

Instalación de certificado SSL/TLS en CentOS

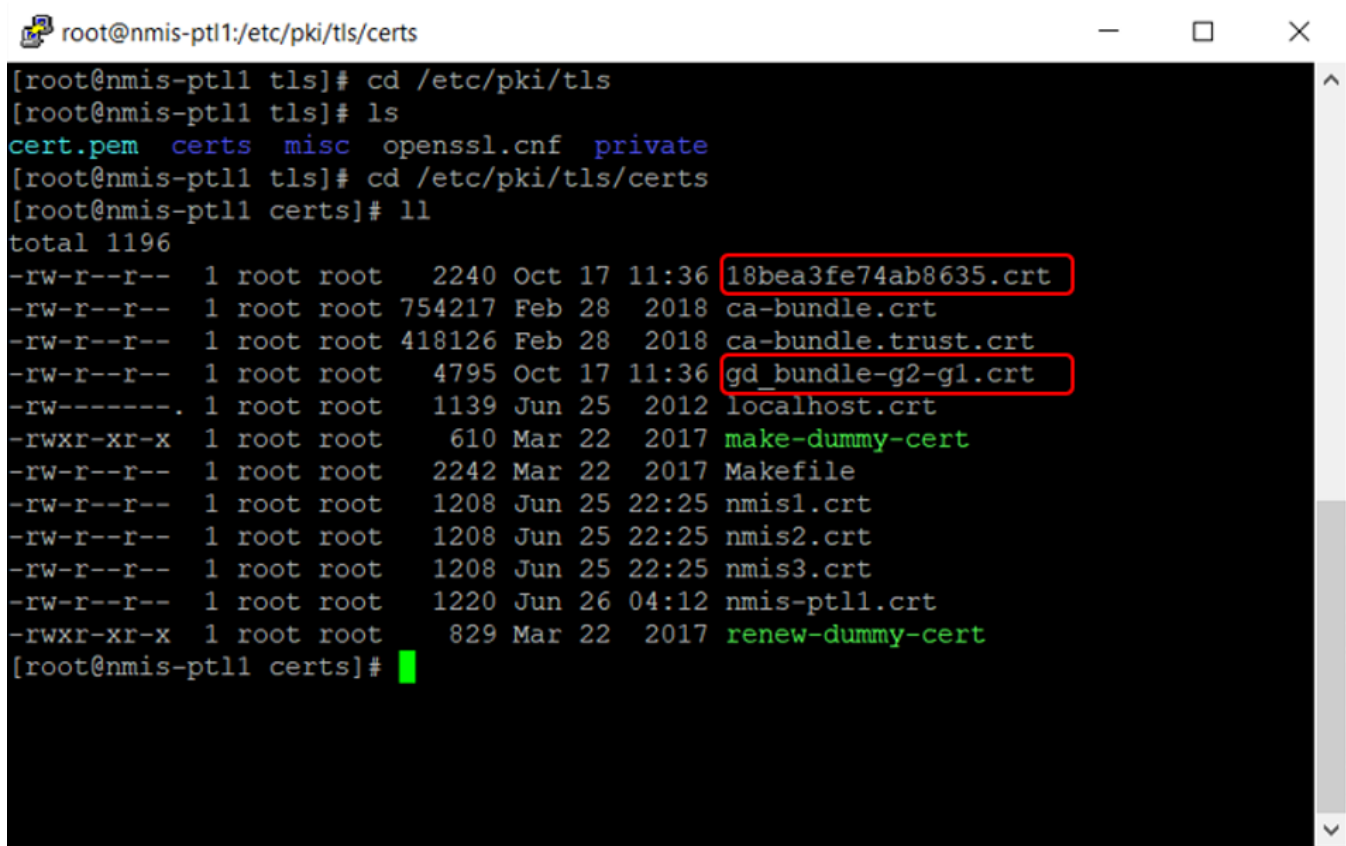
NOTA: Esta configuración se realiza cuando el cliente utiliza un Reverse Proxy.

Copiar los archivos de certificado al servidor OMK

Después de haber obtenido el certificado, tienes que alojar los ficheros CRT y la Clave Privada en el servidor OMK donde desea aplicar el certificado.

Accede a tu servidor y a la ruta `/etc/pki/tls`, donde encontrarás varias carpetas. Por un lado, deberás alojar el certificado de tu dominio en `/etc/pki/tls/certs`. La Clave Privada (y el CSR también lo aconsejamos) en `/etc/pki/tls/private`.

