DESARROLLO DE APLICACIONES WEB

10-11-2023

ROBERTO RODRÍGUEZ JIMÉNEZ

roberto.rodjim.1@educa.jcyl.es

Despliegue de aplicaciones Web

Configuración y administración de servidores web

Tarea 02

Contenido

[Tarea online DAW01 2](#_Toc150539519)

[Enunciado 2](#_Toc150539520)

[Caso práctico 2](#_Toc150539521)

[¿Qué te pedimos que hagas? 2](#_Toc150539522)

[Recursos necesarios y recomendaciones 3](#_Toc150539523)

[Recursos necesarios 3](#_Toc150539524)

[Recomendaciones 3](#_Toc150539525)

[Evaluación de la tarea 4](#_Toc150539526)

[Criterios de evaluación implicados 4](#_Toc150539527)

[¿Cómo valoramos y puntuamos tu tarea? 4](#_Toc150539528)

[Respuestas 5](#_Toc150539529)

[1. Configurar un virtualhost basado en nombre denominado empresa-tarea-daw02 que permita el acceso de la página web de la empresa en Internet al directorio del servidor web: todo-empresa-tarea-daw02 5](#_Toc150539530)

[2. Hacer accesible a través de Internet las siguientes URL que identifican a la empresa: www.empresa-tarea-daw02.local y empresa-tarea-daw02.local 8](#_Toc150539531)

[3. Configurar en el servidor el tipo MIME posible que permite la identificación correcta del vídeo de presentación formato flv situado dentro del directorio videos y de nombre entrada.flv. 9](#_Toc150539532)

[4. Crear el subdirectorio todo-empresa-tarea-daw02/delimitado teniendo en cuenta que: 10](#_Toc150539533)

[5. Permitir el protocolo HTTPS en el virtual host empresa-tarea-daw02 14](#_Toc150539534)

[6. Configurar los archivos de registro como sigue: 17](#_Toc150539535)

[7. Rotar logs por intervalo temporal: cada 24horas. 18](#_Toc150539536)

[Código 19](#_Toc150539537)

# Tarea online DAW01

**Título de la tarea:** Configuración de un servidor Apache  
**Unidad:** 2  
**Ciclo formativo y módulo:** Desarrollo de Aplicaciones Web - Despliegue de Aplicaciones Web  
**Curso académico:** 2021/2022

## Enunciado

### Caso práctico

En BK programación le han encargado a María que comience con un proyecto para una empresa que quiere mostrar y operar con su negocio a través de Internet. De esta forma, el cliente quiere:

* Una página web visible a cualquiera en Internet que publicite su negocio: quienes somos -que contiene una vídeo presentación de la empresa en formato flv-, clientes habituales, donde estamos, novedades.
* Un lugar de la página web solamente accesible al personal de la empresa que tenga el rol 'admin'.
* Asegurar la comunicación del personal de la empresa.

### ¿Qué te pedimos que hagas?

Se pide en un servidor web Apache (apache2):

1. Configurar un virtualhost basado en nombre denominado empresa-tarea-daw02 que permita el acceso de la página web de la empresa en Internet al directorio del servidor web: todo-empresa-tarea-daw02
2. Hacer accesible a través de Internet las siguientes URL que identifican a la empresa:  
   www.empresa-tarea-daw02.local y empresa-tarea-daw02.local
3. 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 entrada.flv.
4. Crear el subdirectorio todo-empresa-tarea-daw02/delimitado teniendo en cuenta que:
   1. El directorio todo-empresa-tarea-daw02 permite el acceso a cualquier usuario.
   2. El subdirectorio todo-empresa-tarea-daw02/delimitado permite el acceso solamente al personal de la empresa que tenga el rol: admin.
5. Pemitir el protocolo HTTPS en el virtualhost empresa-tarea-daw02
6. Configurar los archivos de registro como sigue:
   1. Identificación log de acceso: empresa-tarea-daw02-access.log
   2. Identificación log de error: empresa-tarea-daw02-error.log
   3. Alias logformat: combined
7. Rotar logs por intervalo temporal: cada 24horas.

NOTAS IMPORTANTES:

* Los dominios .local no existen en Internet, con lo cual la tarea se comprobará en red local. Así para que las URL fuesen visibles en Internet realmente habría que comprar el dominio, dirigirlo a la IP del servidor web y expandirlo mediante Servidores DNS.
* Para la solución de la tarea simular la página web con dos archivos HTML:
  + Uno de nombre index.html en la raiz del directorio todo-empresa-tarea-daw02 que contenga el texto 'ACCESO NO LIMITADO'.
  + Uno de nombre index.html en la raiz del directorio todo-empresa-tarea-daw02/delimitado que contenga el texto 'ACCESO LIMITADO'.
* La entrega de cada apartado de la tarea consiste en indicar el archivo a configurar junto con el código necesario para resolver la cuestión correspondiente.

**NOTA IMPORTANTE**

**Para el apartado 3 es necesario entregar las capturas de pantalla de los principales pasos realizados, explicando el proceso seguido en cada uno de ellos. Las capturas de pantalla realizadas deben tener como fondo de pantalla la plataforma con tu usuario mostrando claramente la foto de tu perfil. Aquellos apartados/subapartados que no cumplan esta condición no serán corregidos.**

## Recursos necesarios y recomendaciones

### Recursos necesarios

* Los contenidos de la unidad.
* Un servidor web Apache2 instalado.
* Un navegador para comprobar la realización de la tarea.
* Un procesador de textos para elaborar la documentación y los archivos de la tarea.
* Un ordenador.
* Acceso a Internet.

### 

### Recomendaciones

Ve realizando la tarea de forma secuenciada y al mismo tiempo ve documentando la solución de la misma.

