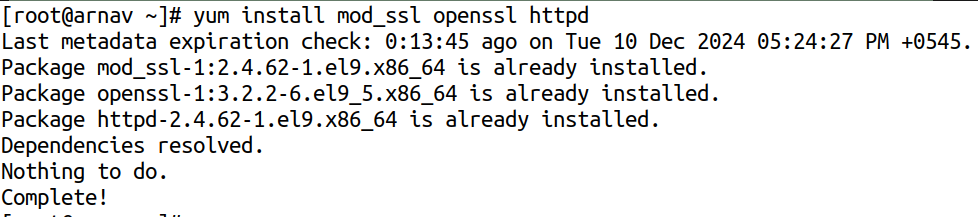
**Task 10**

**Configuring SSL-Enabled Apache (HTTPS) Server (self-signed)**

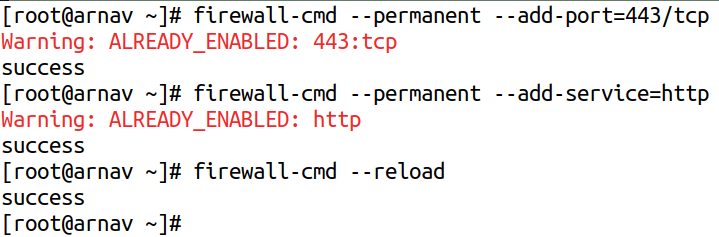
1. Install required package for HTTPS server (httpd, mod\_ssl). Also, start and enable web service.

To install all the required package for HTTPS server, i.e httpd, mod\_ssl, and openssl, we can simply use the command ‘yum install mod\_ssl openssl httpd’.



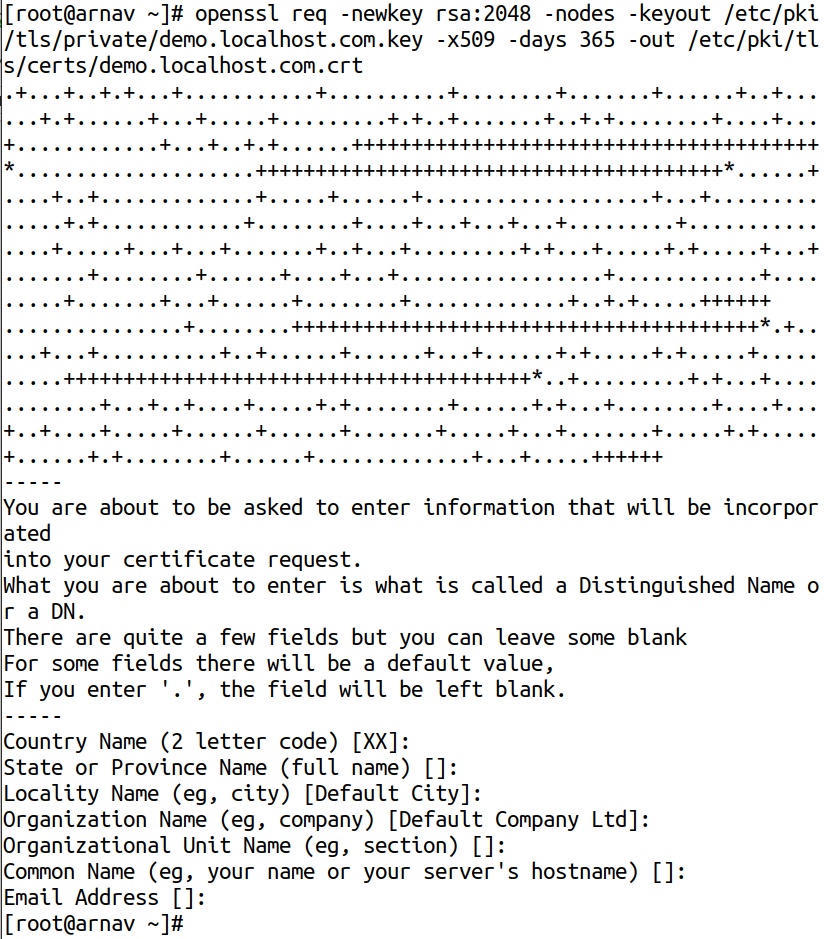
1. Allow https (port 443) packets to enter through the firewall.

We can simply use the firewall-cmd command to allow https packets through the firewall, rather than https as a service, we need to add http as service and then 44/tcp as port through the firewall.



