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



2. 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



3. Completa las funcionalidades del anterior comando

Diagrama

Descripción generada automáticamente

**genpkey** inicia la generación de una clave privada.

**-algorithm** define el tipo de clave (en este caso, RSA).

**-pkeyopt** especifica parámetros adicionales para personalizar la clave.

**rsa\_keygen\_bits** controla el tamaño (seguridad) de la clave

4. Generamos el certificado autofirmado: sudo openssl req -x509 -nodes -days 365 -key server.key -out server.crt 5. ¿Esta configuración cuenta con passphrase? ¿En la anterior práctica estaba implementada? ¿Qué diferencia hay entre tener o no tener passphrase?

Texto

Descripción generada automáticamente

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

No, esta configuración **no utiliza passphrase**, ya que el parámetro -nodes indica explícitamente que la clave privada no estará protegida con una contraseña.

**6. Completa las funcionalidades del anterior comando**

**1 req:** Comienza la generación de un certificado autofirmado.

**2 -x509:** Indica que se genera directamente un certificado, no un CSR.

**3 -nodes:** No cifra la clave privada con una contraseña.

**4 -days 365:** Define que el certificado será válido durante 365 días.

**5 -key:** Usa la clave privada server.key.

**6-out:** Guarda el certificado en el archivo server.crt.

**7. 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:**

Paso 1: Editar el archivo de configuración del host virtual



b. El nombre del servidor.

Interfaz de usuario gráfica, Texto

Descripción generada automáticamente

c. Raíz desde donde buscará los archivos.

d. La referencia a la clave y a los certificados



Texto

Descripción generada automáticamente

Archivo 404

Texto

Descripción generada automáticamente

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

Texto

Descripción generada automáticamente

9. Reiniciar el servicio.



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

11. 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.

12. Reiniciamos el servicio.

13. Probamos la nueva implementación