Red Hat Enterprise Linux 7

Configuring httpd service in Apache

Version: 2.4

Running the httpd Service

```
Yum install httpd
```

Starting httpd service

Use apachectl and systemctl commands in place of service command.
Command to start in httpd service RHEL 6 or older versions

```
Service httpd start
```

In RHEL 7, use:

```
apachectl start
```

or

```
systemctl start httpd
```

Auto start on boot time (startup)

```
systemctl enable httpd.service
```

Note: use disable to the service to run in startup instead of enable.

Verify Service Status

```
Systemctl is-active httpd.service
```

Command	Description
systemctl start httpd.service Or systemctl start httpd or apachectl start	Start httpd service. Even if you do not include .service extension, system will know that it is a service and run it.
systemctl restart httpd.service	Stops httpd and start it immediately again.
systemctl reload httpd.service	Causes running httpd service to reload its configuration file. Any requests being currently processed will be interrupted. Client may see error message in web browser.
apachectl graceful	Reload configuration file without affecting any interruption.

It should show following symlink creation as a result if the service is not in startup already:

```
ln -s '/usr/lib/systemd/system/httpd.service' '/etc/systemd/system/multi-user.target.wants/httpd.service'
```

Configuration files

/etc/httpd/conf/httpd.conf	Main configuration file
/etc/httpd/conf.d	Additional configuration files can be located in this directory.

Sample configuration file: /etc/httpd/conf.d/shiba.com.np.conf

Note: Sample configuration files can be found in /usr/share/doc/httpd-VERSION/httpd-*.conf

```
<VirtualHost *:80>
    ServerAdmin shibaratna@gmail.com
    DocumentRoot "/var/www/vhosts/shiba.com.np/htdocs"
    ServerName www1.shiba.com.np
    ServerAlias www2.shiba.com
    ErrorLog "/var/log/httpd/shiba.com.np-error_log"
    CustomLog "/var/log/httpd/ shiba.com.np-access_log" common
</VirtualHost>
```

Note: www1.shiba.com.np and www2.shiba.com.np should have DNS entry. If not add these domain name in /etc/hosts. Add following line in /etc/hosts

```
192.168.0.1      www1.shiba.com.np    www2.shiba.com.np
```

Configuring SSL Server in Apache

Secure Sockets Layer (SSL): a cryptographic protocol that allows a server and a client to communicate securely [1].

Transport Layer Security (TLS): improved extension to SSL

Requeires: mod_ssl, which uses the OpenSSL toolkit to provide the SSL/TLS support.

Installing required module and package

```
yum install mod_ssl openssl
```

Adds: mod_ssl configuration in /etc/httpd/conf.d/ssl.conf

Using Existing Key:

IP address or domain name is changed.

- Certificates are issued for a particular IP address and domain name pair. If one of these value changes, the certificate becomes void.

You have a certificate from VeriSign and you are changing the server software.

- Certificate issued for one software will not work in another.

Copy/move certificate files in /etc/pki/tls/private/ and /etc/pki/tls/certs respectively:

```
cp mykey.key  /etc/pki/tls/private/server.key
cp certificate.crt  /etc/pki/tls/certs/server.crt
```

adding certificate to /etc/httpd/conf.d/ssl.conf:

```
SSLCertificateFile   /etc/pki/tls/certs/server.key
SSLCertificateKeyFile  /etc/pki/tls/private/server.crt
```

Note: it require restarting httpd service

Generating a New Key and Certificate (Self-Signed)

Require: crypto-utils

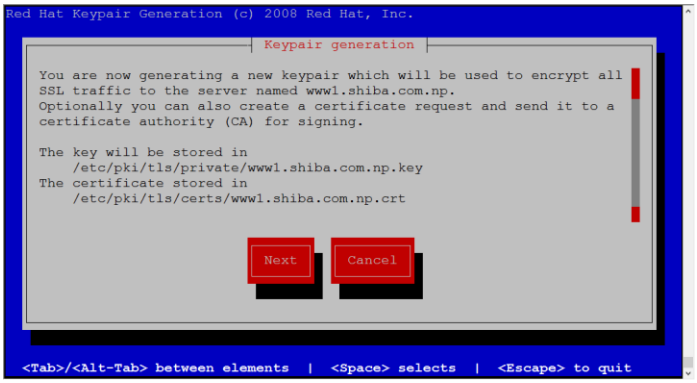
```
yum install crypto-utils
```

Steps to Generate certificate:

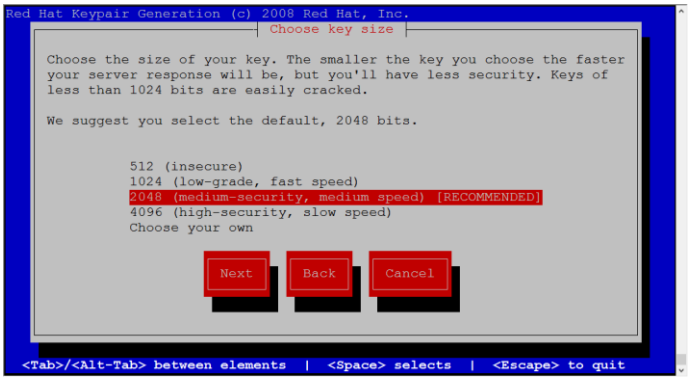
1. Use genkey command

```
yum install crypto-utils.x86_64
```

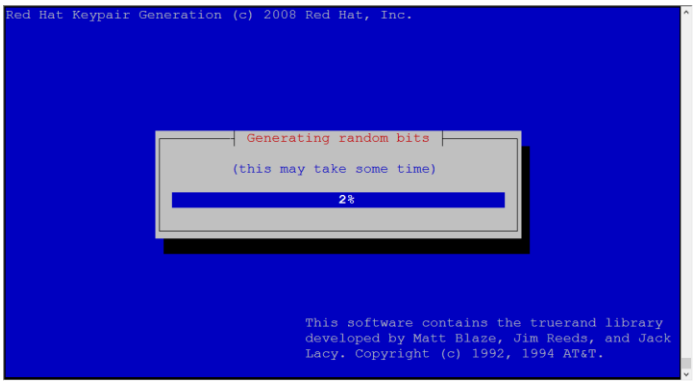
2. Brief information on where key will be stored after created:



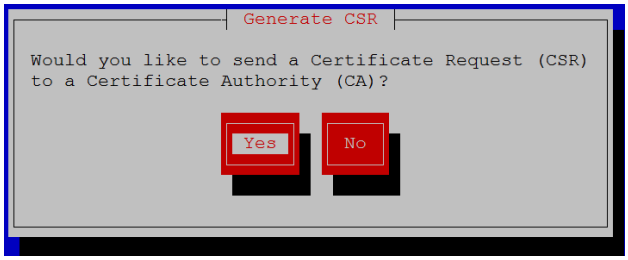
3. Choose security level



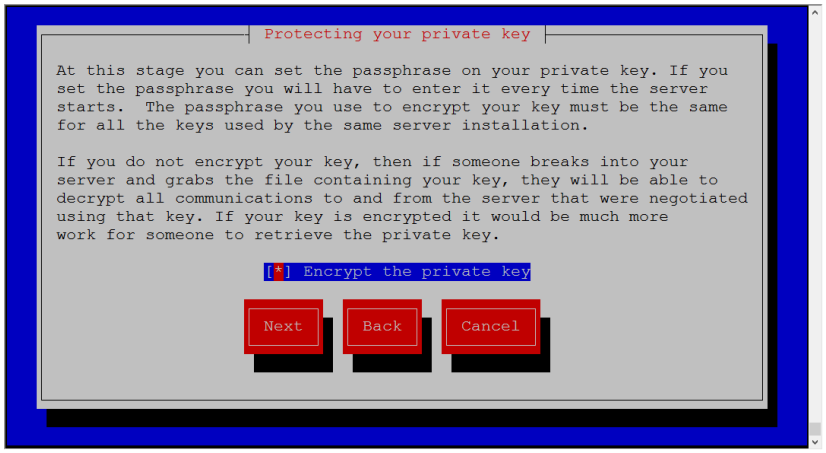
4. Generating random bits



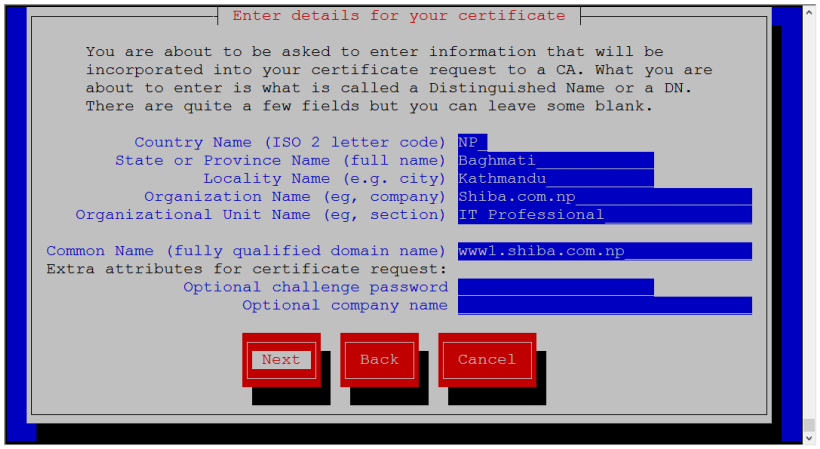
5. Certificate Request (choose no if you want to use self-signed certificate; only require if you want to require for verified digital certificate.)



6. Encrypting private key



7. Providing detail of the company



8. Output:

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIICxzCCAa8CAQAwgYExCzAJBgNVBAYTAk5QMREwDwYDVQQIEwhCYWdobWF0aTES
MBAGA1UEBxMJS2F0aG1hbmR1MRUwEwYDVQQKEwxTaGliYS5jb20ubnAxGDAWBgNV
BAsTD0lUIFByb2Zlc3Npb25hbDEaMBgGA1UEAxMRd3d3MS5zaGliYS5jb20ubnAw
ggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDAFYgw6pTA2IrHeuLXRpWB
1eBxJUFyuZw8/aZ9q/QBe2jj148RFSk8ZaC+s2ihsTvEhSf/nNqKrYGTfi4Mqbku
k7PkzA7NBNmO+A8u6uOAPw5TA2+IH6Ff4589O9KO/ucQ1TTYkTxR8LuOcRdWhR2l
paqshzBpXMFU8NvhMwkO6zwsdsxCzK4vBx4VfMBuGTDeMrxc/TtZ54rUVDTnZDFj
feI+QHHdlUXC1VhV04yJm5BrRXJCgeTk28EY+RtLpj9DT1O3/Q/yj+QXRvWkxPVA
eoMahiOpDeZVJRQTWLFXRyMSzve7uz5aEZTdqaEy88A9ISvc5D4COzDAgIRzI5u3
AgMBAAGgADANBgkqhkiG9w0BAQUFAAOCAQEASZsvoLTKC4xo6kVSn5vJ4msPkFaq
08Xb/Wdlkz664MrovYtuMwqnfz3EnYRaliCclz4KDDnmZWVzzSQzcDkfOlHN5UT7
fGqEMhZ/abJSYXdyzCz+FlWKrjI0u3CtL8rYg3m68xlc/QF8xAv4nqCk7xDNMuxE
zMq4gFPehL84TfAa2dvcYuy7p8gSGDwFi87GwsmVBH8mVgCNarzg6qlRqgym6S8R
Ssf6/DW7dq/JW9M7UA9a6yWFchZS2j4QXqktI1qJbVkY2xgQjGORnxl/KjLb+FVt
s3HlQZDCWfL0HNvPMNmrD/L5c5yoC2oofD5/AR0Bodn1ynciwiF7BRzr9g==
-----END NEW CERTIFICATE REQUEST-----


A copy of this CSR has been saved in the file
/etc/pki/tls/certs/www1.shiba.com.np.0.csr

Press return when ready to continue
```

Additional Help:

```
yum install httpd-manual
```

Configuring SQUID for Web Cache

```
vi /etc/squid/squid.conf
    #Add following lines
    #acl rule called mynet
    acl mynet src 172.16.0.0/16
    #acl rule called myhost
    acl myhost src 172.16.0.1
    #acl rule called prohibited
    acl prohibited dstdomain .games.com

    #Controlling Access to the acl rules created in above lines (runs in FIFO order)
    #deny myhost acl to access web site
    http_access deny myhost
    #deny prohibited destination sites to be opened
    http_access deny prohibited
    #allow mynet acl to access web site
    http_access allow mynet
```