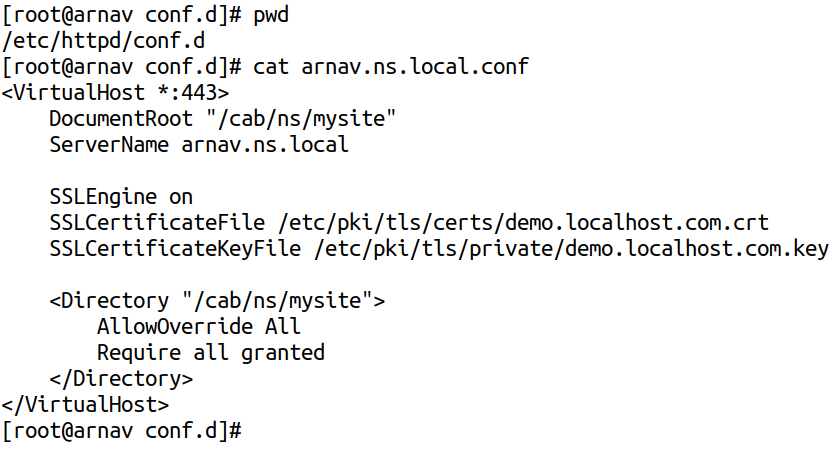
1. Generate self-signed key and cert files using openssl.

We can simply use openssl to generate a self-signed key and certificate file that we can use as ssl certificate, for that, we can use the command as follows:

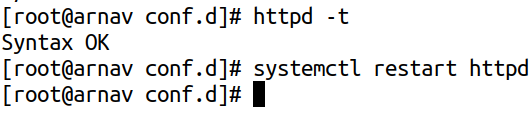


1. Configure web server to listen from port 443 and set DocumentRoot to “/cab/ns/mystie”, locate the required key and cert files. Include the necessary SELinux configuration.

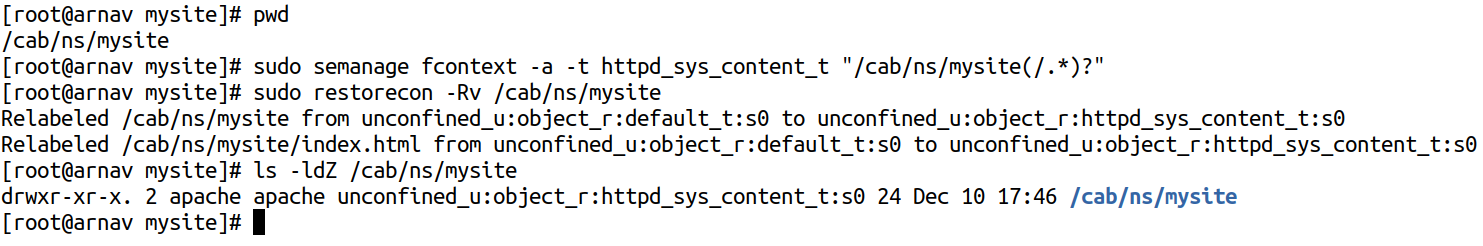
First, we need to define the domain as host entry in our /etc/hosts file, which we have previously done in the lab itself. Then, we need to define a new apache configuration file at the path /etc/httpd/conf.d, as:

The configuration file contains the ssl certificate we generated previously so that we can use https as well.

After writing the configuration, we can check the syntax of the configuration and the restart the webserver as:

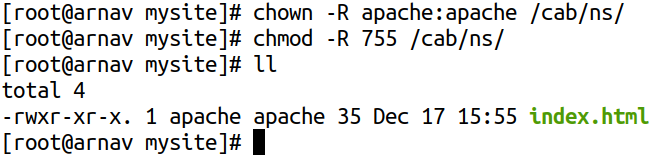


Then, we need to add the necessary SE Linux configuration to the files at /cab/ns/mysite as:



1. Host a web page called index.html on web server named arnav.ns.local.

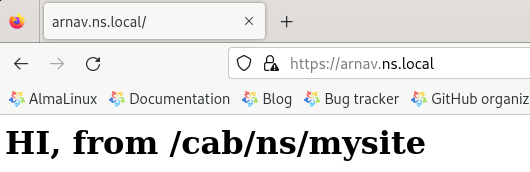
Now, to first host the website at domain, arnav.ns.local, we can add an index.html file at the path /cab/ns/mysite named index.html, and the give the directory required permission so that, the apache user can acess that location as:



The index.html file contains:



Then, we can reload httpd server and then can visit the site from our internal browser as:



We can further inspect the certificate as:

