1. **Sinh key và cert.**

#make server.key

# openssl rsa -in server.key -out server.key

#make server.csr

# openssl x509 -in server.csr -out server.crt -req -signkey server.key -days 1000

1. **Cài đặt httpd và Mod SSL**

Để thiết lập chứng chỉ tự ký, trước tiên chúng tôi phải chắc chắn rằng mod\_ssl, mô-đun Apache cung cấp hỗ trợ mã hóa SSL, đã được cài đặt máy chủ:

yum -y install httpd mod\_ssl  
sudo systemctl enable httpd.service  
systemctl start httpd.service

1. **Thiết lập chứng chỉ**

Điều tiếp theo cần làm là thiết lập các máy chủ ảo để hiển thị chứng chỉ mới.

sudo vi /etc/httpd/conf.d/ssl.conf

<VirtualHost \*:**443**>  
DocumentRoot /var/www/html  
ServerName www.example.com  
**SSLEngine on  
SSLCertificateFile /etc/ssl/private/certificate.crt  
SSLCertificateKeyFile /etc/ssl/private/private.key**  
</VirtualHost>

Khi bạn hoàn thành việc thực hiện những thay đổi này, bạn có thể lưu và đóng tệp.

Điều chỉnh tên tệp để khớp với tệp chứng chỉ của bạn:

SSLCertertFile phải là tệp chứng chỉ của bạn (ví dụ: your\_domain\_name.crt).

SSLCertertKeyFile phải là tệp chính được tạo khi bạn tạo CSR.

1. **Chuyển hướng đến HTTPS**

Để chuyển hướng tất cả lưu lượng truy cập được mã hóa SSL, hãy tạo và mở một tệp kết thúc bằng .conf trong thư mục /etc/httpd/conf.d:

sudo vi /etc/httpd/conf/httpd.conf

<VirtualHost \*:80>  
 ServerName www.example.com  
 Redirect "/" "https://www.example.com/"  
</VirtualHost>

Lưu và đóng tệp này khi bạn hoàn thành.

1. **Kiểm tra cấu hình Apache của bạn trước khi khởi động lại.**

apachectl configtest

Restart Apache.

systemctl restart httpd