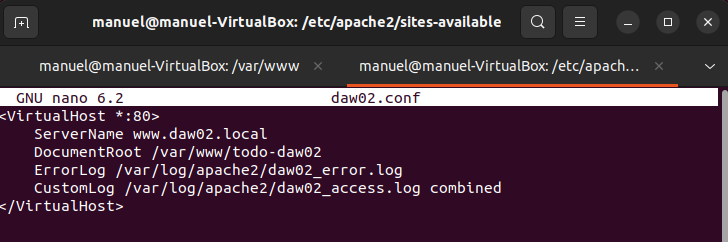
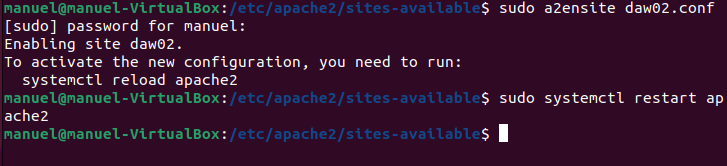


1. Configurar un virtualhost basado en nombre denominado daw02 que permita el acceso de la página web de la empresa en Internet al directorio del servidor web: **todo-daw02.**
2. Hacer accesible a través de Internet las siguientes URL que identifican a la empresa: **www.daw02.local y daw02.local.**

Para crear un nuevo virtualhost, vamos a acceder al directorio **/etc/apache2/sites-available/,** y en dicho directorio vamos a crear el archivo de configuración de nuestro sitio.



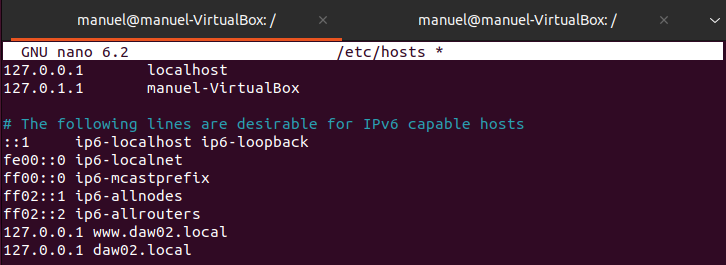
Una vez configurado, vamos a activar el sitio, y a reiniciar apache para que los cambios hagan efecto.



Vamos a crear el directorio al que hemos referenciado en el archivo de configuración como punto de entrada a nuestro sitio.



Ahora, vamos a modificar el archivo **etc/hosts** para hacer accesible nuestra web en local usando la dirección web que nos indica la actividad:



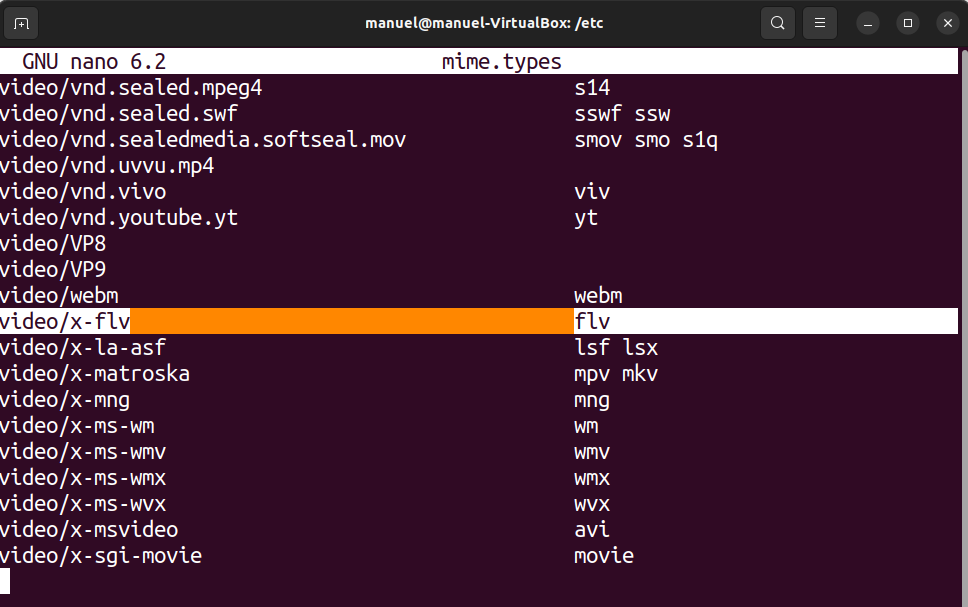
Lo último que nos queda para hacer nuestro sitio accesible es crear un index.html en el directorio que hemos creado para el sitio.

