SUN Cobalt™

Enabling SSL on a Sun Cobalt™ InterShop Commerce RaQ 3 Server

1 Introduction

The Intershop 4 commerce system uses the default HTTP port 8080 in its basic configuration on the Sun Cobalt™ RaQ servers. The decision to implement it this was made at the behest of Intershop when they were advised that the Cobalt servers had an existing web server providing administrative and other services on the *normal* http port 80. Intershop was provided with several Sun Cobalt™ RaQ 3 servers with their software installed in this configuration for testing.

Table of Contents

1.1 Audience

The audience for this technical note are developers who want to enable Secure Socket Layer (SSL) on their InterShop Commerce Sun Cobalt™ RaQ 3 servers

1.2 Applicable Products

This technical note applies only to the Sun Cobalt™ RaQ 3 server with Intershop 4.

Important

There is no warranty implied or otherwise associated with these instructions. Back up all files before starting modification of your server. Use at your own risk.

1.3 Task Analysis

There is only one field inside of the Intershop database for both the host name and the target port number. Without going into specific details, this means that for an Intershop 4 system to employ SSL, it must either operate on the default HTTP port 80 or software modifications must be made to the internal Intershop modules. As the latter is proprietary to Intershop, Sun Cobalt™ has opted for the former.

There were, and are, several ways to do this task. The first would be to combine all the functionality for both the Cobalt GUI server and Intershop 4 server to operate with a single server. While this might seem initially appealing it has the distinct disadvantage that *any* modification to either system could potentially result in both systems becoming unoperational. Using this rationale, this technical note suggests moving the Cobalt GUI server to port 8080 and brought the Intershop 4 server to port 80. This will hopefully minimize any configuration, update, or other conflicts which might arise.

---

2 Enabling SSL on the a Sun Cobalt™ Intershop Commerce RaQ 3 Server

Follow these instructions to enable SSL with Intershop 4 on a Sun Cobalt RaQ 3 server:

1) Log into the server as the Admin.

2) Become the root user. Type:

```
su -
```

3) Type the following command to shut down Intershop before starting work:

```
/etc/rc.d/init.d/intershop4 stop
```

4) Edit the following files and change all instances of the number 80 to the number 8080:

```
/etc/httpd/conf/httpd.conf
/etc/httpd/conf/httpd.conf.master
/etc/httpd/conf/httpd.conf.packagesave


/etc/admserv/conf/srm.conf
/etc/admserv/conf/srm.conf.master
```

5) Execute the following command to re-read the modified configuration files for the Sun Cobalt GUI:

```
kill -HUP `cat /var/run/httpd.pid`
```

6) Try to connect to the Sun Cobalt-provided administrative graphical user interface (GUI) using a web browser with the following URL, replacing <host name> with your Sun Cobalt RaQ 3 server's fully qualified host name:

```
http://<host name>:8080/admin
```

Note that if you have added or plan to add any users to the server, their web pages can only be accessed using the following URL format:

```
http://<host name>:8080/~<user name>
```

Where *<user name>* is the appropriate user's identifier on the Sun RaQ 3 server.

7) Add the SSL-enabled server and support software for Intershop. To do this, you must download several pieces of software. The software and their download locations are listed in Table 1:

Table 1. Software and Location

Package	URL
bc-1.06	ftp://gatekeeper.dec.com/pub/GNU/bc/bc-1.06.tar.gz
mod_ssl-2.8.2-1.3.19	http://www.modssl.org/source/mod_ssl-2.8.2-1.3.19.tar.gz
apache-1.3.19	http://httpd.apache.org/dist/httpd/apache_1.3.19.tar.gz
openssl-0.9.6h	http://www.openssl.org/source/openssl-0.9.6.tar.gz

8) Create a temporary directory on the Sun RaQ 3 for these files. In this example, the temporary directory created is called `intershop`. It was created through the telnet connection with the following commands:

```
cd /home/sites/home/users/admin
mkdir intershop
cd intershop
```

9) Download the packages to your local machine and then upload (ftp) them as the Admin to the Sun Cobalt RaQ 3 temporary directory you created (above).

10) Using your telnet session, execute the following commands:

```
gzip -dc bc-1.06.tar.gz | tar -xvf -
gzip -dc apache_1.3.19.tar.gz | tar -xvf -
gzip -dc mod_ssl-2.8.2-1.3.19.tar.gz | tar -xvf -
gzip -dc openssl-0.9.6.tar.gz | tar -xvf -

cd bc-1.06
./configure
make
make install

cd ../openssl-0.9.6 -fPIC
make
make install

cd ../mod_ssl-2.8.2-1.3.19
./configure --with-apache=../apache_1.3.19

cd ../apache_1.3.19
SSL_BASE=../openssl-0.9.6
export SSL_BASE
./configure  \
    --enable-module=so \
    --enable-module=ssl \
    --prefix=/home/InterShop/isroot4/httpd
make
make install
```

11) You should now be able to check you base installation of SSL-enabled Apache for use with Intershop 4 by executing the following command:

```
/home/InterShop/isroot4/httpd/bin/apachectl start
```

Note
You might see warnings about the use of EAPI but `mod_ssl` requires this, No ill effects have been reported.

You should be able to connect to your Intershop site using a web browser and the URL `http://<host name>` where `<host name>` is replaced by your RaQ 3's fully qualified dns name.

