**CERTIFICADO AUTO ASSINADO**

yum install openssl -y //instalar o openssl

openssl genrsa -out ca.key 4096//Gera uma chave com nome ca.key

openssl req -new -x509 -nodes -sha1 -days 365 -key \ /etc/pki/tls/private/apache-websrv01.key -out apache-websrv01.crt //gerar uma chave auto-assinada

*You are about to be asked to enter information that will be incorporated*

*into your certificate request.*

*What you are about to enter is what is called a Distinguished Name or a DN.*

*There are quite a few fields but you can leave some blank*

*For some fields there will be a default value,*

*If you enter '.', the field will be left blank.*

*-----*

*Country Name (2 letter code) [XX]:****BR***

*State or Province Name (full name) []:****SP***

*Locality Name (eg, city) [Default City]:****COTIA***

*Organization Name (eg, company) [Default Company Ltd]:****HOME***

*Organizational Unit Name (eg, section) []:****HOME***

*Common Name (eg, your name or your server's hostname) []:****apache-websrv01***

*Email Address []:*[***alvkennedy@gmail.com***](mailto:alvkennedy@gmail.com)

vim /etc/httpd/conf.d/ssl.conf //apontar o local da chave no arquivo.

*SSLCertificateFile /etc/pki/tls/certs/****apache-websrv01.crt***

*SSLCertificateKeyFile /etc/pki/tls/private/a****pache-websrv01.key***

systemctl restart httpd.service //Reiniciar apache

**CERTIFICADO COM UNIDADE ENTIDADE CERTIFICADORA (certificate signing request)**

openssl genrsa -out /etc/pki/tls/private/*apache-websrv01*.key //gerando chave

mkdir /etc/pki/tls/ssl.csr //cria diretório

cd /etc/pki/tls/ssl.csr/ //entra no diretório

openssl req -new -key /etc/pki/tls/private/*apache-websrv01*.key -out *apache-websrv01*.csr //gera chave csr que será enviada para a entidade

***NOTA: OU SE NÃO FOR ENVIAR PARA UNIDADE CERTIFICADORA, É POSSÍVEL GERAR COM ESSE COMANDO.***

***openssl x509 -req -days 730 -in apache-websrv01.csr -CA apache-websrv01.crt -CAkey apache-websrv01.key -set\_serial 01 -out public-apache-websrv01.crt***

*Referencia: https://blog.didierstevens.com/2008/12/30/howto-make-your-own-cert-with-openssl/*

*Country Name (2 letter code) [XX]:BR*

*State or Province Name (full name) []:SP*

*Locality Name (eg, city) [Default City]:COTIA*

*Organization Name (eg, company) [Default Company Ltd]:WORKGROUP*

*Organizational Unit Name (eg, section) []:WORKGROUP*

*Common Name (eg, your name or your server's hostname) []:apache-websrv01*

*Email Address []:alvkennedy@gmail.com*

*Please enter the following 'extra' attributes*

*to be sent with your certificate request*

*A challenge password []:*

*An optional company name []:*

Feito isso, enviar o csr para a CA escolhida, ela retornará um arquivo provavelmente por e-mail.

Salve o arquivo dentro de /etc/pki/tls/certs salve o arquivo com o nome do site, por exemplo kennedy-site.crt.

vim /etc/https/conf.d/ssl.conf //edite o arquivo apontando para o certificado crt

*SSLCertificateFile etc/pki/tls/certs/kennedy-site.crt*

ou

touch /etc/httpd/conf.d/kennedy-site.conf //Crie um arquivo .conf e configure o virtualhost

vim /etc/httpd/conf.d/kennedy-site.conf //Edite o arquivo com o exemplo abaixo

*Listen 192.168.0.111:443 //esse endereço é meu servidor virtual*

*<VirtualHost \*:443> //Ouvirá na porta 443*

*ServerName* [*www.kennedy-site.net*](http://www.kennedy-site.net) *//Servidor*

*ServerAlias kennedy-site.net //Nome alternativo*

*ServerAdmin* [*alvkennedy@gmail.com*](mailto:alvkennedy@gmail.com) *//Contato*

*DocumentRoot /home/username/public\_html //Pasta de arquivos html*

*DirectoryIndex index.php index.html \*.html //Procura por esses arquivos caso não seja informado na url*

*SSLEngine On*

*SSLCertificateKeyFile /etc/pki/tls/private/apache-websrv01.key //chave privada*

*SSLCertificateFile /etc/pki/tls/certs/kennedy-site.crt //certificado*

*</VirtualHost>*