SPOnRedHatFedoraCore4

Deploying the SP on Fedora Core 4

We have deployed a Shibboleth 1.3 SP on the following system:

- Red Hat Fedora Core 4 (Linux 2.6.14-1.1656_FC4smp #1 SMP)
- Apache 2.0.54

Protected resources:

- https://computer.ncsa.uiuc.edu/gridshib-ca/
- TestingGridShibCA (internal use only)

The SP providerId:

- https://test-sp.ncsa.uiuc.edu/shibboleth

Note: All NCSA SP providerIds should satisfy the pattern `^https://\(.+\.)?ncsa\.uiuc\.edu/shibboleth$`

Test apache

- http://computer.ncsa.uiuc.edu/
- https://computer.ncsa.uiuc.edu/

If apache is not responding, try poking a couple of holes in the firewall:

```
/sbin/iptables -I RH-Firewall-1-INPUT -p tcp --dport http -j ACCEPT
/sbin/iptables -I RH-Firewall-1-INPUT -p tcp --dport https -j ACCEPT
```

To save this iptables configuration use the following command:

```
/etc/init.d/iptables save
```

Download/install RPMs

```
# get all the RPMs:
$ wget -r -l1 --no-parent --no-directories -A.rpm -o log.txt \
  http://shibboleth.internet2.edu/downloads/RPMS/i386/fedora/4/ &
# sanity check:
$ rpm -ql --package log4cpp-0.3.5rc1-1.i386.rpm

# install log4cpp:
$ su
$ rpm -ihv log4cpp*
$ rpm -ql log4cpp-0.3.5rc1-1
$ rpm -ql log4cpp-debuginfo-0.3.5rc1-1
$ rpm -ql log4cpp-devel-0.3.5rc1-1
$ rpm -ql log4cpp-docs-0.3.5rc1-1

# install xerces:
$ rpm -ihv xerces*
$ rpm -ql xerces-c-2.6.1-2
$ rpm -ql xerces-c-debuginfo-2.6.1-2
$ rpm -ql xerces-c-devel-2.6.1-2
$ rpm -ql xerces-c-doc-2.6.1-2
$ rpm -ql xerces-c-samples-2.6.1-2

# install xml-security:
$ rpm -ihv xml-security*
$ rpm -ql xml-security-c-1.2.0-1
$ rpm -ql xml-security-c-debuginfo-1.2.0-1
$ rpm -ql xml-security-c-devel-1.2.0-1
```

```
$ rpm -ql xml-security-c-docs-1.2.0-1

# install opensaml:
$ rpm -ihv opensaml*
$ rpm -ql opensaml-1.1-5
$ rpm -ql opensaml-debuginfo-1.1-5
$ rpm -ql opensaml-devel-1.1-5

# test opensaml (90% success rate is expected):
$ export SAMLSCHEMAS=/usr/share/xml/opensaml
$ /usr/bin/samltest
Running 10 tests
...
Failed 1 of 10 tests
Success rate: 90%

# install shibboleth:
$ rpm -ihv shibboleth*
error: Failed dependencies:
                  selinux-policy-targeted-sources is needed by
                  shibboleth-selinux-policy-targeted-1.3-8.i386

# install selinux-policy-targeted-sources:
$ yum install selinux-policy-targeted-sources
$ rpm -ql selinux-policy-targeted
/etc/selinux
/etc/selinux/targeted
/etc/selinux/targeted/booleans
/etc/selinux/targeted/contexts
/etc/selinux/targeted/contexts/customizable_types
/etc/selinux/targeted/contexts/dbus_contexts
/etc/selinux/targeted/contexts/default_contexts
/etc/selinux/targeted/contexts/default_type
/etc/selinux/targeted/contexts/failsafe_context
/etc/selinux/targeted/contexts/files
/etc/selinux/targeted/contexts/files/file_contexts
/etc/selinux/targeted/contexts/files/file_contexts.homedirs
/etc/selinux/targeted/contexts/files/homedir_template
/etc/selinux/targeted/contexts/files/media
/etc/selinux/targeted/contexts/initrc_context
/etc/selinux/targeted/contexts/port_types
/etc/selinux/targeted/contexts/removable_context
/etc/selinux/targeted/contexts/userhelper_context
/etc/selinux/targeted/contexts/users
/etc/selinux/targeted/contexts/users/root
/etc/selinux/targeted/policy
/etc/selinux/targeted/policy/policy.19
/etc/selinux/targeted/users
/etc/selinux/targeted/users/local.users
/etc/selinux/targeted/users/system.users
/usr/share/man/man8/ftpd_selinux.8.gz
/usr/share/man/man8/httpd_selinux.8.gz
/usr/share/man/man8/kerberos_selinux.8.gz
/usr/share/man/man8/named_selinux.8.gz
/usr/share/man/man8/nfs_selinux.8.gz
/usr/share/man/man8/nis_selinux.8.gz
/usr/share/man/man8/rsync_selinux.8.gz
/usr/share/man/man8/samba_selinux.8.gz
/usr/share/man/man8/ypbind_selinux.8.gz

# try to install shibboleth again:
$ rpm -ihv shibboleth*
cat: /selinux/policyvers: No such file or directory
cat: /selinux/mls: No such file or directory
cat: /selinux/policyvers: No such file or directory
cat: /selinux/mls: No such file or directory
/usr/sbin/load_policy:  Warning! unable to get boolean names:  No such file or directory
/usr/sbin/load_policy:  security_load_policy failed
make: *** [tmp/load] Error 3

# try to update shibboleth:
```

```
$ rpm -Uhv shibboleth*
Preparing...                                ########################################### [100%]
                  package shibboleth-1.3-8 is already installed
                  package shibboleth-debuginfo-1.3-8 is already installed
                  package shibboleth-devel-1.3-8 is already installed
                  package shibboleth-selinux-policy-targeted-1.3-8 is already installed

# remove shibboleth and selinux:
$ rpm --erase shibboleth-1.3-8 shibboleth-debuginfo-1.3-8 shibboleth-devel-1.3-8 shibboleth-selinux-policy-
targeted-1.3-8
$ rpm --erase selinux-policy-targeted-sources

# custom install shibboleth (no selinux):
$ rpm -ihv shibboleth-1.3-8.i386.rpm shibboleth-debuginfo-1.3-8.i386.rpm shibboleth-devel-1.3-8.i386.rpm
$ rpm -ql shibboleth-1.3-8
$ rpm -ql shibboleth-debuginfo-1.3-8
$ rpm -ql shibboleth-devel-1.3-8

# test opensaml (100% success rate is expected):
$ export SAMLSCHEMAS=/usr/share/xml/shibboleth
$ /usr/bin/samltest
Running 10 tests
...
OK!
```

Install SRPMs

If you prefer to install from source, follow these directions: http://shib.kuleuven.be/docs/sp/build-rpms.shtml

Modify httpd.conf

```
# modify apache config:
$ cp /etc/httpd/conf/httpd.conf /tmp/httpd.conf.bak
$ sed 's/^#ServerName www.example.com:80/ServerName computer.ncsa.uiuc.edu:80/' /etc/httpd/conf/httpd.conf >
/tmp/httpd.conf
$ sed 's/^UseCanonicalName Off/UseCanonicalName On/' /tmp/httpd.conf > /etc/httpd/conf/httpd.conf

# modify ssl config:
$ cp /etc/httpd/conf.d/ssl.conf /tmp/ssl.conf.bak
$ sed 's/^SSLCertificateFile \/etc\/pki\/tls\/certs\/localhost.crt/SSLCertificateFile \/etc\/grid-security\
/hostcert.pem/' /etc/httpd/conf.d/ssl.conf > /tmp/ssl.conf
$ sed 's/^SSLCertificateKeyFile \/etc\/pki\/tls\/private\/localhost.key/SSLCertificateKeyFile \/etc\/grid-
security\/hostkey.pem/' /tmp/ssl.conf > /etc/httpd/conf.d/ssl.conf
$ sed 's/^#DocumentRoot "\/var\/www\/html"/DocumentRoot "\/var\/www\/html"/' /etc/httpd/conf.d/ssl.conf > /tmp
/ssl.conf
$ sed 's/^#ServerName www.example.com:443/ServerName computer.ncsa.uiuc.edu:443/' /tmp/ssl.conf > /etc/httpd
/conf.d/ssl.conf

# create secure resource:
$ mkdir /var/www/html/secure
$ echo '<p>secure</p>' > /var/www/html/secure/index.html
```

Tips:

```
# stop/start apache:
$ /usr/sbin/apachectl stop
$ /usr/sbin/apachectl start

# restart apache:
$ /usr/sbin/apachectl restart
```

Modify shib.conf

TBD

Modify shibboleth.xml

Mods too numerous to mention:

```
diff -b /etc/shibboleth/shibboleth.xml /etc/shibboleth/shibboleth.xml.dist
```

The most important change is the `RequestMap` element in shibboleth.xml:

```
<RequestMapProvider type="edu.internet2.middleware.shibboleth.sp.provider.NativeRequestMapProvider">
  <RequestMap requireSessionWith="IQ" applicationId="default">
        <!--
        This requires a session for documents in /secure on the containing host with http and
        https on the default ports. Note that the name and port in the <Host> elements MUST match
        Apache's ServerName and Port directives or the IIS Site name in the <ISAPI> element
        below.
        -->
        <Host name="computer.ncsa.uiuc.edu">
               <!-- protect /secure -->
               <Path name="secure" authType="shibboleth" requireSession="true" exportAssertion="true">
                 <!-- Example shows the folder "/secure/admin" assigned to a separate <Application> -->
                 <!--
                 <Path name="admin" applicationId="foo-admin"/>
                 -->
               </Path>
               <!-- protect /cgi-bin/SP-CA-protected but in general leave /cgi-bin unprotected -->
               <Path name="cgi-bin">
                 <Path name="SP-CA-protected" authType="shibboleth" requireSession="true" exportAssertion="
true"/>
               </Path>
        </Host>
  </RequestMap>
</RequestMapProvider>
```

