OpenAttestation Installation Guide

Version: 1.7

March 2014

Contents

1 Supported systems

Following environments have been verified to run OpenAttestation project

Servers:

Fedora 19

Ubuntu 13.04

OpenSUSE 12.3

RHEL 6.4

Hosts/Clients:

Fedora 19

Ubuntu 13.04

OpenSUSE 12.3

RHEL 6.4

2 *Background*

2.1 Setup environments

To setup the Attestation environment, 2 systems are required:

- One Fedora, RHEL, Ubuntu or OpenSUSE Linux system severed as Attestation Server.
- One Fedora, RHEL, Ubuntu or OpenSUSE Linux system with TPM enabled as Client/Host system to be verified.

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
- If iptables and selinux must be enabled, make sure port 80, 8080, 8443, 8444 are open.

3 Attestation Server Installation

3.1 Install Fedora or Ubuntu

3.2 Disable server Firewall and SELINUX

3.2.1 For Fedora

- System->Administration->Firewall click on "Disable" in GUI
- System->Administration->SELinux Administration to "Disable" SELINUX in GUI
  Or disable SELINUX in "/etc/sysconfig/selinux" by setting SELINUX=disable

3.2.2 For RHEL

- Edit /etc/selinux/config "SELINUX=disabled"
- service iptables stop

3.2.3 For Ubuntu

- Typing "ufw disable" in command

3.2.4 For OpenSUSE

- Typing "SuSEfirewall off" or "SuSEfirewall2 off" (depends on the specific distribution) in command

3.3 Install required modules

3.3.1 For Fedora and RHEL

```
yum -y install httpd

yum -y install mysql mysql-server
```

* Notes: Just press ENTER button when you are asked to enter password.

```
* Note 2: if you have installed mysql server with password, you should

* remove password firstly.

yum -y install php php-mysql

yum -y install openssl

yum -y install java-1.7.0-openjdk.x86_64
```

3.3.2 For Ubuntu

```
apt-get install apache2

apt-get install mysql-client mysql-server mysql-common

* Notes: Just press ENTER button when you are asked to enter password

* Note 2: if you have installed mysql server with password, you should

* remove password firstly.

apt-get install php5 php5-mysql

apt-get install openssl

apt-get install openjdk-6-jdk
```

3.3.3 For OpenSUSE

```
zypper install apache2 apache2-mod_php5

zypper install mysql

* Notes: Just press ENTER button when you are asked to enter password

* Note 2: if you have installed mysql server with password, you should

* remove password firstly.

zypper install java-1_7_0-openjdk
```

* Note: In recent distribution, if java-1_7_0-openjdk is not available, please install java-1_6_0-openjdk instead

zypper install openssl

zypper install php5 php5-mysql

3.4 Install Attestation Server Package

3.4.1 For Fedora

- Find previous installed Attestation Server package
  - rpm -q OAT-Appraiser-Base-OATapp
- Remove previous installed Attestation Server package
  - rpm -e OAT-Appraiser-Base-OATapp
- Install new Attestation Server package
  - rpm -hiv OAT-Appraiser-Base-OATapp-1.0.0-2.fcxx.x86_64.rpm

3.4.2 For RHEL

- Find previous installed Attestation Server package
  - rpm -q OAT-Appraiser-Base-OATapp
- Remove previous installed Attestation Server package
  - rpm -e OAT-Appraiser-Base-OATapp
- Install new Attestation Server package
  - rpm -hiv OAT-Appraiser-Base-OATapp-1.0.0-2.el6.x86_64.rpm

3.4.3 For Ubuntu

- Find previous installed Attestation Server package
  - dpkg –L oat-appraiser-base-oatapp
- Remove previous installed Attestation Server package
  - dpkg –P oat-appraiser-base-oatapp
- Install new Attestation Server package

- dpkg -i OAT-Appraiser-Base-OATapp-1.0.0-2.ubuntu.x86_64.deb

3.4.4 For OpenSUSE

- Find previous installed Attestation Server package
  - rpm –qa OAT-Appraiser-Base-OATapp
- Remove previous installed Attestation Server package
  - rpm -e OAT-Appraiser-Base-OATapp
- Install new Attestation Server package
  - rpm –ivh OAT-Appraiser-Base-OATapp-1.0.1-2.x86_64.rpm

3.5 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 19 and RHEL 6.4, install modules

- trousers-devel
- java-1.7.0-openjdk
- and make sure the TrouSers service is started:

```
service tcsd restart
```

Note: In some RHEL versions, securityfs module hasn’t been mounted by default, you need run following command to mount it and get event log in /sys/kernel/security/tpm0/ascii_bios_measurements

```
mount -t securityfs security /sys/kernel/security
```