Así es como debería estar `/etc/pki/tls/certs`:

A terminal window titled 'root@nmis-ptl1:/etc/pki/tls/certs' showing the command sequence to list the contents of the directory. The output shows a list of files with their permissions, ownership, size, and timestamps. Two files, '18bea3fe74ab8635.crt' and 'gd_bundle-g2-g1.crt', are highlighted with red boxes.

```
root@nmis-ptl1:/etc/pki/tls/certs
[root@nmis-ptl1 tls]# cd /etc/pki/tls
[root@nmis-ptl1 tls]# ls
cert.pem  certs  misc  openssl.cnf  private
[root@nmis-ptl1 tls]# cd /etc/pki/tls/certs
[root@nmis-ptl1 certs]# ll
total 1196
-rw-r--r--  1 root root   2240 Oct 17 11:36 18bea3fe74ab8635.crt
-rw-r--r--  1 root root 754217 Feb 28 2018 ca-bundle.crt
-rw-r--r--  1 root root 418126 Feb 28 2018 ca-bundle.trust.crt
-rw-r--r--  1 root root   4795 Oct 17 11:36 gd_bundle-g2-g1.crt
-rw-----  1 root root   1139 Jun 25 2012 localhost.crt
-rwxr-xr-x  1 root root    610 Mar 22 2017 make-dummy-cert
-rw-r--r--  1 root root   2242 Mar 22 2017 Makefile
-rw-r--r--  1 root root   1208 Jun 25 22:25 nmis1.crt
-rw-r--r--  1 root root   1208 Jun 25 22:25 nmis2.crt
-rw-r--r--  1 root root   1208 Jun 25 22:25 nmis3.crt
-rw-r--r--  1 root root   1220 Jun 26 04:12 nmis-ptl1.crt
-rwxr-xr-x  1 root root    829 Mar 22 2017 renew-dummy-cert
[root@nmis-ptl1 certs]#
```

Y así `/etc/pki/tls/private`:

```
root@nmis-ptl1:/etc/pki/tls/private
[root@nmis-ptl1 private]# cd /etc/pki/tls/private
[root@nmis-ptl1 private]# ll
total 24
-rw-----. 1 root root 891 Jun 25 2012 localhost.key
-rw----- 1 root root 1679 Oct 17 12:15 nmis1.claro.com.ec.key
-rw----- 1 root root 1704 Jun 25 22:25 nmis1.key
-rw----- 1 root root 1704 Jun 25 22:25 nmis2.key
-rw----- 1 root root 1704 Jun 25 22:25 nmis3.key
-rw----- 1 root root 1704 Jun 26 04:11 nmis-ptl1.key
[root@nmis-ptl1 private]#
```

Configurar el bloque <VirtualHost> para el sitio con SSL

Ahora tendrás que editar el fichero de configuración SSL. Lo encontrarás en `/etc/httpd/conf.d/ssl.conf`.

```
root@nmis-ptl1:/etc/httpd/conf.d
[root@nmis-ptl1 pem]# cd /etc/httpd/conf.d/
[root@nmis-ptl1 conf.d]# ll
total 84
-rw-r--r-- 1 root root 2668 Feb 12 2013 00nmis.conf
-rw-r--r-- 1 root root 2492 Feb 12 2013 01opmantek.conf
-rw-r--r-- 1 root root 2869 Jun 26 04:56 04canidate.conf.OB
-rw-r--r-- 1 root root 2448 Jun 26 16:19 04portal.conf
-rw-r--r-- 1 root root 2448 Jun 26 16:03 04portal.conf.og
-rw-r--r-- 1 root root 8950 Jun 26 09:33 04portal.conf.this
-rw-r--r-- 1 root root 674 Mar 22 2017 php.conf
-rw-r--r-- 1 root root 392 Jun 19 2018 README
-rw-r--r-- 1 root root 1671 Oct 17 12:16 ssl.conf
-rw-r--r-- 1 root root 1582 Oct 16 11:24 ssl.conf.bk16-19-19
-rw-r--r-- 1 root root 1582 Oct 17 11:38 ssl.conf.bk17102019
-rw-r--r-- 1 root root 2573 Jun 25 23:22 ssl.conf.ob
-rw-r--r-- 1 root root 9531 Jun 26 16:03 ssl.conf.og
-rw-r--r-- 1 root root 12104 Jun 26 09:20 ssl.conf.this
-rw-r--r-- 1 root root 299 Feb 19 2018 welcome.conf
[root@nmis-ptl1 conf.d]#
```

Nota: Es importante revisar los permisos de los archivos.

Incorporando lo siguiente con los datos correspondientes

```
<VirtualHost 192.168.0.1:443>
DocumentRoot /var/www/html2
ServerName su.dominio.com
SSLEngine on
SSLCertificateFile /ruta/a/su_dominio.crt
SSLCertificateKeyFile /ruta/a/su_dominio.key
SSLCertificateChainFile /ruta/a/DigiCertCA.crt
</VirtualHost>
```

-----EJEMPLO DE CONFIGURACIÓN-----

NameVirtualHost *:443

```
<VirtualHost *:443>
ServerName monitoreo.nmis.com:443
SSLEngine on
SSLProxyEngine on
ProxyPreserveHost On
SSLCertificateFile /etc/pki/tls/certs/b56f36291nk4.crt
SSLCertificateKeyFile /etc/pki/tls/private/Certificado.key
SSLCertificateChainFile /etc/pki/tls/certs/gd_bundle.crt
</VirtualHost>
```