Aunque existen varias posibilidades para controlar el acceso a los usuarios, te recomiendo que comienzes a trabajar con la autenticación HTTP Basic. Una vez configurada puedes intentarlo mediante autenticación LDAP.

Te ayudará mucho saber que está pasando en cada momento en tu servidor web, así puedes comprobar en tiempo real que es lo que ocurre en el acceso a los directorios todo-empresa-tarea-daw02 y todo-empresa-tarea-daw02/delimitado mediante el comando:

**tail -f fichero.log**

donde fichero.log identifica el nombre del fichero de registro a comprobar.

## Evaluación de la tarea

### Criterios de evaluación implicados

1. Se han reconocido los parámetros de administración más importantes del servidor Web.
2. Se ha ampliado la funcionalidad del servidor mediante la activación y configuración de módulos.
3. Se han creado y configurado sitios virtuales.
4. Se han configurado los mecanismos de autenticación y control de acceso del servidor.
5. Se han obtenido e instalado certificados digitales.
6. Se han establecido mecanismos para asegurar las comunicaciones entre el cliente y el servidor.
7. Se han realizado los ajustes necesarios para la implantación de aplicaciones en el servidor Web.
8. Se ha elaborado documentación relativa a la configuración, administración segura y recomendaciones de uso del servidor.

### ¿Cómo valoramos y puntuamos tu tarea?

|  |  |
| --- | --- |
| **Rúbrica de la tarea** | |
| **Apartado 1:** Configurar un virtualhost basado en nombre | 1 punto |
| **Apartado 2:** Hacer accesible a través de Internet las URLs de la empresa. | 1 punto |
| **Apartado 3:**Configurar en el servidor el tipo MIME. | 1 punto |
| **Apartado 4:**Crear el subdirectorio. | 2 puntos |
| **Apartado 5: P**emitir el protocolo HTTPS en el virtualhost. | 3 puntos |
| **Apartado 6:**Configurar los archivos de registro. | 1 punto |
| **Apartado 7:**Rotar logs. | 1 punto |

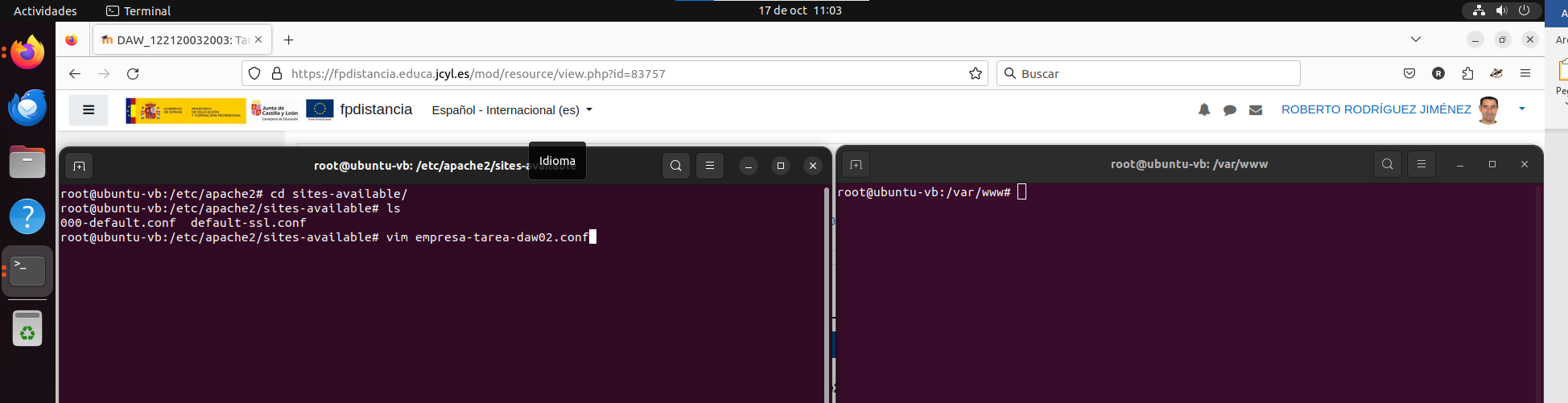
**NOTA IMPORTANTE**

**Aquellos apartados/subapartados en los que las capturas de pantalla no sean claras o no tengan como fondo de pantalla la plataforma con tu usuario mostrando claramente la foto de tu perfil, no serán corregidos.**

## Respuestas

### Configurar un virtualhost basado en nombre denominado empresa-tarea-daw02 que permita el acceso de la página web de la empresa en Internet al directorio del servidor web: todo-empresa-tarea-daw02

Creamos el archivo de configuración empresa-tarea-daw02 para el servidor en /etc/apche2/sites-available.