4.3.2 For Ubuntu 13.04, install modules

- trousers
- libtspi1
- openjdk-7-jdk
- openjdk-7-jre
- and edit trousers daemon scripts by:

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

- then restart trousers daemon:

```
service trousers restart
```

4.3.3 For OpenSuse 12.3, install modules

- trousers
- libtspi1
- xerces-j2
- java-1.7.0-openjdk or java-1.7.0-ibm
- and make sure the TrouSers service is started:

```
service tcsd restart
```

4.3.4 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'

4.3.5 Unzip Open Attestation Client Installation package to your local disk

4.3.6 Change TPM Owner Auth in Configure Files

- Prepare 20-char clear text TPM owner passphrase

  If the TPM ownership must be taken with a previous call to tpm_takeownership, make sure using "tpm_takeownership -z" command with a 20-char clear text TPM owner passphrase.

  If the TPM ownership can be left to the oat client installation process to take, then prepare a 20-char owner passphrase for use.

  For example, we can use passphrase like "01234567890123456789".
- Create 40 character hex passphrase

  Translate the 20-char passphrase into 40-digit hex string like below:

  ```
  # echo -n <20-char clear text tpm owner passphrase> | xxd –p
  ```

  The -n is important, it prevents the '\n' at the end of the string from being converted into the hex string. Verify the hex string is exactly 40 characters long, like "3031323334353537383930313233343535373839".

- Replace passphrase in configuration files

  The placeholders in the provisioner.sh and OATprovisioner.properties must be replaced with the actual passphrase (the 40-digit hex passphrase generated in the previous step).

  ```
  # cd <ClientInstaller_DIR>
  # sed -i "s/1111111111111111111111111111111111111111/<40-digit passphrase>/" provisioner.sh
  # sed -i "s/TpmOwnerAuth = 1111111111111111111111111111111111111111/TpmOwnerAuth = <40-digit passphrase>/g" OATprovisioner.properties
  ```

  Note: <ClientInstaller_DIR> is the directory of extracted ClientInstallForLinux package in section 4.3.5.

4.3.7 Run general-install.sh to install the package

```
sh general-install.sh –ecs FILE
```

-ecs with FILE/NVRAM is the EC storage option and is optional. If the option is FILE, the client will store EC in file system. If the option is NVRAM, the client will store EC in NVRAM.

4.3.8 Restart OS or start client program manually

via "/etc/init.d/OATClient start"

4.3.9 Verify the report

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

5 Database Tuning

5.1 Appraiser Web Service next action checking interval configuration

- Get database connection username via connection.username in /usr/lib/apache-tomcat-6.0.29/conf/context.xml
- Get database connection password via connection.password in /usr/lib/apache-tomcat-6.0.29/conf/context.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';

6 Attestation Property files explanation

6.1 Appraiser Configuration

- Query API configurations in /etc/oat-appraiser/OpenAttestation.properties
  - 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
- Query API configurations in /etc/oat-appraiser/OpenAttestationWebServices.properties
  - Tunable value in appraiser. Decrease the value may reduce attest response time. Increase the value may reduce the loop overhead.

    check_attest_interval=2000
- Report configurations in /etc/oat-appraiser/OAT.properties
  - Set IR_DIR in this configuration file, the integrity report will be written into the given directory or else it will be saved in DB. If the property is set, OAT expects the given directory exists and is accessible; on Fedora it means that the user 'tomcat' should be the owner of directory.

    IR_DIR=/var/log/oat_ir
  - Set digest method is used to check the integrity of reports in case they are stored on file.

    IR_DIGEST_METHOD=SHA-256
  - Activates/Deactivates the scalability mechanism. If it is set to "on" the client will receive a report type defining whether the entire list of measurements will be sent or just the measurements have not sent. If the property is set to "off" (or not set), OAT behavior will be unchanged.

    SCALABILITY=on

- Activates/Deactivates a space-saving feature that discards an integrity report if it is identical to the last one received. If the property is set to "off" (or not set), OAT behavior will be unchanged.

  DISCARD_IDENTICAL_IR=on

6.2 Client Provisioning Configuration

- Client provisioning in ~/Downloads/ClientInstallForLinux/OATprovisioner.properties
  - 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

6.3 Client application configuration

- /OAT/OAT.properties
  - Appraiser Web Service URL

    WebServiceUrl=https://<server.domain>:8443/HisWebServices
  - TrustStore file

    TrustStore=TrustStore.jks

7 Example of creating White List

7.1 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"

7.2 Create White List entry via OpenAttestation API or Command Tool

- Refer to API document Overview.pdf and the command tools README in CommandTool/ folder on Github source tree.