

DAW Práctica 2.5: Certificados Nginx en host virtual.

Creamos el directorio ssl en /etc/nginx y generamos la clave privada y el certificado con los comandos:

```
sudo openssl genpkey -algorithm RSA -out
/etc/nginx/ssl/server.key -pkeyopt rsa_keygen_bits:2048
```

```
Mir20220819 [Comando] - Oracle VM VirtualBox
Andrés Molano Ver Entrada Inapropiada Ayuda

usuario@desaweb:/etc/nginx/sbin$

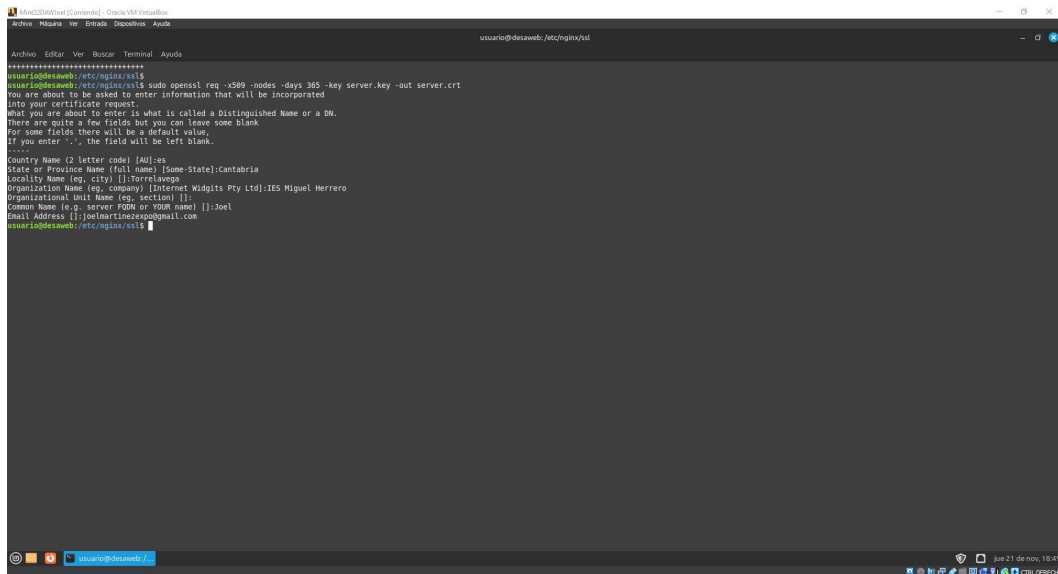
Archivo Editar Ver Buscar Terminal Ayuda

Certificate request self-signature ok
subject = cn = ST = Contralib, o = torrelavega, ou = ies miguel herrero, CN = Joel, emailAddress = joelmarlainez@gmail.com
usuario@desaweb:/etc/apache2/$ cd /
usuario@desaweb:/ $ sudo nano /etc/apache2/sites-available/default-ssl.conf
usuario@desaweb:/ $ sudo systemctl restart apache2
# Enter passphrase for SSL/TLS keys for 327.0.1.1:443 (RSA): ****
usuario@desaweb:/ $ sudo systemctl restart apache2
# Enter passphrase for SSL/TLS keys for 327.0.1.1:443 (RSA): ****
usuario@desaweb:/ $ sudo nano /etc/apache2/sites-available/default-ssl.conf
[sudo] contraseña para usuario:
usuario@desaweb:/ $
usuario@desaweb:/ $ sudo systemctl stop apache2
[sudo] contraseña para usuario:
# Enter passphrase for SSL/TLS keys for fe80::3339:bda5:8c80:2e21:443 (RSA): *****
usuario@desaweb:/ $ sudo systemctl start nginx
usuario@desaweb:/ $ sudo systemctl status nginx
● nginx.service - A high performance web server and a reverse proxy server
   Loaded: loaded (/usr/lib/systemd/system/nginx.service; enabled; preset: enabled)
   Active: active (running) since Thu 2024-11-21 18:43:10 CET; 6s ago
     Docs: man:nginx(8)
    Process: 5511 ExecStartPre=/usr/sbin/nginx -t -q -g daemon on; master process on; (code=exited, status=0/SUCCESS)
    Process: 5512 ExecStart=/usr/sbin/nginx -g daemon on; master process on; (code=exited, status=0/SUCCESS)
   Main PID: 5514 (nginx)
      Tasks: 4 (limit: 11842)
     Memory: 3.1M (peak: 3.4M)
        CPU: 3ms
     CGroup: /system.slice/nginx.service
            └─5514 "nginx: master process /usr/sbin/nginx -g daemon on; master process on;"
               └─5515 "nginx: worker process"
                  └─5516 "nginx: worker process"
                     └─5517 "nginx: worker process"
```

- **genpkey:** Especifica que estamos generando una clave privada.
- **-algorithm RSA:** Indica que queremos usar el algoritmo RSA para generar la clave.
- **-out /etc/nginx/ssl/server.key:** Define el archivo donde se guardará la clave privada.
- **-pkeyopt rsa_keygen_bits:2048:** Configura la longitud de la clave, en este caso, 2048 bits.