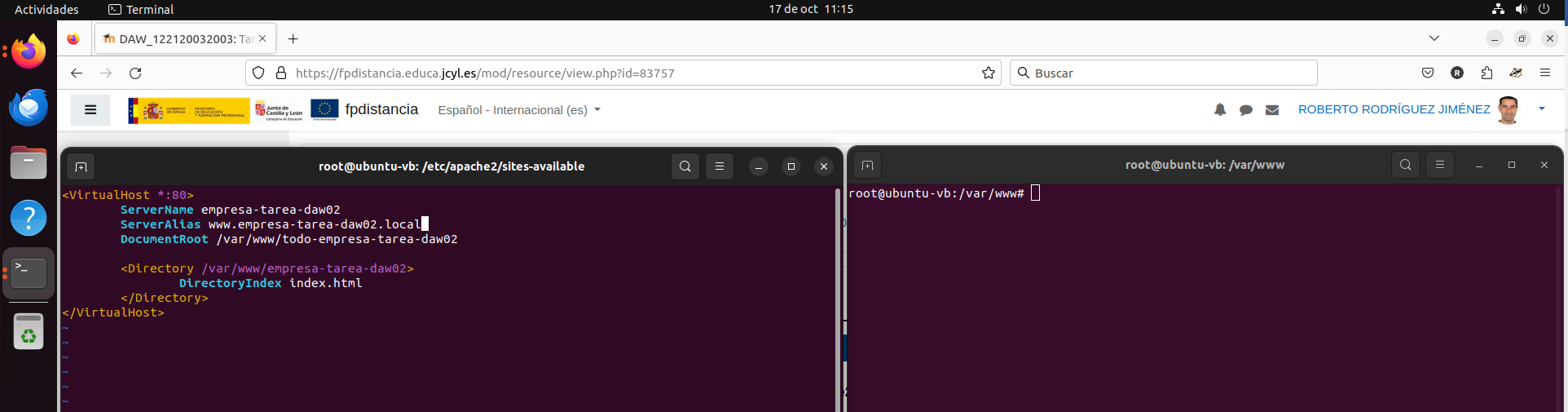


Configuramos el archivo empresa-tarea-daw02 con *vim*

* ServerName: empresa-tarea-daw02
* ServerAlias: [www.empresa-tarea-daw02.local](http://www.empresa-tarea-daw02.local)
* DocumentRoot: /var/www/todo-empresa-tarea-daw02

Especificamos el documento por defecto en la directiva *Directory* para el directorio del host:

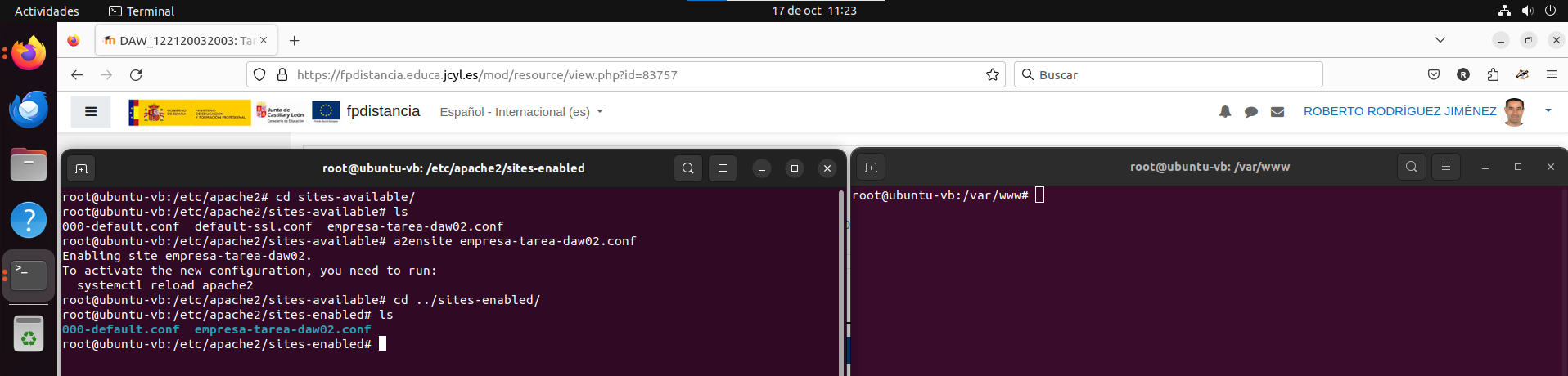
* DirectoryIndex: index.html



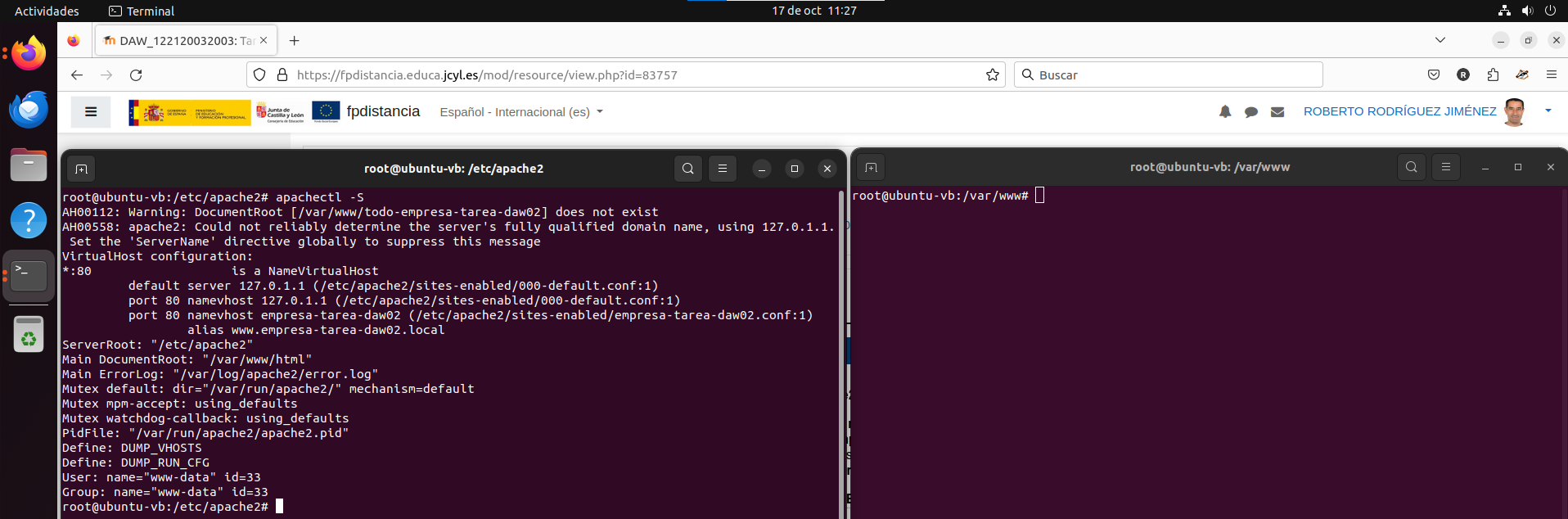
El directorio correcto es  
todo-empresa-tarea-daw02

