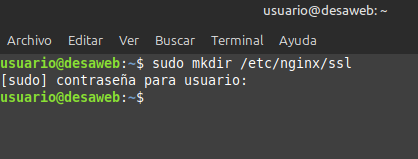
DAW Práctica 2.5: Certificados Nginx en host virtual

**Elabora un documento donde figuren todos los pasos realizados con las pantallas significativas, explicando cada uno de los pasos**.

**Procedimiento:**

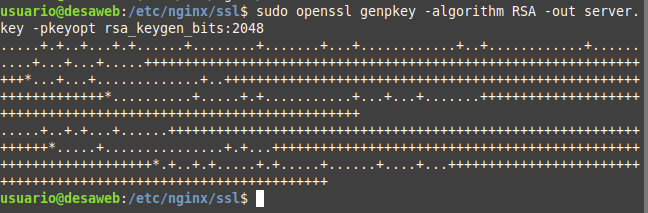
Nginx

1. Creamos un directorio llamado ssl en /etc/nginx



1. Dentro del directorio recientemente creado generamos la clave privada con el cifrado RSA y la longitud 2048 bits. Pedirá introducir el nombre que vamos a generar como clave.

sudo openssl genpkey -algorithm RSA -out server.key -pkeyopt rsa\_keygen\_bits:2048



1. Completa las funcionalidades del anterior comando

***genpkey***

***-algorithm***

***-pkeyopt Numbits (2048)***

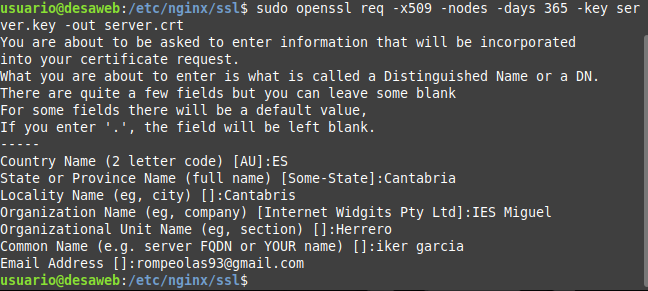
Genpkey es la version de genrsa para generar claves privadas con mayor flexibilidad y control.

-algorithm es el comando para especificar el algoritmo que se va a utilizar en nuestro caso RSA.

-pkeyopt se utiliza para especificar parametros adicionales para generar la clave privada, en este caso el parametro es rsa\_keygen\_bits que sirve para especificar la longitud de la contraseña en bits, respondiendo tambien a esta pregunta Numbits(2048) es lalongitud en bits que tendra nuestra contraseña.

1. Generamos el certificado autofirmado:

sudo openssl req -x509 -nodes -days 365 -key server.key -out server.crt



1. ¿Esta configuración cuenta con passphrase? ¿En la anterior práctica estaba implementada? ¿Qué diferencia hay entre tener o no tener passphrase?

Esta configuración no cuenta con passphrase porque al usar –nodes indicamos que no queremos encriptación, haciendo que no nos pida una contraseña al iniciar, esto simplifica las configuraciones automaticas de nuestro servidor.

Por lo tanto, si lo tuviese, nos pediría la contraseña al iniciar el servidor.

1. Completa las funcionalidades del anterior comando

***req***

***-nodes***

***-days***

***-key***

***-out***

-req: Se utiliza para permitirnos trabajar con solicitudes de certificado, ya sea haciéndolas o procesándolas.

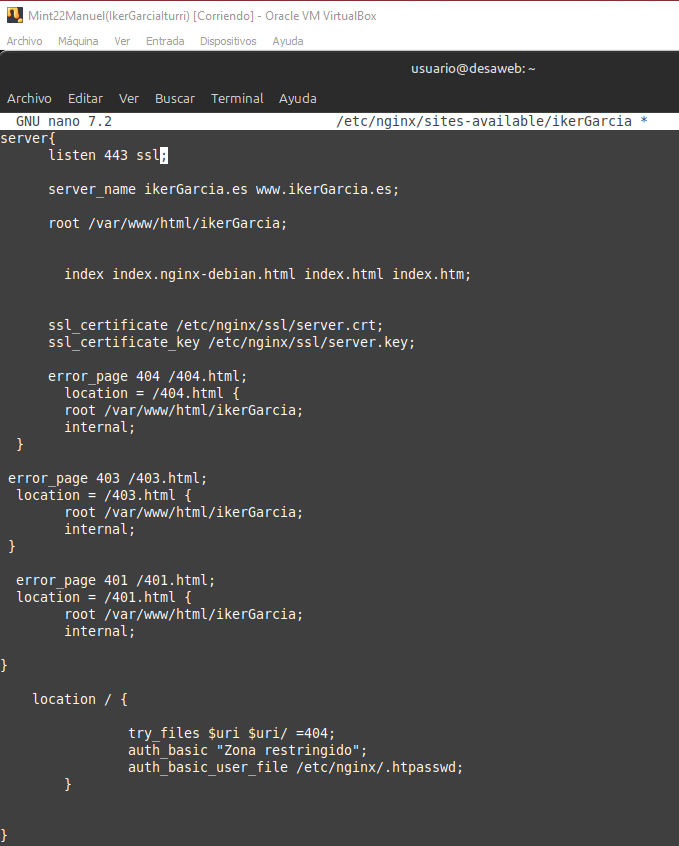
-nodes: Sirve para que la clave privada que generemos no este cifrada, haciendo que al arrancar el servidor no nos pida contraseña, simplificando el proceso.