---

12) After you have finished verifying that the new installation of Apache is functional, execute the command:

```
 /home/InterShop/isroot4/httpd/bin/apachectl stop
```

13) Modify the new Apache httpd.conf file for Intershop 4 so that SSL is enabled. Edit the file `/home/InterShop/isroot4/httpd/conf/httpd.conf` and make the following changes:

• Search for the text "Port 8080" and change it to read "Port 80".

• Search for the text "Listen 8080" and change it to read "Listen 80"

• Add the text "Listen 443" under the line "Listen 80"

• Search for the text "libWIApache.so" and change it to read "libWIApacheSSL.so"

• Search for the text "ISFCGIAdapter.so" and change it to read "ISFCGIAdapterSSL.so"

• Search for the text "IISFCGIReader.so" and change it to read "ISFCGIReaderSSL.so"

14) Append the following lines to the end of the file, replacing the text NETWORK_ADDRESS with the IP address of you RaQ 3 server:

```
#########################################################
# The following are mod_ssl defines
# See mod_ssl documents for more information
#########################################################

SSLSessionCache         none
SSLMutex   file:logs/ssl_mutex

SSLRandomSeed startup file:/dev/urandom 512
SSLRandomSeed connect file:/dev/urandom 512


SSLLog      logs/ssl_engine_log
SSLLogLevel info




<VirtualHost NETWORK_ADDRESS>

# Using defines from global section

</VirtualHost>



<VirtualHost NETWORK_ADDRESS:443>
```

```
    SSLEngine on
    SSLCipherSuite
ALL:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP:+eNULL
    SSLCertificateFile /home/InterShop/isroot4/httpd/conf/certificate
    SSLCertificateKeyFile /home/InterShop/isroot4/httpd/conf/key

    TransferLog logs/transfer_log

</VirtualHost>

##########################################################
# End of mod_ssl defines
##########################################################
```

The next step is to generate and install a private key and certificate for test purposes only. To do so, execute the following commands:

```
/home/sites/home/users/admin/intershop/apache_1.3.19/make certificate
```

Give appropriate answers for each of the questions asked. If you make an error, you can type `Control-C` and re-execute the command to start over.

When prompted for encrypting your private key, choose the **N(o)** option.

Once completed, type the following:

```
cp /home/sites/home/users/admin/intershop/apache_1.3.19/conf/ssl.crt/
server.crt \
    /home/InterShop/isroot4/httpd/conf/certificate

chmod ugo-rwx /home/InterShop/isroot4/httpd/conf/certificate
chmod u+r /home/InterShop/isroot4/httpd/conf/certificate

cp /home/sites/home/users/admin/intershop/apache_1.3.19/conf/ssl.key/
server.key \
    /home/InterShop/isroot4/httpd/conf/key


chmod ugo-rwx /home/InterShop/isroot4/httpd/conf/key
chmod u+r /home/InterShop/isroot4/httpd/conf/key
```

3 Testing the server

To test the server. type the following:

```
/home/InterShop/isroot4/httpd/bin/apachectl startssl
```

Note that the errors previously received during the startup of Apache regarding EAPI should not appear. This is because EAPI is a requirement `for mod_ssl` and the Intershop 4 modules for SSL were compiled correctly for this functionality.

Verify that SSL is operating correctly by using your web browser to connect to you Sun Cobalt RaQ 3 / Intershop 4 server using the following URL:

```
https://<host name>
```

Shut down the Intershop Apache server before continuing with the following command:

```
/home/InterShop/isroot4/httpd/bin/apachectl stop
```

There are two last files that you must be edit. By modifying these files, you will reset the Intershop 4 database to point to the correct port.

Edit and change all instances of the number 8080 to 80 in these files:

```
/etc/rc.d/init.d/is4.startup1.sh
/etc/rc.d/init.d/is4.adjustdb.sql
```

3.1 Restarting Intershop

You must restart the entire Intershop 4 software. You must be logged in as root to execute these commands. Type:

```
/etc/rc.d/init.d/intershop4 stop
```

Wait until all commands are executed and the shell prompt is again active. Type:

```
/etc/rc.d/init.d/intershop4 start
```

Intershop 4 should now be operational with SSL on your Sun Cobalt RaQ 3 server. You can enable SSL via the administrative control panels and also use it for secure transactions by modifying your form templates to use the `#FormTagAttributeSSL` tag.

4 Implementation Notes

1) The move of the Cobalt graphical user interface (GUI) server from port 80 to port 8080 has not been tested fully through proper Quality Assurance procedures. This is an unsupported modification to the server; however, Sun Cobalt has been supplied with a copy of these instructions for their own reference and comment.

2) Any patches, Sun Cobalt-supplied or otherwise, to the Sun Cobalt GUI Apache server(s) might require that you re-edit the `httpd.conf[.master|.packagesave]` and `srm.conf[.master]` files mentioned in the first section of this document.

3) Once you obtain a real private key and certificate they should be, in the described setup, be placed at the following locations:

```
/home/InterShop/isroot4/httpd/conf/key
/home/InterShop/isroot4/httpd/conf/certificate
```

Their permissions should be set to root user `read only` for security. Refer to the key-certificate creation and copy section for the appropriate `chmod` commands to perform this action.