OpenAttestation Installation Guide

Version: 1.7

March 2014

Contents

1 *Supported systems*

Following environments have been verified to run OpenAttestation project

Servers:

Fedora16/17/18/19

Ubuntu12.10/12.04/13.04

Suse Enterprise Linux Server 11 SP2

Hosts/Clients:

Ubuntu12.10/12.04/13.04

OpenSuse11.4, OpenSuse12.3

OpenSuse12.3 + tboot + Xen

SLES11 SP2

RHEL6.1/6.3/6.4

Fedora/16/17/18/19

2　*Background*

2.1　Setup environments

To setup the Attestation environment, 2 systems are required:

➢　Fedora, RHEL6.x, SLES or Ubuntu12.10 Linux system severed as Attestation Server. We use Fedora, Ubuntu 12.10 and SLES 11 as example in the document

➢　Fedora, RHEL, Ubuntu, OpenSuse, SLES Linux system with TPM enabled as Client/Host system to be verified. We use Fedora 17 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

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 ubuntu

- ➢ Typing "ufw disable" in command

3.2.3 For SLES

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

3.3 Install required modules

3.3.1 For fedora

yum -y install httpd

dramatic

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 SLES

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.fc14.x86_64.rpm

3.4.2 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

3.4.3 For SLES

- ➤ 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, install modules

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

4.3.2   For RHEL 6.4, install modules

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

- ➢ trousers
- ➢ java-1.7.0-openjdk
- ➢ and make sure the TrouSers service is started:
  - service tcsd restart

4.3.3   For Ubuntu 13.04, install modules

- ➢ trousers
- ➢ libtspi1
- ➢ 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

4.3.4 For OpenSuse 12.3 and SLES 11, 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

4.3.5 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

> sh general-install.sh –ecs NVRAM

-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. It stores EC in NVRAM by default.

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 the integrity report will be written into the given directory. It will be saved on DB otherwise. If the property is set, OAT expects that given directory exists and it's accessible; on Fedora it means that the user 'tomcat' should be the directory owner.

        IR_DIR=/var/log/oat_ir
    - Set digest method 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 if it has to send the entire list of measurements or only measurements not already sent. If the property is set to "off" (or not set), OAT behaviour 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.