Apache HTTP Server 2.2.x and Luna SA/Luna PCI

Integration Guide

Preface

Part Number: 009502-003 (Rev B, 08/2009)

SafeNet, Inc.

4690 Millennium Drive
Belcamp, Maryland 21017
USA

Limitations

This document does not include the steps to set up the third-party software. The steps given in this document must be modified accordingly. Refer to Luna SA / Luna PCI documentation for general Luna setup procedures.

Disclaimers

The foregoing integration was performed and tested only with the specific versions of equipment and software and only in the configuration indicated. If your setup matches exactly, you should expect no trouble, and Customer Support can assist with any missteps. If your setup differs, then the foregoing is merely a template and you will need to adjust the instructions to fit your situation. Customer Support will attempt to assist, but cannot guarantee success in setups that we have not tested.

Technical Support

If you encounter a problem while installing, registering or operating this product, please make sure that you have read the documentation. If you cannot resolve the issue, please contact your supplier or SafeNet support.

SafeNet support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between SafeNet and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Technical Support Contact Information:
Phone: 800-545-6608, 410-931-7520
Email: support@safenet-inc.com

THIS PAGE INTENTIONALLY LEFT BLANK

Table of Contents

THIS PAGE INTENTIONALLY LEFT BLANK

Chapter 1
Introduction

This document covers the necessary information to install, configure and integrate Apache HTTP Server v2.2.x with SafeNet Luna Hardware Security Modules (HSM).

The Luna HSMs integrates with the Apache HTTP Server to provide significant performance improvements by off-loading cryptographic operations from the Apache HTTP Server to the Luna HSMs. In addition, the Luna HSMs provides extra security by protecting and managing the server's high value SSL private key within a FIPS 140-2 certified hardware security module.

Scope

3rd Party Application Details

- Apache HTTP Server v2.2.x for Unix

Supported Platforms

The following platforms are supported for Luna SA 1U v4.4.0:

- Red Hat Enterprise Linux 5
- Solaris 10 SPARC
- Solaris 10 x86
- AIX 5.3

The following platforms are supported for Luna PCI v3.0:

- Red Hat Enterprise Linux 5
- Solaris 10 SPARC

HSMs and Firmware Version

- K5 HSM f/w 4.6.8 (Luna SA)
- K5 HSM f/w 4.7.1 (Luna PCI)

Library and Driver Support

- PKCS#11 v2.01 dynamic library

Distributions

- Luna SA 1U Appliance s/w v4.4.0
- Luna SA Client s/w v4.4.0
- Luna PCI Client s/w v3.0

Prerequisites:

Luna SA Setup:

Please refer to the **Luna SA** documentation for installation steps and details regarding to configure and setup the box on RHEL, Solaris SPARC, and Solaris x86 systems. Before you get started ensure the following:

- Luna SA appliance a secure admin password
- Luna SA a hostname, suitable for your network
- Luna SA network parameters are set to work with your network
- Initialized the HSM on the Luna SA appliance.
- Created and exchanged certificates between the Luna SA and your "Client" system.
- Created a partition on the HSM, remember the partition password that will be later used by the Apache HTTP Server. Register the Client with the partition. And run the "vtl verify" command on the client system to display a partition from Luna SA. The general form of command is “/usr/lunasa/bin/vtl verify”.
- Enabled Partition "Activation" and "Auto Activation" (Partition policy settings 22 and 23 (applies to Luna SA with Trusted Path Authentication [which is FIPS 140-2 level 3] only).

Luna PCI Setup:

Please refer to the **Luna PCI** documentation for installation steps and details regarding configuring and setting up the box on RHEL and Solaris SPARC systems. Before you get started ensure the following:

- Initialize the HSM on the Luna PCI appliance
- Create a partition on the HSM that will be later used by the Apache HTTP Server.
- Enable Partition "Activation" and "Auto Activation" (Partition policy settings 22 and 23 (applies to Luna PCI with Trusted Path Authentication [which is FIPS 140-2 level 3] only).

Apache v2.2.x Setup:

Apache HTTP Server 2.2.x installation files are provided in the Luna SA v4.4.0 / Luna PCI 3.0 product CD to carry on with the integration process. Apache HTTP Server is a separate installation, in addition to Luna SA/ Luna PCI client software.

Note: If you already have Apache installed, uninstall it before proceeding with the installation.

Chapter 2
Integrating Apache HTTP Server 2.2.x with Luna SA

To configure Apache HTTP Server 2.2.x to recognize the Luna SA 4.4.0 cryptographic device:

1. Traverse to the directory in the product CD:
   /cdrom/source/apache

2. Run the install script:
   sh install.sh

3. The install script copies the relevant apache configuration scripts to the Luna SA installation directory:
   /usr/lunasa/apache

4. The Luna SA configuration file (/etc/Chrystoki.conf) is now configured for Apache HTTP Server.

```
Misc = {
Apache = 1;
}
EngineLunaCA3 = {
EnableSessionMutex = 1;
NO_NORM_FINALIZE = 0;
NO_FORK_FINALIZE = 0;
DisableRand = 1;
DisableDsa = 1;
DisableRsa = 0;
FORK_CHECK = 0;
EngineInit = 1:10:11;
LibPath = /usr/lib/libCryptoki2.so;}
```