-days: Especifica el número de días que será válido la auto firma.

-key: sirve para decir cuál será la clave privada que se utiliza en esta operación.

-out:Especifica el archivo donde se guardará el resultado de la operación.

1. Incluir el certificado en Nginx modificando el fichero de configuración de nuestro host vitual. En el fichero de configuración se deberá añadir una nueva configuración de servidor con, al menos, las siguientes características:
   1. SSL escuche por el puerto 443 (listen 443 ssl).
   2. El nombre del servidor.
   3. Raíz desde donde buscará los archivos.
   4. Texto  Descripción generada automáticamenteLa referencia a la clave y a los certificados.
   5. Location / para que busque las url o muestre el error 404 al no encontrarlas.



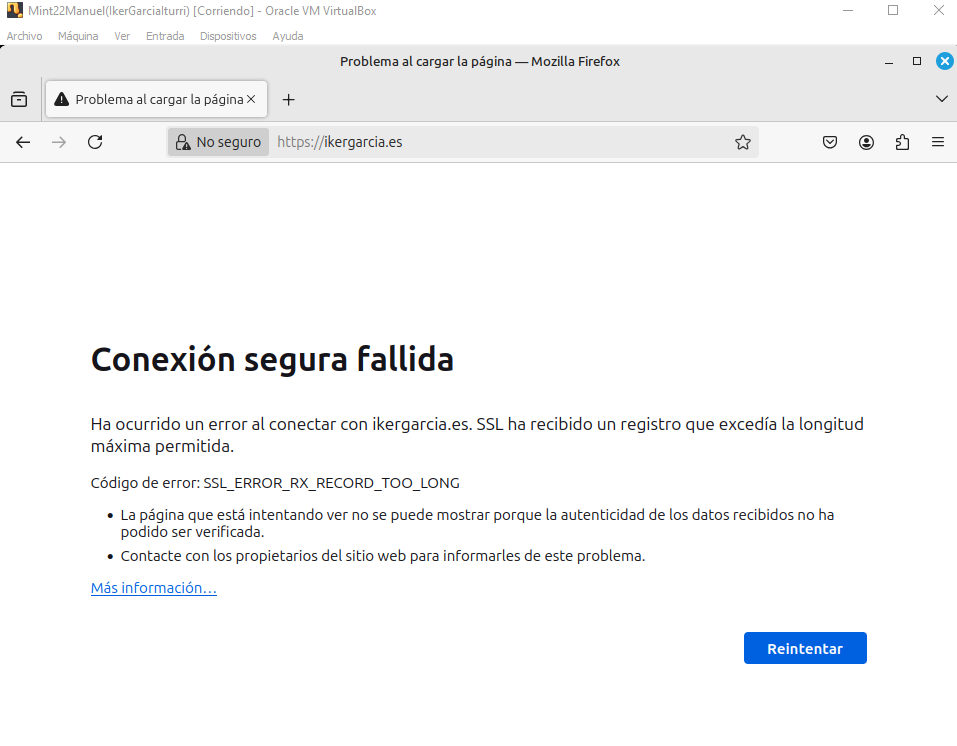
1. Confirmar la correcta sintaxis de los ficheros de configuración.



1. Reiniciar el servicio.

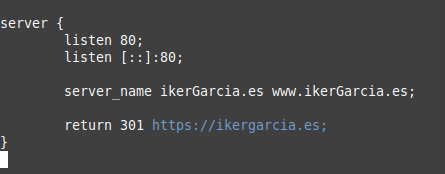


1. ¿Qué aparece al intentar acceder con https? ¿Por qué sucede?

Sucede porque aunque hayamos creado un certificado,no es oficial no esta verificado por una entidad autentica y no sirve.

1. Ahora que se ha implementado https puede ser interesante que se redirija el posible tráfico de http. Para ello, en la parte del puerto 80 del fichero de configuración, si estamos trabajando con Nginx añadimos la siguiente instrucción.





1. Reiniciamos el servicio.



1. Probamos la nueva implementación.

