OpenAttestation Installation Guide

March 2012

Contents

1 Supported systems

Following environments have been verified to run OpenAttestation project

Servers:

Fedora14

Hosts/Clients:

Ubuntu11.10

OpenSuse11.4, OpenSuse12.1

OpenSuse12.1 + tboot + Xen

SLES11 SP1

RHEL6.1

Fedora14

2 *Background*

2.1 Setup environments

To setup the Attestation environment, 2 systems are required

- Fedora14 or RHEL6.x Linux system severed as Attestation Server. We use Fedora 14 as example in the document
- Fedora, RHEL, Ubuntu, OpenSuse, SLES Linux system with TPM and TXT enabled as Client/Host system to be verified. We use Fedora 14 as example in the document

2.2 Note

- <server.domain> in this guide means the host name of Attestation Server
- Setup systems with full domain names, for example, OpenAttestation.TrustedPool.com

3 Attestation Server Installation

Attestation Server Installation is verified on Fedora 14 and RHEL 6.1

3.1 Install Fedora

3.2 Download Installation Package AttestationSDK.tgz

3.3 Disable server Firewall and SELINUX

- System->Administration->Firewall click on "Disable" in GUI
- System->Administration->SELinux Administration to "Disable" SELINUX in GUI

3.4 Install required modules

```
yum -y install httpd

yum -y install mysql mysql-server

yum -y install php php-mysql

yum -y install openssl

yum -y install java-1.6.0-openjdk.x86_64
```

3.5 Install Attestation Server Package

- Find previous installed Attestation Server package
  - rpm -q OAT-Appraiser-Base-OATapp
- Remove previous installed Attestation Server package
  - rpm -e "Result from above operation"
- Install new Attestation Server package
  - rpm -hiv OAT-Appraiser-Base-OATapp-1.0.0-2.fc14.x86_64.rpm

3.6 Verify the installation

- Access http://<server.domain>/OAT/ in Browser

4 Attestation Client Installation

4.1 Prerequisite

Client system must have TPM 1.2 compliant device with driver installed, and TPM/TXT enabled in BIOS to perform the operation

Perform OpenAttestation package installation with ROOT super user mode

4.2 Enable TPM in BIOS and Install OS

4.3 Install modules according to your OS

4.3.1 For Fedora 14, install modules

- trousers-devel
- java-1.6.0-openjdk
- and make sure the TrouSers service is started:

  service tcsd restart

4.3.2 For RHEL 6.1, install modules

We recommend to install these package from RHEL 6.1 CD for your convenience

- trousers
- java-1.6.0-openjdk
- and make sure the TrouSers service is started:

  service tcsd restart

4.3.3 For Ubuntu 11.10, install modules

- trousers
- libtspi1
- openjdk-6-jre

- and edit trousers daemon scripts by:

```
sed -i 's/--chuid \${USER}//g' /etc/init.d/trousers
```

- then restart trousers daemon:

```
service trousers restart
```

4.3.4 For OpenSuse 12.1 and SLES 11, install modules

- trousers
- libtspi1
- java-1.6.0-openjdk or java-1.6.0-ibm
- and make sure the TrouSers service is started:

```
service tcsd restart
```

4.3.5 Download Open Attestation Client Installation Package

- via http://<server.domain>/ClientInstaller.html in browser
- Download the client package by clicking 'Client Installation Files For Linux'

4.3.6 Unzip Open Attestation Client Installation package to your local disk

4.3.7 Run general-install.sh to install the package

4.3.8 Restart OS or start client program manually

via "/etc/init.d/OAT.sh start"