5. Traverse to the directory:
   /usr/lunasa/apache

Note: For AIX 5.3, use Apache HTTP Server v2.2.11 and edit the abuild-2.2 script with APACHEVER="2.2.11" instead of APACHEVER="2.2.9"

6. Run the configuration script to install Apache HTTP Server v2.2.x and Openssl 0.9.8x for Luna SA:
   ./abuild-2.2 --build

7. Traverse to the directory:

   For **RHEL:**
   /usr/lunasa/apache/linux

   For **Solaris SPARC**:
   /usr/lunasa/apache/solaris

   For **Solaris x86**:
   /usr/lunasa/apache/solaris_x86

   For **AIX**:
   /usr/lunasa/apache/aix

8. Now open a session to the Luna SA using the **sautil** utility under the respective (linux, solaris , solaris_x86 or aix) folder.
   ./sautil -o -s <slot number> -i 10:11 -p <partition password>

   where:
   -o -> open session
   -s -> slot
   -i -> application IDs
   -p -> partition password

9. Under /usr/lunasa/apache, run the **abuild-2.2** script to generate keys on the Luna SA.
   ./abuild-2.2 --genrsa

   Enter the relevant information as prompted for the keys to be generated.

10. Traverse to apache installation directory:
    /usr/local/apache2/conf

11. Open the apache configuration file (httpd.conf) and edit the **ServerName** field with the hostname or IP address of the server.

12. Traverse to the directory:
    /usr/local/apache2/conf/extra

13. Open the ssl configuration file (httpd-ssl.conf) and edit the Virtual Host section as below:
    <Virtual Host Hostname or IP Address:443>

14. Traverse to the directory:
    /usr/local/apache2/bin

15. Start the Apache HTTP Server with the **SSL** option:
    ./apachectl -DSSL.

16. Open any browser (IE/Firefox) and access the HTTP Server:
    https://<HostName or IP Address>

17. Accept the certificate.

Chapter 3
Integrating Apache HTTP Server 2.2.x with Luna PCI

To configure Apache HTTP Server 2.2.x to recognize the Luna PCI cryptographic device:

1. Traverse to the directory in the product CD:
   /cdrom/source/apache

2. Run the install script:
   sh install.sh

3. The install script copies the relevant apache configuration scripts to the Luna PCI installation directory:
   /usr/lunapci/apache

4. The Luna PCI configuration file (/etc/Chrystoki.conf) is now configured for Apache HTTP Server.

```
Misc = {
Apache = 1;
}
EngineLunaCA3 = {
EnableSessionMutex = 1;
NO_NORM_FINALIZE = 0;
NO_FORK_FINALIZE = 0;
DisableRand = 0;
DisableDsa = 0;
DisableRsa = 0;
FORK_CHECK = 0;
EngineInit = 1:10:11;
LibPath = /usr/lib/libCryptoki2.so;}
```

5. Traverse to the directory:
   /usr/lunapci/apache

6. Run the configuration script to install Apache HTTP Server v2.2.x and Openssl 0.9.8x for Luna PCI:
   ./abuild-2.2 --build

7. Traverse to the directory:

   For **RHEL:**
   /usr/lunapci/apache/linux

   For **Solaris SPARC**:
   /usr/lunapci/apache/solaris

8. Now open a session to the Luna PCI using the **sautil** utility under the respective (linux or solaris) folder.
   ./sautil -o -s <slot number> -i 10:11 -p <partition password>

   where:

-o -> open session
-s -> slot
-i -> application IDs
-p -> partition password

9. Under /usr/lunapci/apache, run the **abuild-2.2** script to generate keys on the Luna PCI.
   ./abuild-2.2 --genrsa

   Enter the relevant information as prompted for the keys to be generated.

10. Traverse to apache installation directory:
    /usr/local/apache2/conf

11. Open the apache configuration file (httpd.conf) and edit the **ServerName** field with the hostname or IP address of the server.

12. Traverse to the directory:
    /usr/local/apache2/conf/extra

13. Open the ssl configuration file (httpd-ssl.conf) and edit the Virtual Host section as below:
    <Virtual Host Hostname or IP Address:443>

14. Traverse to the directory:
    /usr/local/apache2/bin

15. Start the Apache HTTP Server with the **SSL** option:
    ./apachectl -DSSL.

16. Open any browser (IE/Firefox) and access the HTTP Server:
    https://<HostName or IP Address>

17. Accept the certificate.

Chapter 4 Troubleshooting Tips

1. Problem : Error message **“httpd: bad group name daemon”** when trying ./apachectl –DSSL
   Solution:
   1. Edit /usr/local/apache2/conf/httpd.conf
   2. Change the line **"User daemon" to "User nobody"** and the line **"Group daemon" to "Group nobody"**. This uses the standard UNIX/AIX user called "nobody".

   OR

   1. Create a UNIX user and UNIX group both called daemon.

2. Problem : For OpenSSL or Apache compilation error on AIX 5.3
   Solution:

   Set following environment variables on AIX 5.3:
   export PATH=$PATH:/usr/ccs/bin
   export PATH=$PATH:/usr/local/ssl
   export PATH=$PATH:/usr/local/ssl/bin
   export PATH=$PATH:/opt/freeware/bin
   export LIBRARY_PATH=$LIBRARY_PATH:/usr/local/ssl/lib