Habilitamos el host con a2ensite

cd sites-available  
a2ensite empresa-tarea-daw02



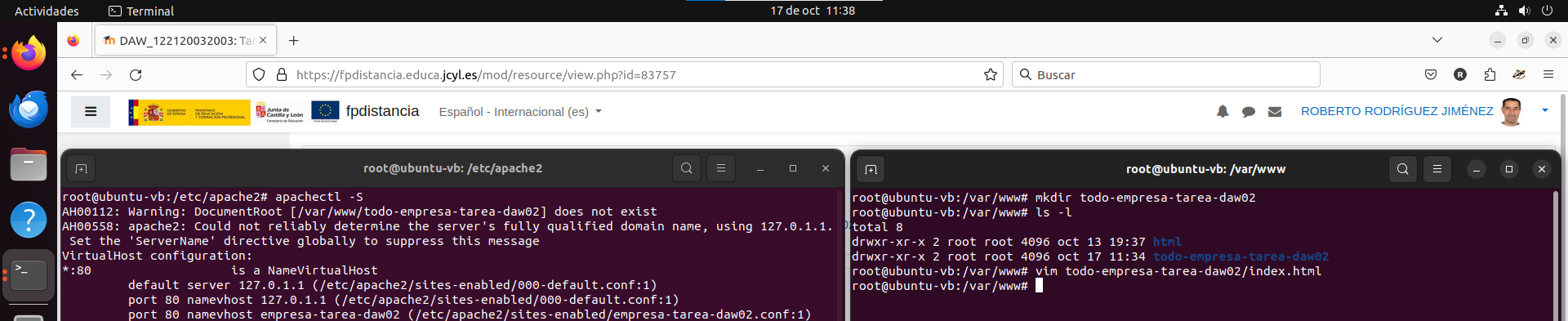
Podemos ver que el servidor ya está creado con apachectl -S

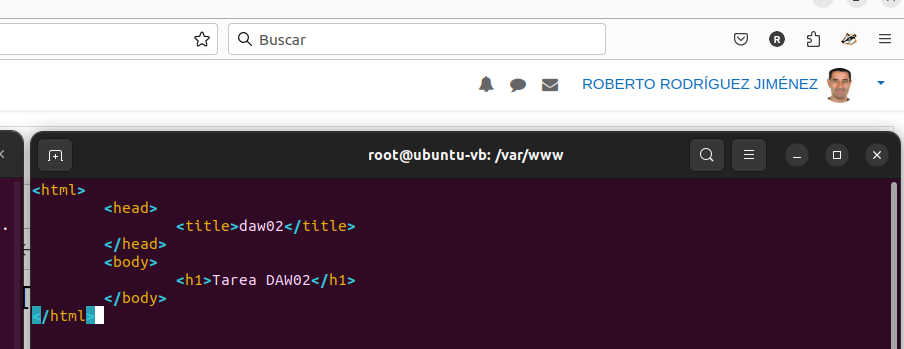


Creamos el directorio y la página index.html en el directorio /var/www

En index.html simplemente ponemos un título un h1

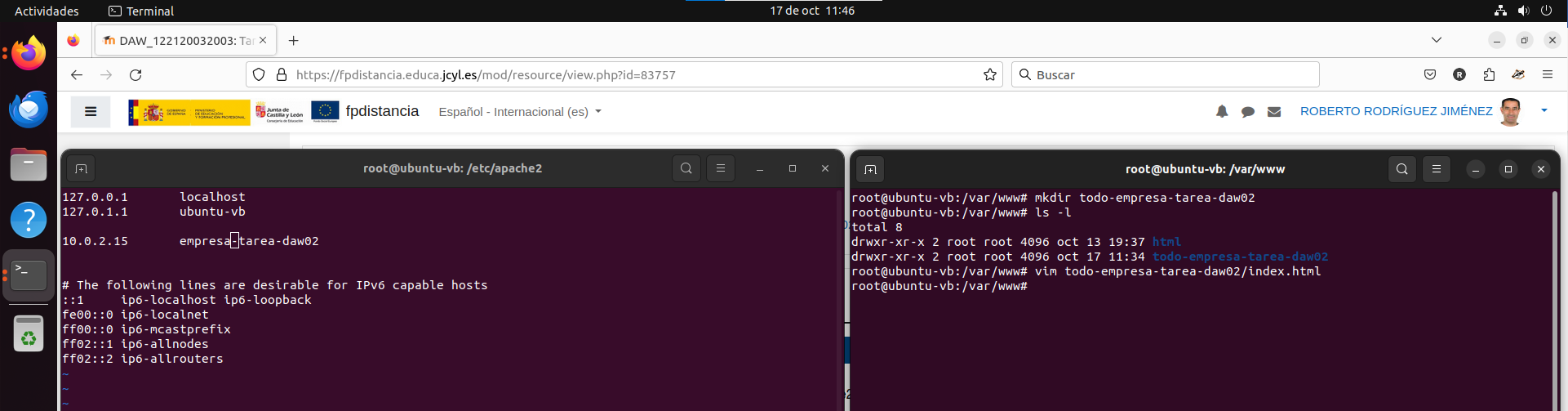
mkdir todo-empresa-tarea-daw02  
vim todo-empresa-tarea-daw02/index.html



