HIRS Installation Notes

Version 1.0.3

This page describes downloading, installing, setting up, and using the open source elements of the HIRS framework. For online version visit: https://github.com/nsacyber/HIRS/wiki/installation_notes .

Supported Platforms

The HIRS Attestation Certificate Authority (ACA) supports installation on CentOS 6 and 7 instances.

The HIRS Provisioner supports both types of TPMs: 1.2 and 2.0. TPM 1.2 support is available on CentOS 6 and 7. Due to the limitations on the libraries available on CentOS 6, TPM 2.0 support is only available on CentOS 7.

Before You Begin

Confirm that the target environments for both the ACA and the Provisioner (which may be the same) meet the below requirements:

1. The OS must be installed and configured for networking prior to installation. This should include:
    1. An administrative account that will be used for installing HIRS.
    2. A Fully Qualified Domain Name (FQDN) be assigned to the server running the ACA and
    3. A DNS system will resolve the name to an address. The certificate verification will not be able to complete successfully if the FQDN is not resolvable by DNS.
2. The hardware must meet the HIRS minimum requirements.
    1. HIRS ACA may be a virtual machine or physical device
        1. Centos 6 (latest) or 7.X OS
        2. 50GB HD space
        3. 6GB RAM
    2. The Client device must have a TPM 1.2 or TPM 2.0, and the TPM must be cleared and enabled in the BIOS/UEFI setup. The settings for the TPM are generally found in the BIOS/UEFI setup application which is specific the platform hosting the TPM. Refer to the server/desktop user manuals for instruction on how to enable/clear the TPM.
3. The Provisioner will need connectivity to the ACA. Check that any firewalls between the ACA server and Provisioner have port 8443 enabled.
4. Setup an OS repository for the device. The HIRS installation package will attempt to install its dependencies for the system local software repository if they are not currently

installed. It is highly suggested that an repository be setup prior to avoid dependency issues.

5. Dependencies for the HIRS-Provisioner using TPM 1.2 provisioning (Centos 6 or Centos 7) include:
    1. Java 1.8 (latest version)
    2. gcc
    3. TrouSerS
    4. tpm-tools

```
> sudo yum install java-1.8.0-openjdk gcc wget util-linux chkconfig sed
initscripts coreutils dmidecode trousers tpm-tools
```

6. To perform TPM 2.0 provisioning (Centos 7 latest version unless otherwise noted):
    1. Java 1.8 (latest version)
    2. gcc
    3. tpm2-tss
    4. tpm2-tools (1.1 or 3.0.1)
    5. log4cplus (requires epel-release)
    6. protobuf
    7. re2 (requires epel-release)

```
> sudo yum install epel-release java-1.8.0-openjdk gcc log4cplus protobuf re2
tpm2-tss tpm2-tools
```

7. Dependencies for the HIRS Attestation CA include:
    1. Java 1.8 (latest version)
    2. Tomcat (latest version)
    3. MySQL/MariaDB (latest version)

ACA Dependency installation on Centos 6:

```
> sudo yum install mysql-server openssl tomcat6 java-1.8.0 rpmdevtools
coreutils initscripts chkconfig sed grep iptables
```

ACA Dependency installation on Centos 7:

```
> sudo yum install mariadb-server openssl tomcat java-1.8.0 rpmdevtools
coreutils initscripts chkconfig sed grep firewalld
```

Getting the HIRS ACA and Provisioner

Currently, the HIRS ACA and Provisioner are provided as a set of CentOS 6 and 7 RPMs. In the future, the full source of these packages will be released along with documentation for building these packages. To download the currently released packages, visit the 'Releases' page.

Installing the ACA

To install the ACA, navigate to directory where the ACA was downloaded from the release page and enter the following command:

```
> sudo yum localinstall HIRS_AttestationCA*.rpm
```

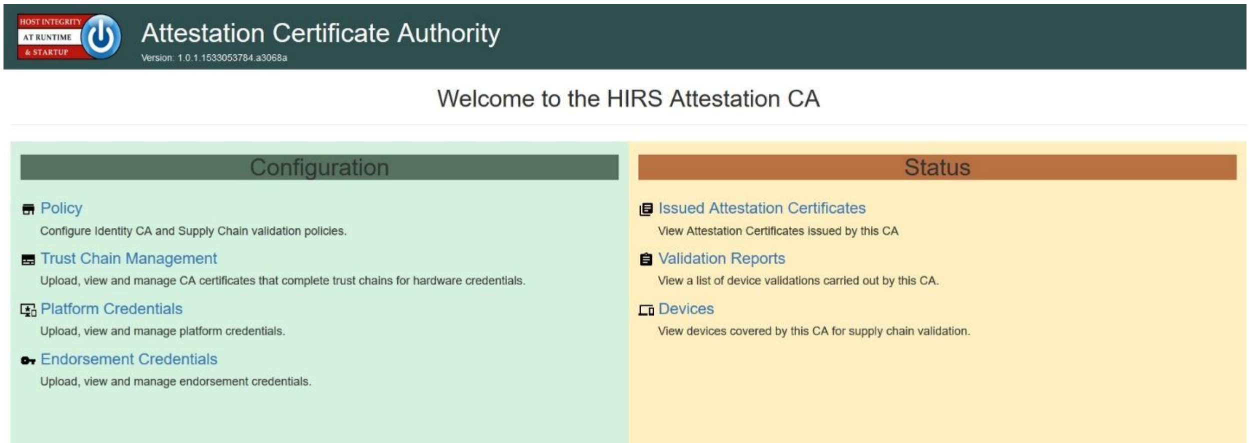
Testing the install:

After the ACA is installed, the HIRS ACA Portal should be up and running

In your browser, navigate to the ACA Portal URL:

```
https://<ACAserveraddress>:8443/HIRS_AttestationCAPortal/
```

On installation, the ACA creates a self signed certificate to use as its SSL certificate. This may produce a warning in your browser. Once you acknowledge the warning, and perhaps configure an exception, the following page should appear:



Attestation Certificate Authority

Version: 1.0.1.1533053784.a3068a

Welcome to the HIRS Attestation CA

Configuration

Policy
Configure Identity CA and Supply Chain validation policies.

Trust Chain Management
Upload, view and manage CA certificates that complete trust chains for hardware credentials.

Platform Credentials
Upload, view and manage platform credentials.

Endorsement Credentials
Upload, view and manage endorsement credentials.

Status

Issued Attestation Certificates
View Attestation Certificates issued by this CA

Validation Reports
View a list of device validations carried out by this CA.

Devices
View devices covered by this CA for supply chain validation.

Note that there may be delay after installing the ACA RPM as it starts up for the first time. The ACA portal will shortly be available via the browser.

Installing PACCOR

The HIRS Provisioners depend on the nsacyber/paccor project for part of the provisioning process.

In order to install and successfully run the Provisioner you will need to download the latest RPM package from the PACCOR repository. Once downloaded, perform the following:

```
> sudo yum install paccor-*.rpm
```

NOTE: For users working in a non-RHEL environment, please use the same package manager to install both the PACCOR and Provisioner packages, e.g. `apt` in a DEB environment.

Installing the Provisioner

The Provisioner is intended to be run on a host device with a TPM. It does not have to be installed on the HIRS ACA, but can be if the HIRS ACA is on a device with a TPM.

Before installing the Provisioner, you must install PACCOR, which is used by the Provisioner to collect information about the device on which it is running.

To install the Provisioner, you will need to determine if the TPM is version 1.2 or 2.0. If you are not sure, the following command should provide a hint. Ensure that the TPM is enabled in your BIOS/UEFI before running the command:

```
> dmesg | grep -i tpm_tis
```

There are different RPMs for TPM 1.2 and TPM 2.0. For TPM 1.2 there are 2 RPMs to install which are available on the release page.

For TPM 1.2 devices perform the following

```
> yum localinstall tpm_module*.rpm
> yum localinstall HIRS_Provisioner_TPM_1_2*.rpm
```

NOTE: Before installing the Provisioner on a device with a 2.0 TPM, it is important to know which version of `tpm2-tools` you have installed: 1.1.0 or 3.0.1. Each version requires its own process to manage access to the TPM. 1.1.0 uses a process called `resourcemgr`; 3.0.1 uses a process called `tpm2-abrmd`, which must be running as the `tss` user. If neither or both are running, or if the wrong one is running, provisioning will fail because communication with the TPM will fail. You can test for these processes running by using the commands `ps aux | grep resourcemgr` and `ps aux | grep abrmd`, respectively.

For TPM 2.0 devices only 1 RPM is needed:

```
> yum localinstall HIRS_Provisioner_TPM_2_0*.rpm
```

Provisioner Setup

The first step in configuring the installed provisioner is to point it to the ACA. Using the TPM 1.2 Provisioner, generate the hirs-site.config with the following command:

For a device with a TPM 1.2:

```
> sudo hirs-provisioner -c
```

for a device with a TPM 2.0:

```
> sudo hirs-provisioner-tpm2 -c
```

This produces a default hirs-site.config in /etc/hirs. Using the TPM 2.0 Provisioner, this file is generated by RPM install. This default setup must be edited.

The file should look like the following:

```
#*******************************************
#* HIRS site configuration properties file
#*******************************************
# Client configuration
TPM_ENABLED=
IMA_ENABLED=
CLIENT_HOSTNAME=$HOSTNAME
# Site-specific configuration
ATTESTATION_CA_FQDN=
ATTESTATION_CA_PORT=8443
BROKER_FQDN=
BROKER_PORT=61616
PORTAL_FQDN=
PORTAL_PORT=8443
```

The ATTESTATION_CA_FQDN and ATTESTATION_CA_PORT keys should be set to the hostname of the server running the ACA and the port on that server the ACA is configured to listen on (8443 by default), respectively. The BROKER_FQDN and PORTAL_FQDN should also be set to the hostname of the server running the ACA. TPM_ENABLED should be set to true and IMA_ENABLED should be set to false.

Testing the install:

Follow the Getting Started Guide to test provisioning of the TPM and performing supply chain validation.

Notes on SeLinux

The use of SeLinux with the default ("targeted") policy on Centos 7 is supported by a custom SeLinux policy file. As of the 1.1 release the SeLinux policy file that enables tomcat to use mysql will be installed by default when installing the HIRS ACA using the release rpm package. You will need to make sure you have the policycoresutils package to enable semodule used by the rpm. To enable the policy manually run the following command as root:

```
>sudo semodule -i /opt/hirs/extras/aca/tomcat-mysql-hirs.pp
```