Una vez creado, accediendo a **[http://daw02.local](http://daw02.local,)**[,](http://daw02.local,) podremos visualizar nuestro nuevo sitio.



1. Configurar en el servidor el tipo **MIME** posible que permite la identificación correcta del vídeo presentación formato flv situado dentro del directorio videos y de nombre video.flv.

Para añadir el tipo de vídeo flv a nuestro servidor, vamos a acceder al archivo de configuración de tipos MIME de nuestro servidor, **/etc/mime.types**. Dentro de este fichero, por defecto, ya tenemos añadido el tipo flv.



Una vez tenemos el tipo añadido, vamos a introducir un video en el directorio /var/www/todo-daw02/videos.



Vamos a modificar nuestro html para introducir el video e indicarle el tipo de vídeo que debe de procesar:



Ahora, al acceder a nuestra web, podremos ver el vídeo.



Finalmente, el formato flv muestra ciertas incompatibilidades, por lo que hemos optado por mostrar un vídeo en formato mp4. El proceso exactamente igual que con flv, pero sin la necesidad de modificar el fichero **mime.types**,ya que por defecto es compatible.

1. Crear el subdirectorio todo-daw02/delimitado teniendo en cuenta que:

- El directorio todo-daw02 permite el acceso a cualquier usuario.

- El subdirectorio todo-daw02/delimitado permite el acceso solamente al

personal de la empresa que tenga el rol: admin.

Lo primero que debemos hacer es crear el directorio “delimitado” dentro de todo-daw02.



Ahora, debemos asignar permisos a cada directorio, para que al directorio todo-daw02 pueda acceder cualquier usuario, y al directorio delimitado solo puedan acceder usuarios con el rol admin.

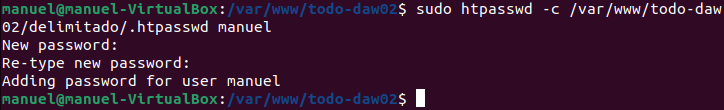


Con chmod 777 damos permisos de lectura y escritura a cualquier usuario sobre el directorio todo-daw02.

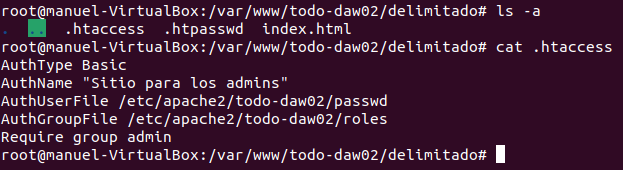


Con chmod 700 damos permisos únicamente a los usuarios con el mismo rol que el creador del archivo, es decir, usuarios con el rol admin.

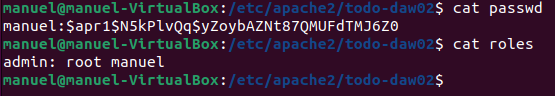
Vamos a configurar un sistema de autenticación. Para ello, vamos a crear el archivo .htpasswd, agregando un usuario y una contraseña mediante el siguiente comando:



Ahora vamos a crear el fichero .htaccess para definir el acceso al directorio “delimitado”.

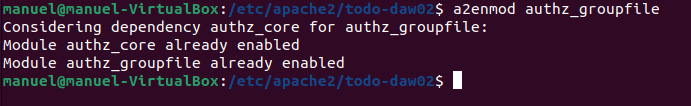


Vamos a crear los ficheros “passwd” y “roles”, a los que referenciamos desde el archivo de configuración “.htaccess”.