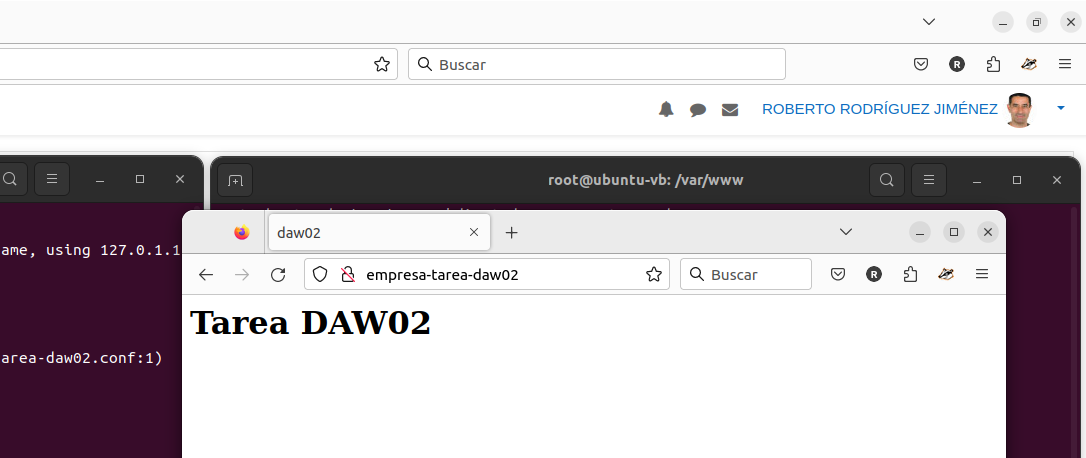


Añadimos la IP al archivo /etc/hosts para que se pueda acceder al host mediante el nombre del servidor.  
Al igual que *localhost* apunta a 127.0.0.1, *empresa-tarea-daw02* lo hace a 10.0.2.15  
*localhost* es el nombre del servidor por defecto de apache y su archivo de configuración en *000-default.conf*.

10.0.2.15 empresa-tarea-daw02

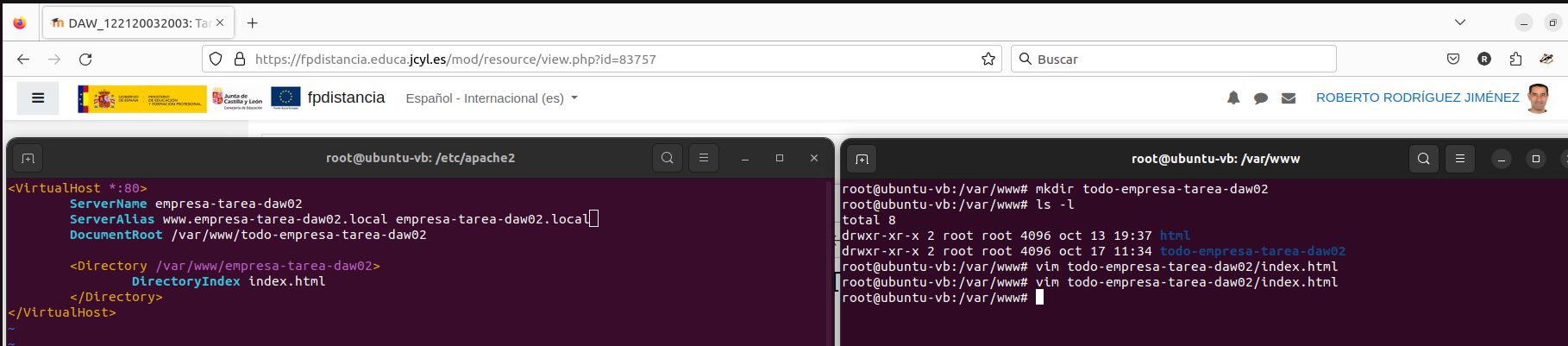


Vemos el resultado

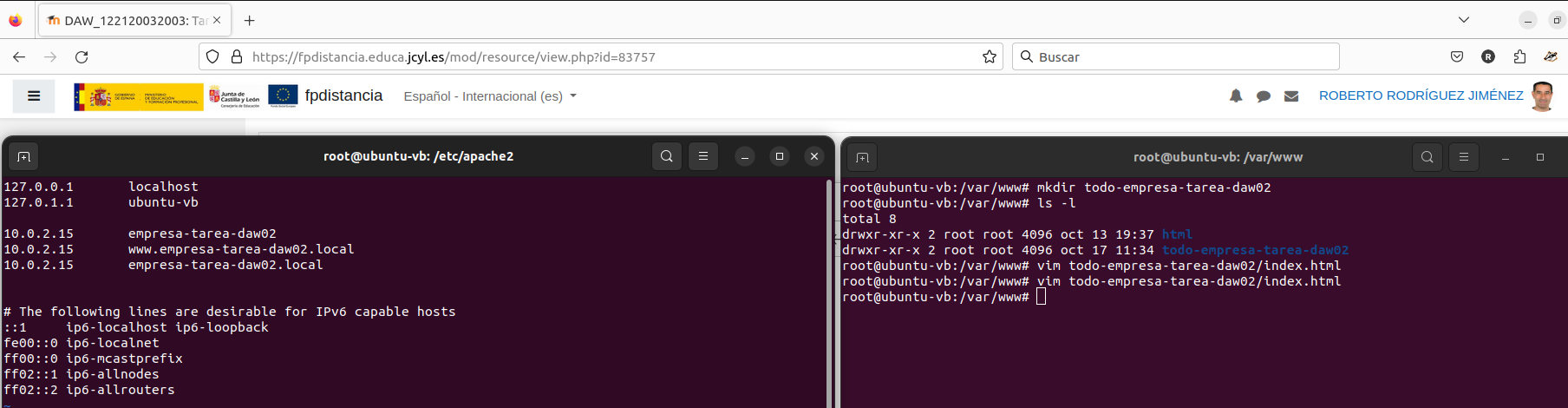


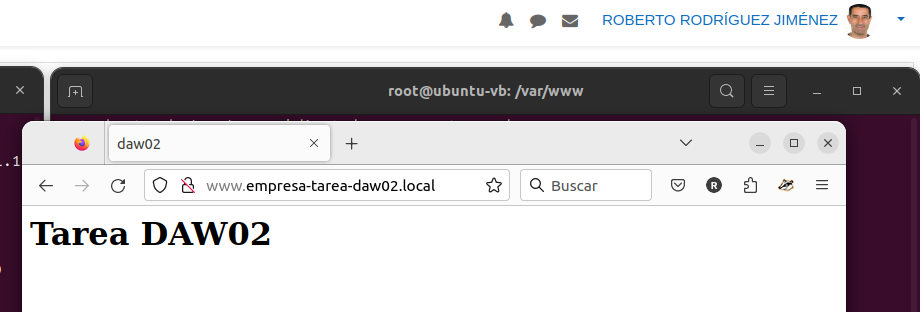
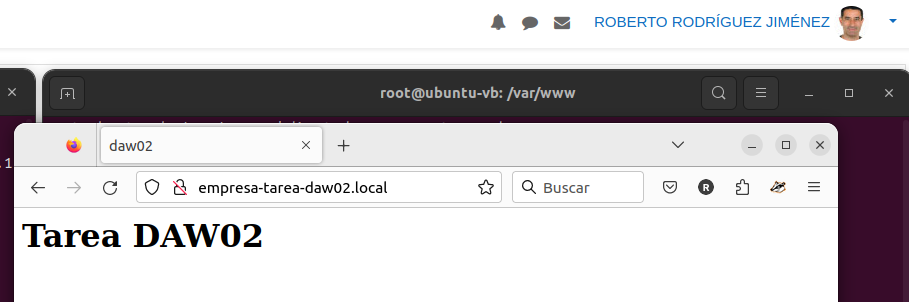
### Hacer accesible a través de Internet las siguientes URL que identifican a la empresa: www.empresa-tarea-daw02.local y empresa-tarea-daw02.local

Configuramos los alias en el archivo de configuración y le añadimos todo-empresa-tarea-daw02.local



En el archivo *hosts* añadimos los nuevos dominios

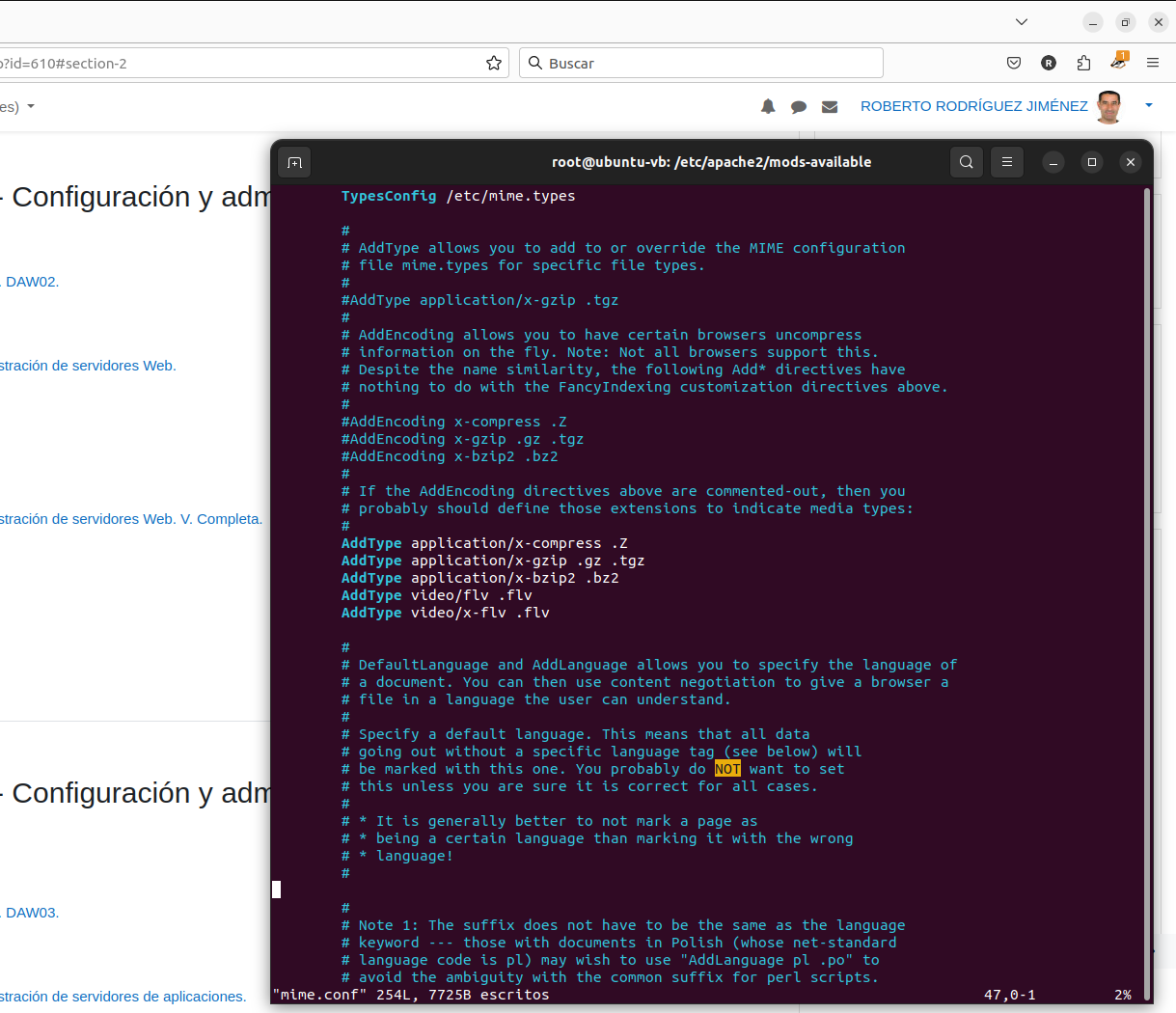


### Configurar en el servidor el tipo MIME posible que permite la identificación correcta del vídeo de presentación formato flv situado dentro del directorio videos y de nombre entrada.flv.