Install debug scripts

Numerous useful test scripts, in a variety of languages: http://shib.kuleuven.be/download/sp/test_scripts/

Set log level="DEBUG"

```
# (may not be necessary)
$ touch /var/log/httpd/native.log
$ chmod 777 /var/log/httpd/native.log  # FIX THIS!
```

Generate bossie credential

https://bossie.doit.wisc.edu:3443/cert/i2server/csr

Join InQueue

TBD

Refresh metadata

```
# the wrong way to retrieve metadata:
$ wget http://wayf.internet2.edu/InQueue/IQ-metadata.xml

# the correct way to retrieve metadata:
$ wget http://wayf.internet2.edu/InQueue/inqueue.pem
$ /usr/sbin/siterefresh --cert inqueue.pem \
  --url http://wayf.internet2.edu/InQueue/IQ-metadata.xml \
  --out IQ-metadata.xml
```

Modify AAP.xml

TBD

How to use the shibd script

```
# this was done by the RPM:
$ /sbin/chkconfig --add /etc/shibboleth/shibd

# restart shibd:
$ /etc/init.d/shibd status
shibd is stopped
$ /etc/init.d/shibd start
Starting shibd:
$ /etc/init.d/shibd status
shibd (pid 2386) is running...
```

Upgrading the SP

```
# query old packages:
$ rpm -ql opensaml-1.1-5
$ rpm -ql opensaml-debuginfo-1.1-5
$ rpm -ql opensaml-devel-1.1-5
$ rpm -ql shibboleth-1.3-8
$ rpm -ql shibboleth-debuginfo-1.3-8
$ rpm -ql shibboleth-devel-1.3-8

# backup shibboleth config:
$ tar cvf /tmp/shibboleth-1.3-8.tar /etc/shibboleth/ /etc/init.d/shibd /etc/httpd/conf.d/shib.conf

# get opensaml and shibboleth rpms:
$ cd /tmp
$ wget -r -l1 --no-parent --no-directories -Aopensaml*.rpm -o log.txt http://shibboleth.internet2.edu/downloads
/RPMS/i386/fedora/4/ &
$ wget -r -l1 --no-parent --no-directories -Ashibboleth*.rpm -o log.txt http://shibboleth.internet2.edu
/downloads/RPMS/i386/fedora/4/ &

# query new packages:
$ rpm -qip opensaml-1.1-6.i386.rpm
$ rpm -qip opensaml-debuginfo-1.1-6.i386.rpm
$ rpm -qip opensaml-devel-1.1-6.i386.rpm
$ rpm -qip shibboleth-1.3-11.i386.rpm
$ rpm -qip shibboleth-debuginfo-1.3-11.i386.rpm
$ rpm -qip shibboleth-devel-1.3-11.i386.rpm

# test new packages:
$ rpm -U --test opensaml-1.1-6.i386.rpm
$ rpm -U --test opensaml-debuginfo-1.1-6.i386.rpm
$ rpm -U --test opensaml-devel-1.1-6.i386.rpm
$ rpm -U --test shibboleth-1.3-11.i386.rpm
$ rpm -U --test shibboleth-debuginfo-1.3-11.i386.rpm
```

```
$ rpm -U --test shibboleth-devel-1.3-11.i386.rpm

# stop shibd:
$ /etc/init.d/shibd status
shibd (pid 1712) is running...
$ /etc/init.d/shibd stop
/etc/init.d/shibd stop

# update opensaml:
$ rpm -Uvh opensaml-1.1-6.i386.rpm
$ rpm -Uvh opensaml-debuginfo-1.1-6.i386.rpm
$ rpm -Uvh opensaml-devel-1.1-6.i386.rpm

# test opensaml (90% success rate is expected):
$ export SAMLSCHEMAS=/usr/share/xml/opensaml
$ /usr/bin/samltest
..
Failed 1 of 10 tests
Success rate: 90%

# update shibboleth:
$ rpm -Uvh shibboleth-1.3-11.i386.rpm
$ rpm -Uvh shibboleth-debuginfo-1.3-11.i386.rpm
$ rpm -Uvh shibboleth-devel-1.3-11.i386.rpm

# test opensaml (100% success rate is expected):
$ export SAMLSCHEMAS=/usr/share/xml/shibboleth
$ /usr/bin/samltest
Running 10 tests
...
OK!

# start processes:
$ /etc/init.d/shibd status
shibd is stopped
$ /etc/init.d/shibd start
Starting shibd:
$ /etc/init.d/httpd graceful
```