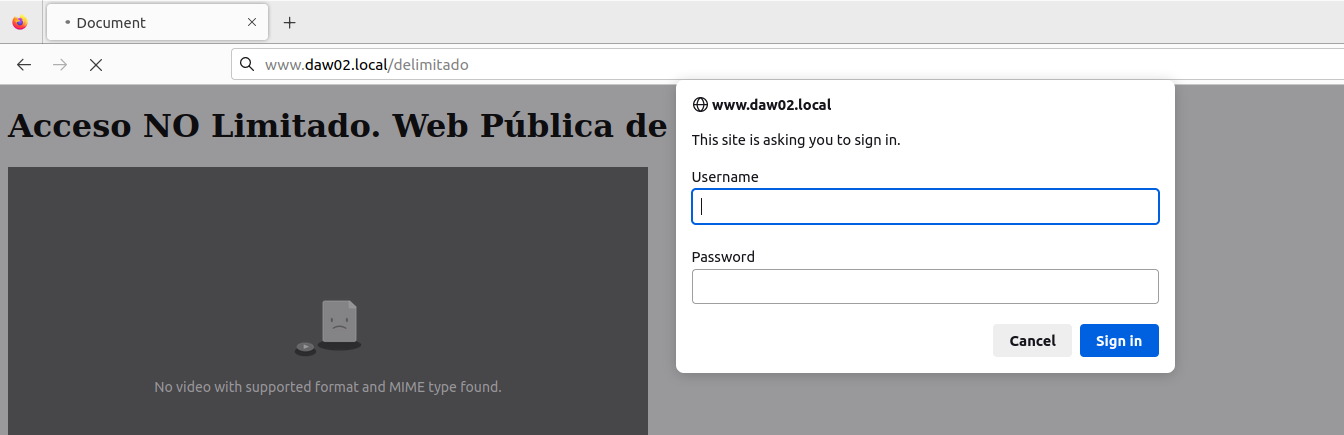
En el archivo “passwd” tenemos la contraseña establecida cifrada. Para establecerla, usamos el comando **htpasswd -c /etc/apache2/todo-daw02 miusuario**.

Por último, tenemos que habilitar el módulo **authz\_groupfile** con el comando **a2enmod**, el cual nos permite habilitar módulos de apache2. Este módulo nos va a habilitar el funcionamiento de la autenticación basada en grupos en apache2.



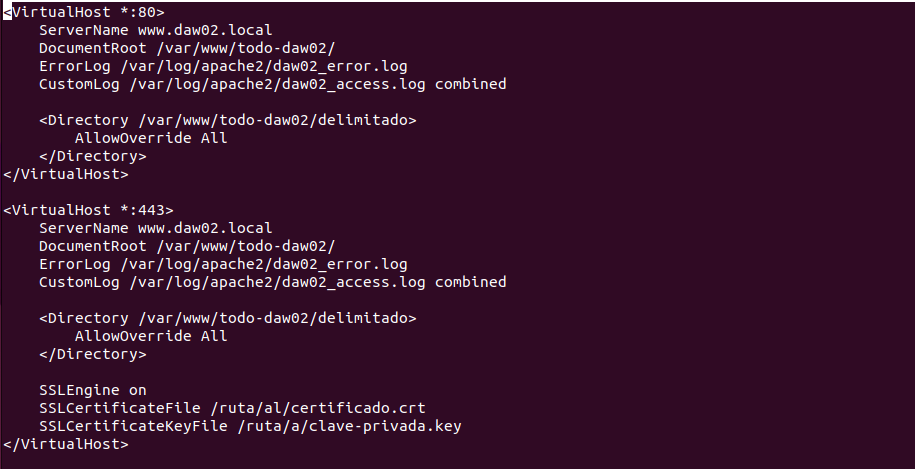
Ya los había habilitado previamente, por eso aparecen como already enabled.

Una vez tenemos hechas todas nuestras configuraciones, al intentar acceder a la sección “delimitado” desde nuestro navegador, el servidor nos mostrará un login para identificar que somos un usuario administrador. Si este login no resulta exitoso, no se nos mostrará la sección “delimitado”.



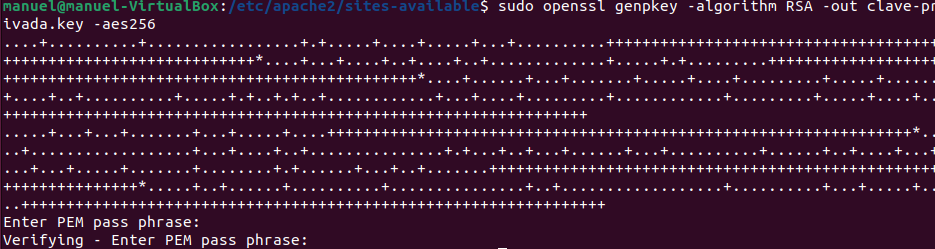
1. Permitir el protocolo HTTPS en el virtualhost daw02 y comprobar que funciona.

Para habilitar el protocolo https en un servidor web Apache, es necesario configurar el servidor para permitir el acceso mediante SSL/TLS. Para ello, vamos a modificar el archivo de configuración **/etc/apache2/sites-available/daw02.conf**.