Después creamos el certificado con el comando:

```
sudo openssl req -x509 -nodes -days 365 -key
/etc/nginx/ssl/server.key -out /etc/nginx/ssl/server.crt
```



```
usuario@desaweb: /etc/nginx/ssl
=====
usuario@desaweb:/etc/nginx/ssl$ sudo openssl req -x509 -nodes -days 365 -key server.key -out server.crt
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) [AU]:es
State or Province Name (full name) [Some-State]:Cantabria
Locality Name (eg, city) []:Torrelavega
Organization Name (eg, company) [Internet Widdits Pty Ltd]:IES Miguel Herrero
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:joel
Email Address []:joelmartinezcano@gmail.com
usuario@desaweb:/etc/nginx/ssl$
```

Esta configuración no cuenta con passphrase ya que el parámetro `-nodes` desactiva la solicitud de passphrase. Sí en la pagina anterior estaba implementada. La diferencia es que con passphrase la clave privada esta protegida con una contraseña y que sin passphrase no se requiere utilizar contraseña.

- **req:** Genera una solicitud de certificado o un certificado autofirmado.
- **-x509:** Crea un certificado X.509, que es el estándar para certificados digitales.
- **-nodes:** No cifra la clave privada (sin passphrase).
- **-days 365:** Establece la validez del certificado en 365 días.
- **-key:** Especifica la clave privada a utilizar.
- **-out:** Define el archivo donde se guardará el certificado autofirmado.

Editamos el archivo de configuración de nuestro host virtual. Por ejemplo, si el archivo es `/etc/nginx/sites-available/default`.

Una vez hecho confirmamos la correcta sintaxis con `sudo nginx -t` y reiniciamos el servidor.

```
Min22D4Klvel [Comando] - Oracle VM VirtualBox
usuario@desaweb:/etc/nginx/sites-available

Archivo  Editor  Ver  Buscar  Terminal  Ayuda

usuario@desaweb:/etc/nginx/sites$
usuario@desaweb:/etc/nginx/sites$ sudo openssl req -x509 -nodes -days 365 -key server.key -out server.crt
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) [AU]:es
State or Province Name (full name) [Some-State]:Cantabria
Locality Name (eg, city) []:Torrelavega
Organization Name (eg, company) [Internet Widgits Pty Ltd]:IES Miguel Herrero
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:Joel
Email Address []:joelhartinez@gmail.com
usuario@desaweb:/etc/nginx/sites$ cd ..
usuario@desaweb:/etc/nginx$ ls
conf.d  fastcgi.conf  fastcgi_params  koi-utf  koi-win  mime.types  modules-available  modules-enabled  nginx.conf  proxy_params  scgi_params  sites-available  sites-enabled  snippets  ssl  uwsgi_params  win-utf
usuario@desaweb:/etc/nginx$ cd sites-available
usuario@desaweb:/etc/nginx/sites-available$ ls
default  joel
usuario@desaweb:/etc/nginx/sites-available$ sudo nano joel
usuario@desaweb:/etc/nginx/sites-available$ cd ..
usuario@desaweb:/etc/nginx$ ls
conf.d  fastcgi.conf  fastcgi_params  koi-utf  koi-win  mime.types  modules-available  proxy_params  sites-enabled  uwsgi_params
usuario@desaweb:/etc/nginx$ cd sites-available
usuario@desaweb:/etc/nginx/sites-available$ sudo nano joel
usuario@desaweb:/etc/nginx/sites-available$ sudo nginx -t
2024/11/21 18:59:39 [emerg] 5633#5633: directive "ssl_certificate_key" is not terminated by ";" in /etc/nginx/sites-enabled/joel:13
usuario@desaweb:/etc/nginx/sites-available$ sudo nano joel
usuario@desaweb:/etc/nginx/sites-available$ sudo nginx -t
nginx: configuration file /etc/nginx/nginx.conf syntax is ok
nginx: configuration file /etc/nginx/nginx.conf test is successful
usuario@desaweb:/etc/nginx/sites-available$
```

```
Min22D4Klvel [Comando] - Oracle VM VirtualBox
usuario@desaweb:/etc/nginx/sites-available

Archivo  Editor  Ver  Buscar  Terminal  Ayuda

usuario@desaweb:/etc/nginx/sites-available$ sudo nano 7.2
server {
    listen 80;
    listen [::]:80;
    listen 433 ssl;

    root /var/www/html/joel/public.html;
    index index.html index.htm index.nginx-debian.html;
    server_name joel.com www.joel.com;

    ssl_certificate /etc/nginx/ssl/server.crt;
    ssl_certificate_key /etc/nginx/ssl/server.key;
    location / {
        try_files $uri $uri/ =404;
        auth_basic "Zona restringida";
        auth_basic_user_file /etc/nginx/.htpasswd;

        # Página de error 401
        error_page 401 /401.html;

    }

    # Configuración para servir la página de error 401
    location = /401.html {
        root /var/www/html; # Ubicación donde se encuentra 401.html
        internal;
    }

    # Página de error 403 que redirige a 404.html
    error_page 403 /404.html;

    # Configuración para servir la página de error 404
    location = /404.html {
        root /var/www/html; # Ubicación donde se encuentra 404.html
        internal;
    }
}

36 líneas leídas
```

Cuando intentamos acceder al sitio, el navegador mostrará un mensaje de advertencia porque el certificado es autofirmado. Esto ocurre porque los navegadores no confían en certificados que no estén emitidos por una autoridad certificadora (CA) reconocida.



Página de Joel



Después modificaremos el archivo de configuración de nuevo para que nos redirija al https si intentamos acceder a http. Una vez hecho reiniciamos el servicio.

```
server {
    listen 80;
    listen [::]:80;

    root /var/www/html/joel/public_html;
    index index.html index.htm index.nginx-debian.html;
    server_name joel.com www.joel.com;

    return 301 https://$host$request_uri;
}
```

De esta manera si intentamos acceder al sitio web mediante http se nos redirigirá automáticamente al sitio web con https