Ajustar los nombres de archivo para que coincida con los archivos de certificado:

- **SSLCertificateFile** debe ser el archivo del certificado DigiCert (por ejemplo, su_dominio.crt).
- **SSLCertificateKeyFile** debe ser el archivo de claves generadas al crear la CSR.
- **SSLCertificateChainFile** debe ser el archivo intermedio DigiCert certificado (DigiCertCA.crt)

Si la directiva SSLCertificateChainFile no funciona, pruebe a usar la directiva SSLCACertificateFile lugar.

root@nmis-ptl1:/etc/httpd/conf.d

```
LoadModule ssl_module modules/mod_ssl.so
Listen 443
SSLPassPhraseDialog builtin
SSLSessionCache shmcb:/var/cache/mod_ssl/scache(512000)
SSLSessionCacheTimeout 300
SSLMutex default
SSLRandomSeed startup file:/dev/urandom 256
SSLRandomSeed connect builtin
SSLCryptoDevice builtin
SSLProtocol All -SSLv2 -SSLv3
NameVirtualHost *:443

<VirtualHost *:443>
    ServerName nmis1.claro.com.ec:443

    SSLEngine on
    SSLProxyEngine on
    SSLProxyVerify none
    SSLProxyCheckPeerCN off
    SSLProxyCheckPeerExpire off

    ProxyRequests off
    ProxyPreserveHost On
    SSLCertificateFile /etc/pki/tls/certs/18bea3fe74ab8635.crt
    SSLCertificateKeyFile /etc/pki/tls/private/nmis1.claro.com.ec.key
    SSLCertificateChainFile /etc/pki/tls/certs/gd_bundle-g2-g1.crt

    ProxyPass / https://10.57.11.11/
    ProxyPassReverse / https://10.57.11.11/
</VirtualHost>

<VirtualHost *:443>
    ServerName nmis2.claro.com.ec:443

    SSLEngine on
    SSLProxyEngine on
    SSLProxyVerify none
    SSLProxyCheckPeerCN off
    SSLProxyCheckPeerExpire off

    ProxyRequests off
    ProxyPreserveHost On
    SSLCertificateFile /etc/pki/tls/certs/nmis2.crt
    SSLCertificateKeyFile /etc/pki/tls/private/nmis2.key

    ProxyPass / https://10.57.11.51/
    ProxyPassReverse / https://10.57.11.51/
```

Redireccionar dominio a HTTPS

Se modifica el siguiente archivo: `/etc/httpd/conf.d/04omk-proxy.conf` reemplazando "http" por "https" en esta línea: RequestHeader establece X-Forwarded-Proto "http"

```
root@cvtmxomk01:/etc/httpd/conf.d
# if you are using the Opmantek applications behind an ssl-terminating apache vhost,
# then you should adjust the vhost configuration to add this header but with
# protocol "https".
# The Opmantek applications are location- and protocol-independent in almost all
# cases.
RequestHeader set X-Forwarded-Proto "https"
</IfModule>

<Location "/omk">
    ProxyPass http://localhost:8042/omk retry=5
    ProxyPassReverse http://localhost:8042/omk
    ErrorDocument 503 '<html><head><meta http-equiv="refresh" content="60"></head><body><h1>Temporary Service Interruption</h1>The requested OMK page should be back soon. This page will automatically reload in 60 seconds.</body></html>\'
</Location>

# the first location directive only covers /omk and /omk/something,
# not /omk.json
<Location "/omk.json">
    ProxyPass http://localhost:8042/omk.json retry=5
    ProxyPassReverse http://localhost:8042/omk.json
-- INSERT --
```

Probar la configuración de Apache antes de reiniciar

Siempre es mejor para ver sus archivos de configuración de Apache de los errores antes de reiniciar, ya que Apache no se inicia de nuevo si los archivos de configuración tiene errores de sintaxis. Ejecute el siguiente comando: (es apache2ctl en algunos sistemas)

```
service httpd configtest
```

Reiniciar servicio de Apache

```
Service httpd restart
```

Comprobación

Anteriormente al ingresar con el dominio al portal de NMIS, primero aparecía como sitio no seguro



La conexión no es privada

Es posible que los atacantes estén intentando robar tu información de **nmis2.claro.com.ec** (por ejemplo, contraseñas, mensajes o tarjetas de crédito). [Más información](#)

NET::ERR_CERT_AUTHORITY_INVALID

☐ Ayuda a mejorar la Navegación Segura enviando [datos del sistema y contenido de las páginas](#) a Google. [Política de Privacidad](#)

Configuración avanzada

Volver para estar a salvo

Posterior a la implementación del certificado, ingresa directamente como un sitio seguro. Con el icono del candado.



[NMIS8 Dashboard](#)

[NMIS8 Documentation and Community](#)

[Open-Audit V2 Dashboard](#)

[Open-Audit Documentation and Community](#)