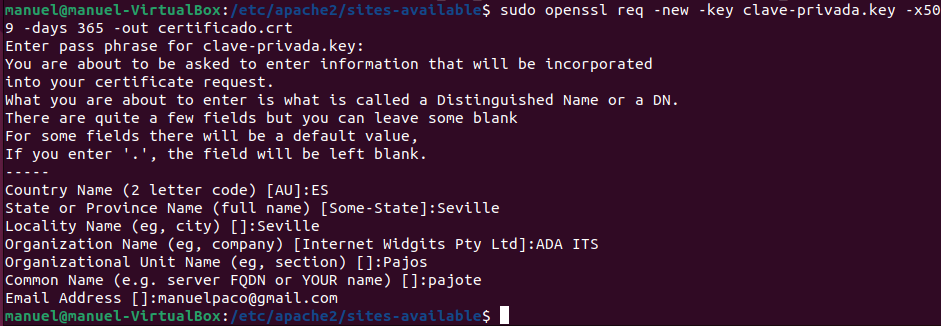


Al final del archivo de configuración vemos que nos pide un certificado ssl y una clave de acceso privada. Vamos a generarlos y a modificar el archivo con las rutas reales en nuestro equipo.

Primero vamos a generar la clave de acceso privada, la cual nos pedirá una contraseña de seguridad.



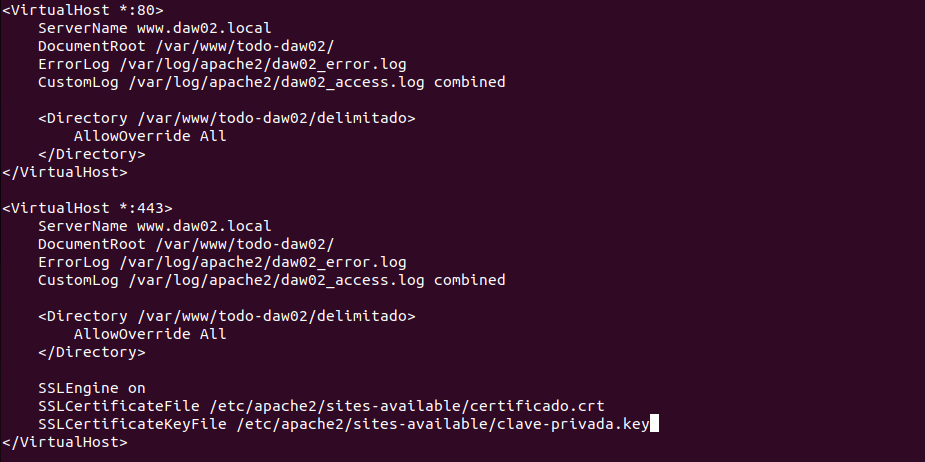
Ahora, vamos a generar el certificado:



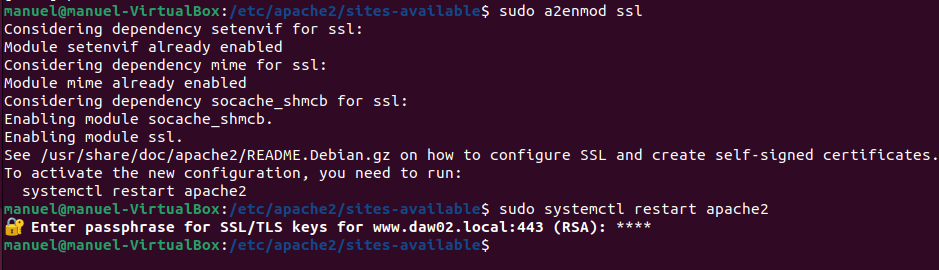
Si no indicamos ninguna ruta en el comando, el certificado y la clave de acceso se crearán en la ruta donde los ejecutemos, en mi caso **/etc/apache2/sites-available**.

Existen directorios predefinidos para almacenar este tipo de ficheros, para certificados **/etc/ssl/certs/** y para las claves de acceso **/etc/ssl/private/**. En estos directorios es donde deberían ser almacenadas.

Una vez ya tenemos todo creado, vamos a modificar el fichero de configuración para referenciar las rutas de acceso a los ficheros.



Vamos a activar el módulo ssl en Apache. Una vez instalado, vamos a reiniciar el servicio apache2.



En el reinicio nos pide la contraseña de acceso a nuestra clave privada.