4.3.9 Verify the report

via http://<server.domain>/OAT/reports.php

5 Setup Two Way SSL/TLS Authentication for Admin Console and Attestation API

5.1 Edit tomcat server configuration file to include a new Service

- In /usr/lib/apache-tomcat-6.0.29/conf/server.xml
- The key properties are
  - **appBase="webappsAPI"** - Set service application base folder to webappsAPI
  - **port="8444" -** Set the service listening at port 8444
  - **clientAuth="true" –** Enable Two-Way SSL authentication for the service
- Add below snippet in <Server> part of server.xml
  - Change keystorePass to the keystorePass value which already exists in <Connector /> of server.xml
  - Change truststorePass to the truststorePass value which already exists in <Connector /> of server.xml

```
<Service>
<Engine name="Catalina2" defaultHost="localhost">
<Realm className="org.apache.catalina.realm.UserDatabaseRealm"
resourceName="UserDatabase"/>
<Host name="localhost"  appBase="webappsAPI" unpackWARs="true"
autoDeploy="true" xmlValidation="false" xmlNamespaceAware="false"></Host>
</Engine>
<Connector port="8444" minSpareThreads="5" maxSpareThreads="75"
enableLookups="false" disableUploadTimeout="true" acceptCount="100"
maxThreads="200" scheme="https" secure="true" SSLEnabled="true"
clientAuth="true" sslProtocol="TLS"
ciphers="TLS_ECDH_anon_WITH_AES_256_CBC_SHA,
TLS_ECDH_anon_WITH_AES_128_CBC_SHA,
TLS_ECDH_anon_WITH_3DES_EDE_CBC_SHA,
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA,
TLS_ECDH_RSA_WITH_AES_256_CBC_SHA,
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA,
TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA,
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA,
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA,
TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA,
TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA,
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA,
TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA,
TLS_DHE_RSA_WITH_AES_256_CBC_SHA,
TLS_DHE_DSS_WITH_AES_256_CBC_SHA, TLS_RSA_WITH_AES_256_CBC_SHA,
TLS_DHE_RSA_WITH_AES_128_CBC_SHA,
TLS_DHE_DSS_WITH_AES_128_CBC_SHA, TLS_RSA_WITH_AES_128_CBC_SHA"
keystoreFile="/usr/lib/apache-tomcat-6.0.29/Certificate/keystore.jks"
keystorePass="4cea3ba9308495790c1078140824d9" truststoreFile="/usr/lib/apache-tomcat-6.0.29/Certificate/TrustStore.jks" truststorePass="password" />
 </Service>
```

5.2 Create webappsAPI folder

- in /usr/lib/apache-tomcat-6.0.29/
  mkdir webappsAPI

5.3 Move QueryAPI, ManifestAPI and AdminConsole war package to webappsAPI folder

- in /usr/lib/apache-tomcat-6.0.29/
- cp webapps/OpenAttestationAdminConsole.war webappsAPI/
- cp webapps/OpenAttestationManifestWebServices.war webappsAPI/

- cp webapps/OpenAttestationWebServices.war webappsAPI/

5.4 Unpack packages via re-start Tomcat Server

- /usr/lib/apache-tomcat-6.0.29/bin/shutdown.sh
- /usr/lib/apache-tomcat-6.0.29/bin/startup.sh

5.5 Create properties for Two-Way SSL in Admin Console configuration files

- Add new properties In /usr/lib/apache-tomcat-6.0.29/webappsAPI/OpenAttestationAdminConsole/WEB-INF/classes/manifest.properties
  - keystore_path=/usr/lib/apache-tomcat-6.0.29/Certificate/APIclient.p12
  - trust_store_password=password
  - key_store_password=password
- Add new properties In /usr/lib/apache-tomcat-6.0.29/webappsAPI/OpenAttestationAdminConsole/WEB-INF/classes/OpenAttestation.properties
  - keystore_path=/usr/lib/apache-tomcat-6.0.29/Certificate/APIclient.p12
  - trust_store_password=password
  - key_store_password=password

5.6 Change Query/Manifest API port from 8443 to 8444

- Replace 8443 with 8444 in /usr/lib/apache-tomcat-6.0.29/webappsAPI/OpenAttestationAdminConsole/WEB-INF/classes/ manifest.properties and OpenAttestation.properties

5.7 Create ISV API certificate APIclient.cer and APIclient.p12

- in /usr/lib/apache-tomcat-6.0.29/Certificate/

- openssl req -x509 -nodes -days 730 -newkey rsa:2048 -keyout APIclient.pem -out APIclient.cer -subj "/C=US/O=U.S.Government/OU=DoD/CN=`hostname`API"
- openssl pkcs12 -export -in APIclient.cer -inkey APIclient.pem -out APIclient.p12 -passout pass:password

5.8 Import ISV API certificate APIclient.cer into Tomcat truststore

- in /usr/lib/apache-tomcat-6.0.29/Certificate/
- keytool -import -keystore TrustStore.jks -alias OATAPI -storepass password -file APIclient.cer –noprompt

5.9 Restart Tomcat Server

service tomcat6 restart

5.10 Import ISV P12 certificate APIclient.p12 in Browser to enable Two-Way SSL authentication for Admin Console access

- In Firefox Menu, Edit/Advanced/Encryption/View Certificates/Your Certificates /Import/ to select APIclient.p12
- Access Admin Console throught url https://xxx:8444/OpenAttestationAdminConsole/AdminConsole.jsp

6 Database Tuning

6.1 Appraiser Web Service next action checking interval configuration

- Get database connection username via connection.username in /usr/lib/apache-tomcat-6.0.29/webapps/HisWebServices/WEB-INF/classes/hibernateOat.cfg.xml
- Get database connection password via connection.password in /usr/lib/apache-tomcat-6.0.29/webapps/HisWebServices/WEB-INF/classes/hibernateOat.cfg.xml
- Enter mysql command management via command

  mysql –u<database username in step 1>
- Enter password <database password in step 2>
- Use Attestation dababase

  mysql> use oat_db;
- Show current next action checking interval

  mysql> select * from system_constants;
- Modify next action checking interval to 20 seconds

  mysql> update system_constants set value='20000';

7 Attestation Property files explanation

7.1 Appraiser Web Service Configuration

- OAT.properties in /usr/lib/apache-tomcat-6.0.29/webapps/HisWebServices/WEB-INF/classes
  - Set PCR_SELECT to FFFFFF like:

    ```
    #PCR 0~23 selected for integrity reports attestation
     PCR_SELECT=FFFFFF
    ```

  - Set ALERT_MASK_CSV to whatever PCR numbers (0~23) you want to validate and keep 'signature' in the end, for example:

    ```
    #Attestation to verify PCR0, 4, 5 and signature
    ALERT_MASK_CSV=0,4,5,signature
    ```

7.2 Appraiser Admin Console Configuration

- WhiteList API configurations in /usr/lib/apache-tomcat-6.0.29/webapps/OpenAttestationAdminConsole/WEB-INF/classes/ manifest.properties
  - Set manifest web service url

    ```
    manifest_webservice_url=https://<server.domain>:8443/OpenAttestationManifestWebServices/V1.0/PCR
    ```

  - Set truststore path

    ```
    truststore_path=/usr/lib/apache-tomcat-6.0.29/Certificate/TrustStore.jks
    ```

- Query API configurations in /usr/lib/apache-tomcat-6.0.29/webapps/OpenAttestationAdminConsole/WEB-INF/classes/ OpenAttestation.properties
  - Set Query API web service url AttestationWebServicesUrl=https:// <server.domain>:8443/OpenAttestationWebServices/V1.0

- Set default attest interval

  default_attest_interval=60000

- Set default attest timeout

  default_attest_timeout=60000

- Set truststore path

  TrustStore=/usr/lib/apache-tomcat-6.0.29/Certificate/TrustStore.jks

7.3 Client Provisioning Configuration

- Client provisioning in ~/Downloads/ClientInstallForLinux/OATprovisioner.properties
  - Tpm Owner Auth password

    TpmOwnerAuth = 1111111111111111111111111111111111111111
  - Privacy CA certificate file

    PrivacyCaCertFile = PrivacyCA.cer
  - Privacy CA web service URL

    PrivacyCaUrl = https://<server.domain>:8443/HisPrivacyCAWebServices2
  - Appraiser web service URL

    HisRegistrationUrl = https://<server.domain>:8443/HisWebServices
  - Client Trust Store file

    TrustStore = TrustStore.jks
  - Client installation path

    ClientPath = /OAT
- Client provisioning in ~/Downloads/ClientInstallForLinux/TPMModule.properties
  - TPM tool executable file name

    ExeName = NIARL_TPM_Module
  - Trousers Mode

    TrousersMode = True
  - Debug Mode

    DebugMode = False

7.4 Client application configuration

- /OAT/OAT.properties

- Appraiser Web Service URL

  WebServiceUrl=https://<server.domain>:8443/HisWebServices
- TPM tool executable file name

  TpmQuoteExecutableName=NIARL_TPM_Module
- TrustStore file

  TrustStore=TrustStore.jks

8 Example of creating White List

8.1 Retrieve specific PCR values from portal

- Open portal at http://<server.domain>/OAT/pcrs.php
- Copy specific PCR value, for example, PRC 5 value "B45D33B7312EFA9A1D8E223640B5F37215CC801E"

8.2 Create White List entry in Admin Console

- Open Admin Console While List page at https://<server.domain>:8443/OpenAttestationAdminConsole/PCRManifest.jsp
- Click "Add PCR" link at left menu bar to add a new PCR value in White List
  - Enter PCR number "5" to PCR Number text box
  - Paste PCR 5 value from Step 7.1 to PCR Value text box
  - Enter any description in PCR Description
  - Then Click "Add" button

8.3 Check White List in Admin Console

- Check all the PCRs value in While List at https://<server.domain>:8443/OpenAttestationAdminConsole/GetAllPCRServlet