Aunque el temario dice que se debe añadir la directiva *DefaultType*, esta está obsoleta.  
Para hacer que se reconozca una aplicación por su extensión (cosa que con flv no va a funcionar) se añade el tipo en el fichero /etc/apache2/mods-available/mime.conf

AddType video/flv .flv  
AddType video/x-flv .flv

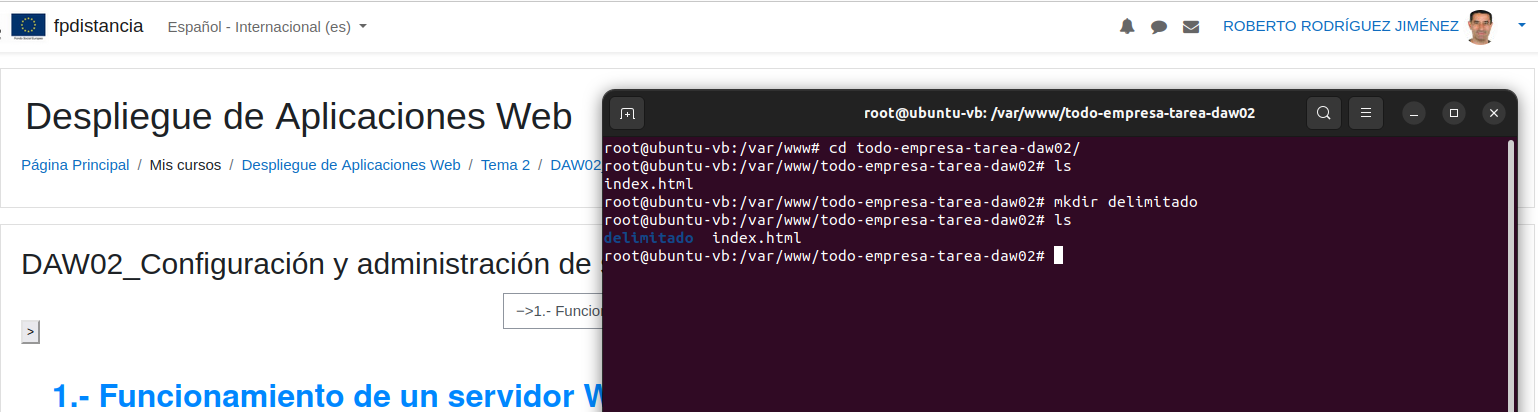


### Crear el subdirectorio todo-empresa-tarea-daw02/delimitado teniendo en cuenta que:

1. El directorio todo-empresa-tarea-daw02 permite el acceso a cualquier usuario.
2. El subdirectorio todo-empresa-tarea-daw02/delimitado permite el acceso solamente al personal de la empresa que tenga el rol: admin.

Creamos el subdirectorio dentro de todo-empresa-tarea-daw02

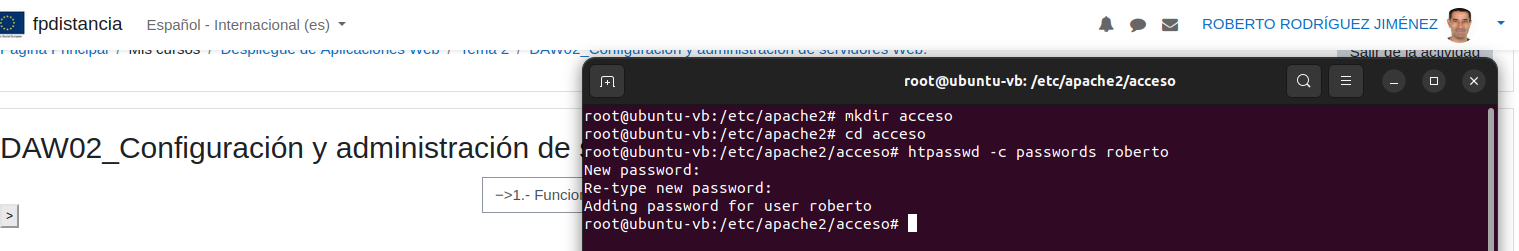
mkdir delimitado



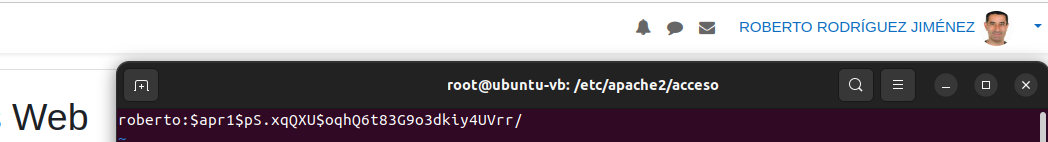
Vamos a restringir el acceso a */delimitado* mediante el archivo .htaccess que crearemos dentro del directorio.

