsdSSL.conf** in gedit
- Locate the **Listen Ports** section (approx line 81) and add the following second entry: **`listen = ssl://7333`**
- Locate the **SSL Server Setup** section (approx line 242) and specify the server certificate (as a slingle line)

  ```
  ssl_server_identity =
  /opt/tibco/soa/ems/8.2/samples/certs/server.cert.pem
  ```
- Specify the server private key (as a single line):

  ```
  ssl_server_key =
  /opt/tibco/soa/ems/8.2/samples/certs/server.key.pem
  ```
- Comment the ssl_password line: **`#ssl_password =`**
- **Save** and Close the **tibemsdSSL.conf** file

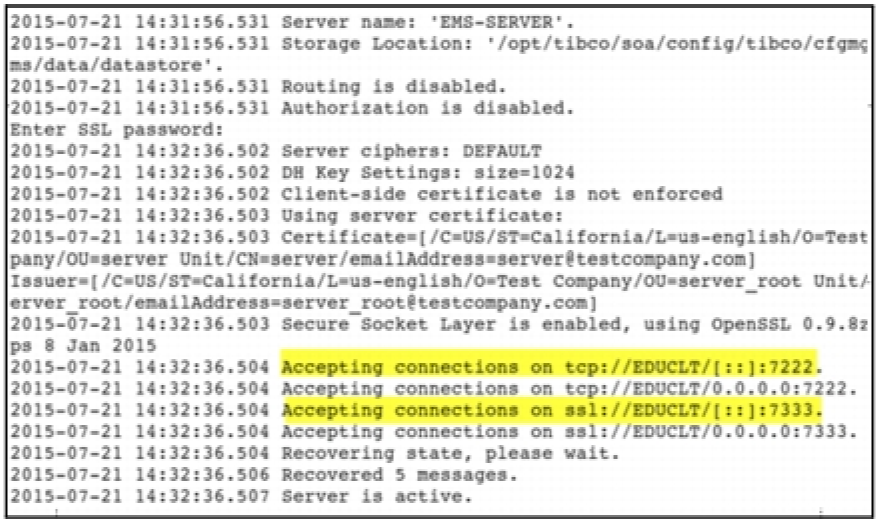
2. Start EMS Server in SSL mode.

- Open a Terminal and issue the following command (in a single line)

  ```
  tibemsd64 -config
  /opt/tibco/soa/config/tibco/cfgmgmt/ems/data/tibemsdSSL.conf -
  ssl_trace -ssl_debug_trace -trace CONNECT
  ```
    - When prompted for password, type: **`password`**

Note: You are prompted to provide a password, even though you did not specify one in the configuration file, as required by the certificate you are using.

- Verify that the server is "accepting connections" on tcp://7222 and ssl://7333



```
2015-07-21 14:31:56.531 Server name: 'EMS-SERVER'.
2015-07-21 14:31:56.531 Storage Location: '/opt/tibco/soa/config/tibco/cfgmg
ms/data/datastore'.
2015-07-21 14:31:56.531 Routing is disabled.
2015-07-21 14:31:56.531 Authorization is disabled.
Enter SSL password:
2015-07-21 14:32:36.502 Server ciphers: DEFAULT
2015-07-21 14:32:36.502 DH Key Settings: size=1024
2015-07-21 14:32:36.502 Client-side certificate is not enforced
2015-07-21 14:32:36.503 Using server certificate:
2015-07-21 14:32:36.503 Certificate=[/C=US/ST=California/L=us-english/O=Test
pany/OU=server Unit/CN=server/emailAddress=server@testcompany.com]
Issuer=[/C=US/ST=California/L=us-english/O=Test Company/OU=server_root Unit/
erver_root/emailAddress=server_root@testcompany.com]
2015-07-21 14:32:36.503 Secure Socket Layer is enabled, using OpenSSL 0.9.8z
ps 8 Jan 2015
2015-07-21 14:32:36.504 Accepting connections on tcp://EDUCLT/[::]:7222.
2015-07-21 14:32:36.504 Accepting connections on tcp://EDUCLT/0.0.0.0:7222.
2015-07-21 14:32:36.504 Accepting connections on ssl://EDUCLT/[::]:7333.
2015-07-21 14:32:36.504 Accepting connections on ssl://EDUCLT/0.0.0.0:7333.
2015-07-21 14:32:36.504 Recovering state, please wait.
2015-07-21 14:32:36.506 Recovered 5 messages.
2015-07-21 14:32:36.507 Server is active.
```

Tip: If the SSL port is being "ignored", verify that you entered password correctly.

- Connect to the EMS Server as the admin user using the SSL connection port:
  - Start the EMS Administration Tool and connect as admin
  - Type: **`connect ssl://7333`**
  - Type **`yes`** to confirm that you want to disconnect
    - Press <**Enter**> twice to log in as the default admin user

3. Create a digital certificate in JKS format.

- In a Terminal, navigate to the directory `/home/tibco/EMS206Files/scripts`
  - Execute the script **`CreateKeyStore.sh`**
    - Type **`yes`** when prompted to confirm to trust the certificate
    - Observe messages confirming successful imports of certificates
  - Verify that the script created a JKS keystore in the folder `/home/tibco/EMS206Files/keystore`
    - Execute the command

      `ls /home/tibco/EMS206Files/keystore`

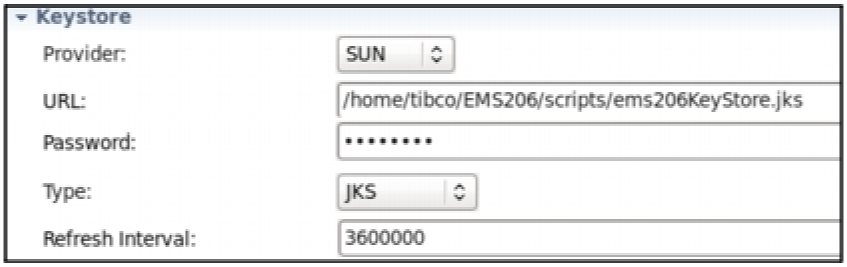
      - Verify that the file `ems206KeyStore.jks` is listed
- Verify that the keystore contains both required certificates
  - Issue the following command:

    `keytool -list -v -keystore ems206KeyStore.jks`

    - When prompted to enter keystore password, type **`password`**
  - Observe the information about two keys contained in the keystore

4. Configure Keystore Resource for the digital certificate.

- Return to TIBCO Business Studio
- Create and configure a new Keystore Resource
  - In Project Explorer, right-click *EMS206project* > ***Resources***
    - Select *New* > ***Keystore Provider***
      - Resource Name: **`EMS206KeystoreProvider`**
    - Click **Finish**
  - Notice that the new resource Editor view is opened
- Configure the **EMS206KeystoreProvider** resource
  - Provider: **SUN** (select from dropbox)
  - URL: **`/home/tibco/EMS206Files/keystore/ems206KeyStore.jks`**
  - Password: **`password`**
  - Type: **JKS** (select from dropdown)
- **Save**



Keystore

Provider: SUN

URL: /home/tibco/EMS206/scripts/ems206KeyStore.jks

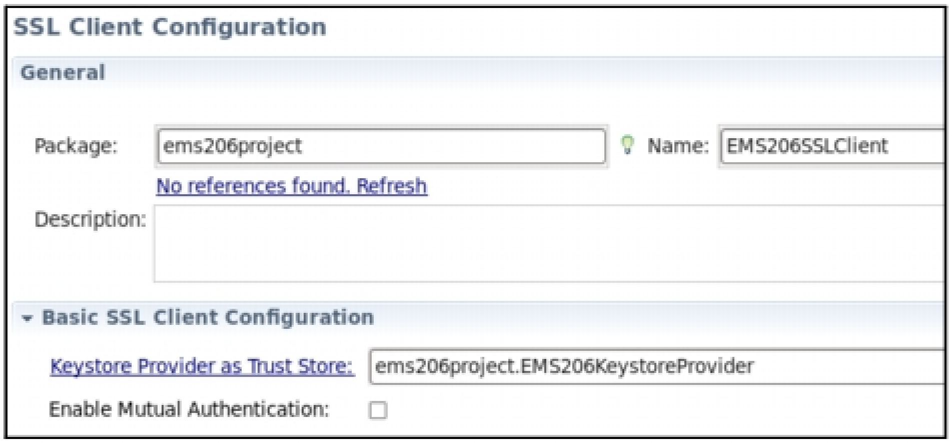
Password: •••••••••

Type: JKS

Refresh Interval: 3600000

5. Configure SSL Client resource for the digital certificate.

- Create and configure a new SSLClient Resource
  - Right-click *EMS206project* > ***Resources***
    - Select *New* > ***SSL Client Configuration***
      - Resource Name: **`EMS206SSLClient`**
    - Click **Finish**
  - **Basic SSL Client Configuration**
    - Keystore Provider as Trust Store: Browse for **EMS206project.EMS206KeystoreProvider**
  - **Save**



SSL Client Configuration

General

Package: ems206project

Name: EMS206SSLClient

No references found. Refresh

Description:

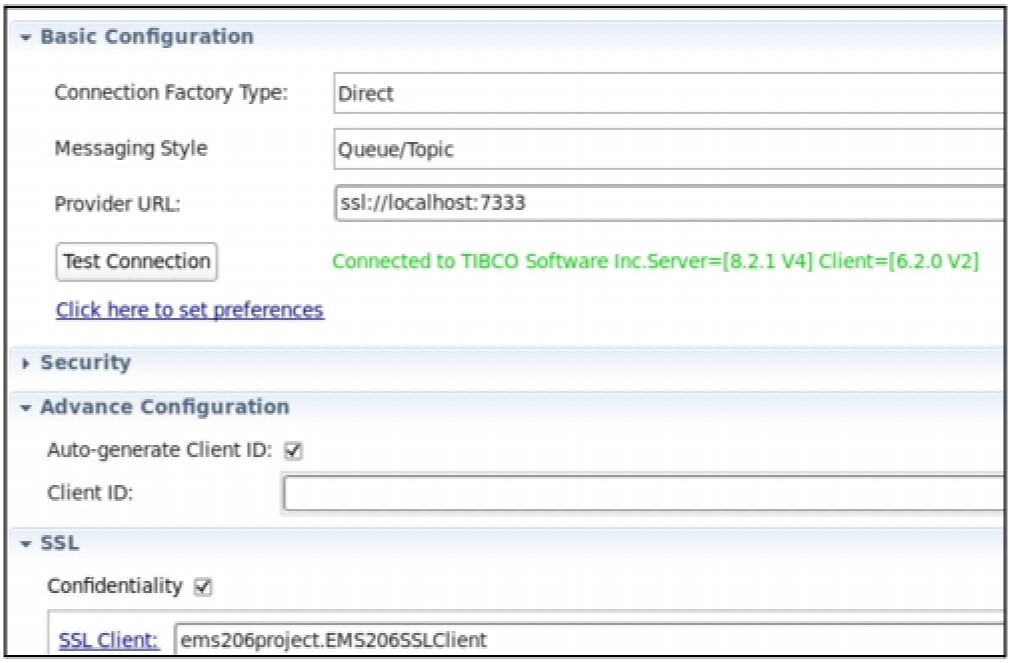
Basic SSL Client Configuration

Keystore Provider as Trust Store: ems206project.EMS206KeystoreProvider

Enable Mutual Authentication: □

6. Create and configure SSL JMS Connection Resource.

- Right-click *EMS206project* > ***Resources***
  - Select *New* > ***JMS Connection***
    - Resource Name: **`JMS_SSL_Connection`**
    - Click **Finish**
- Configure the JMS Connection resource as follows:
  - **Basic Configuration**
    - Connection Factory Type: **Direct** (select from dropdown)
    - Messaging Style: **Queue/Topic** (from dropdown)
    - Provider URL: **`ssl://localhost:7333`**
  - **SSL** (scroll down to reveal if necessary)
    - Confidentiality: checked
    - SSL Client: Browse for **EMS206project.EMS206SSLClient**
  - **Save**
- Click **Test Connection** - you should see successful message



Connection Factory Type: Direct

Messaging Style: Queue/Topic

Provider URL: ssl://localhost:7333

Connected to TIBCO Software Inc.Server=[8.2.1 V4] Client=[6.2.0 V2]

Auto-generate Client ID: ☑

Client ID:

Confidentiality ☑

SSL Client: ems206project.EMS206SSLClient

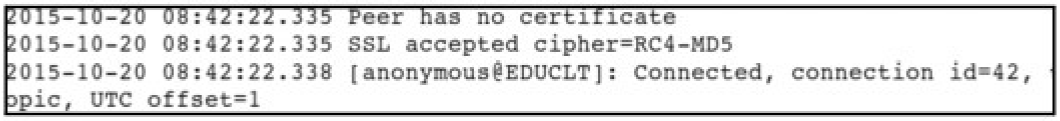
7. Modify existing processes to use SSL encrypted connection to the server.

- In the EMS206project/Processes create folder **`LabE`**
  - Copy the following processes from *EMS206project/Processes/**LabA*** to the *EMS206project/Processes/**LabE***
    - *SendShipmentNotification*
    - *ReceiveShipmentNotification-Customer*
- Rename the process *SendShipmentNotification*
  - Right-click *SendShipmentNotification* in *EMS206project/Processes/**LabE***
  - Select *Rename*
    - New Name: **`SSL_Send`**
    - Click **OK**
- Similarly, rename *ReceiveShipmentNotification-Customer* to **`SSL_Receive`**

- Modify the *SSL_Send* process
  - Double-click *SSL_Send* in *EMS206project/Processes/**LabE***
  - Select the **JMS Topic Publisher** activity
    - JMS Connection: Browse for **EMS206project.JMS_SSL_Connection**
  - **Save**
- Modify *SSL_Receive*
  - Double-click *SSL_Receive* in *EMS206project/Processes/**LabE***
  - Select the **JMS Topic Subscriber - Customer** activity
    - JMS Connection: Browse for **EMS206project.JMS_SSL_Connection**
- **Save**

8. Test your SSL-enabled processes.

- Configure the Components list
  - *SSL_Send*
  - *SSL_Receive*
- Launch the debugger
  - In the *BusinessWorks Jobs* view, observe that a single job is executed for both processes
  - Verify that *Console view* shows that the message is published and received
- Observe that the communication was using SSL protocol
  - View the Terminal where the EMS was started
  - Observe the EMS Console Log and verify that clients connected using SSL



```
2015-10-20 08:42:22.335 Peer has no certificate
2015-10-20 08:42:22.335 SSL accepted cipher=RC4-MD5
2015-10-20 08:42:22.338 [anonymous@EDUCLT]: Connected, connection id=42,
opic, UTC offset=1
```

- Terminate the debugger
- Shutdown the EMS Server (*Applications* > *TIBCO* > *EMS* > ***TIBCO EMS Server - Stop***)