Ahora, al tratar de acceder a **<https://www.daw02.local>** podemos ver con éxito nuestro sitio web.



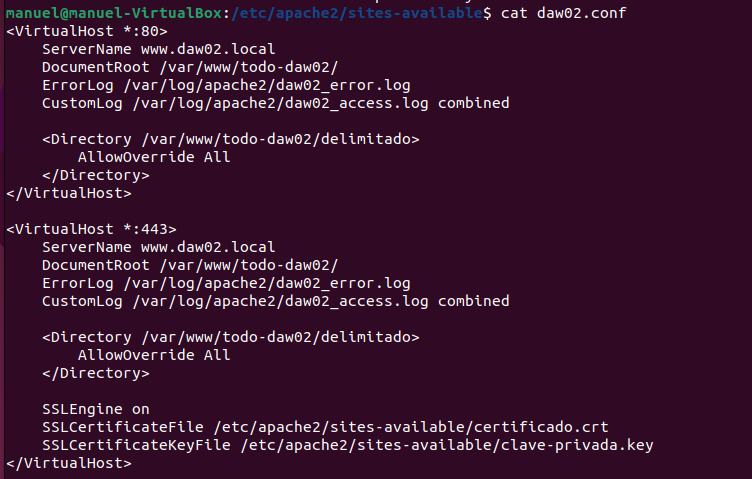
1. Configurar los archivos de registro como sigue:

 - Identificación log de acceso: daw02-access.log

- Identificación log de error: daw02-error.log

 - Alias logformat: combined

Para configurar los logs tal y como se nos pide, vamos a modificar el archivo de configuración **/etc/apache2/sites-available/daw02.conf**.

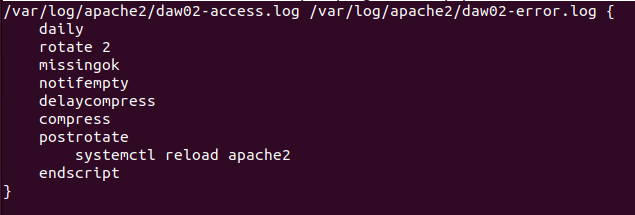


Como vemos, en las reglas “ErrorLog” y “CustomLog” definimos los ficheros donde queremos registrar lo ocurrido. Estos ficheros vamos a crearlos dentro de nuestro sitio de apache, **/etc/apache2/sites-available/daw02.conf**.

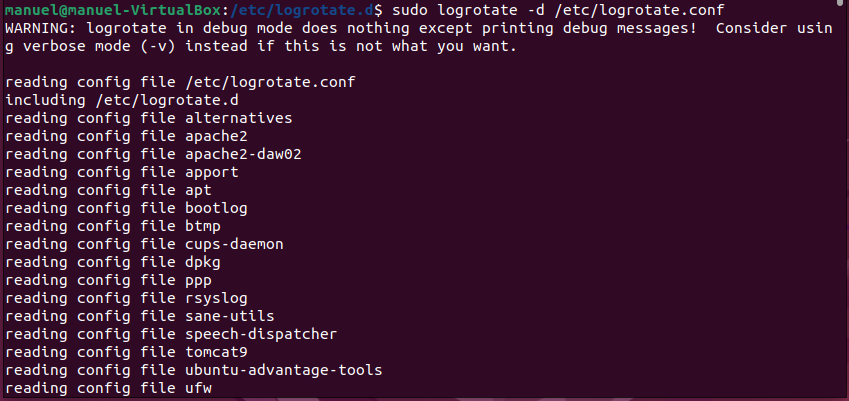
1. Rotar logs por intervalo temporal: cada 48 horas.

Para configurar que los logs roten cada 48 horas, vamos a crear un fichero de configuración **logrotate** en **etc/logrotate.d/**, donde vamos a introducir la configuración necesaria.





Una vez hemos introducido la configuración, vamos a ejecutar el comando **sudo logrotate -d /etc/logrotate.conf**. Este comando verificará la configuración y mostrará errores si los hay.



Podemos ver que el comando ha leído nuestro archivo de configuración y no ha mostrado ningun error en él.

Por último, vamos a ejecutar el comando **sudo logrotate -f /etc/logrotate.conf** para forzar la rotación de registros o logs, que también nos devolverá errores en caso de que la configuración no sea correcta.



Nuevamente, no obtenemos ningún error. Nuestra configuración funciona correctamente.