Necesitamos un archivo para guardar las contraseñas:

* Fichero de texto guardado en un lugar inaccesible desde la web.
* Creamos un directorio en */etc/apache2* llamado *acceso* y en él archivo passwords.
* Ahora creamos en passwd el archivo con un usuario *admin*.   
  El parámetro -c introduce al crear el archivo.  
  htpasswd -c passwords roberto



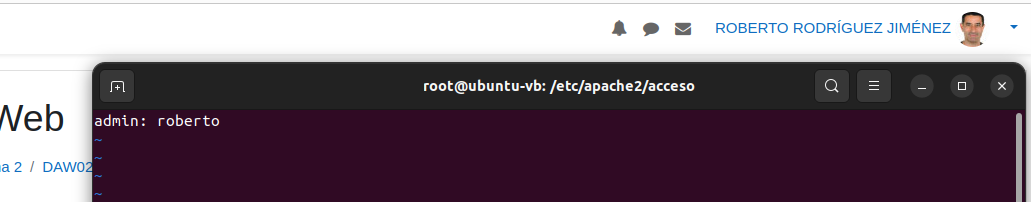
Contenido del fichero *passwords* con el usuario *roberto*

**

Hacemos lo mismo para especificar los roles: creamos un archivo llamado *grupos* en el directorio */etc/apache2/acceso*.  
Dentro del fichero especificamos el nombre del rol y los usuarios asociados.

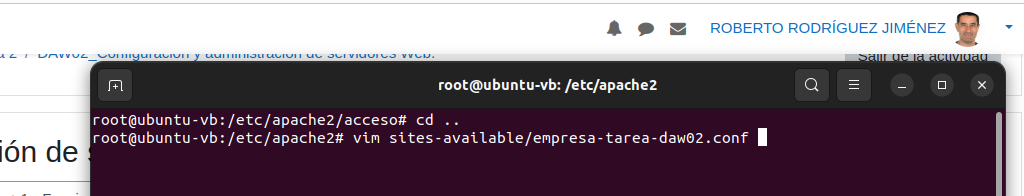
vim groups

Contenido del fichero *acceso/grupos*



Ya tenemos un usuario y el rol al que pertenece.  
Ahora debemos configurara el archivo .htaccess en el directorio que queremos proteger, pero antes debemos permitir poner directivas de autenticación en el archivo.

Para ello editamos el archivo de configuración del host virtual y añadimos la directiva AllowOverride AuthConfig.

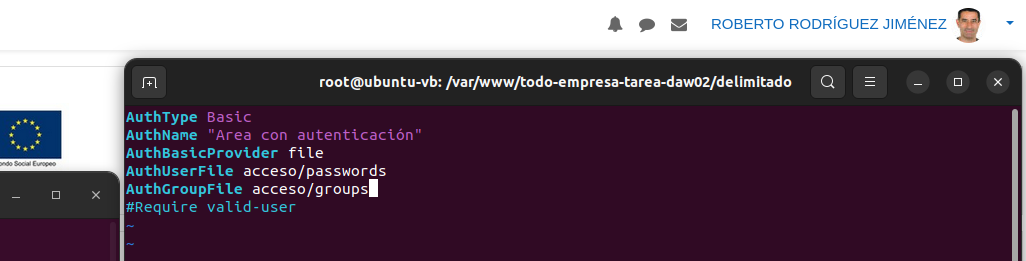




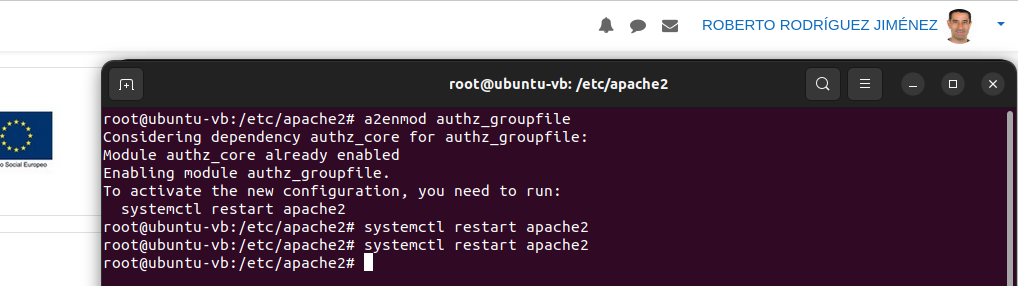
Creamos el archivo .htaccess en el directorio /*delimitado*

cd /var/www/todo-empresa-tarea-daw02/delimitado  
vim .htacces

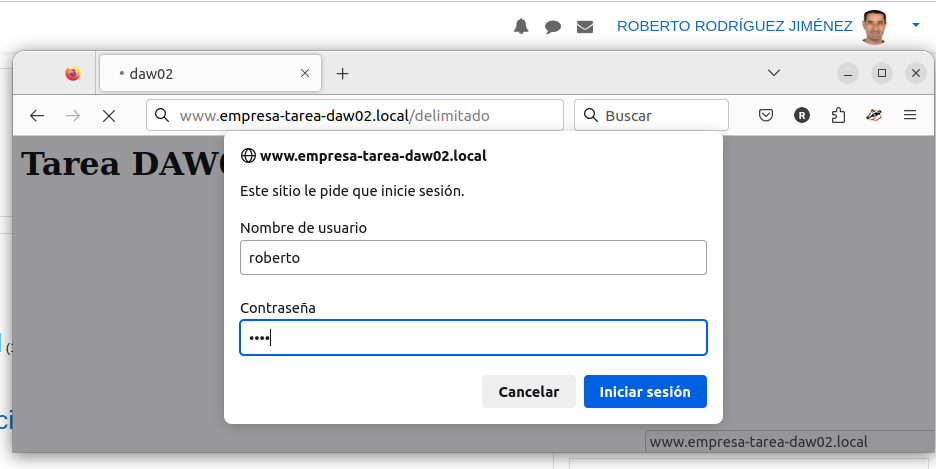
Contenido el fichero .htacces

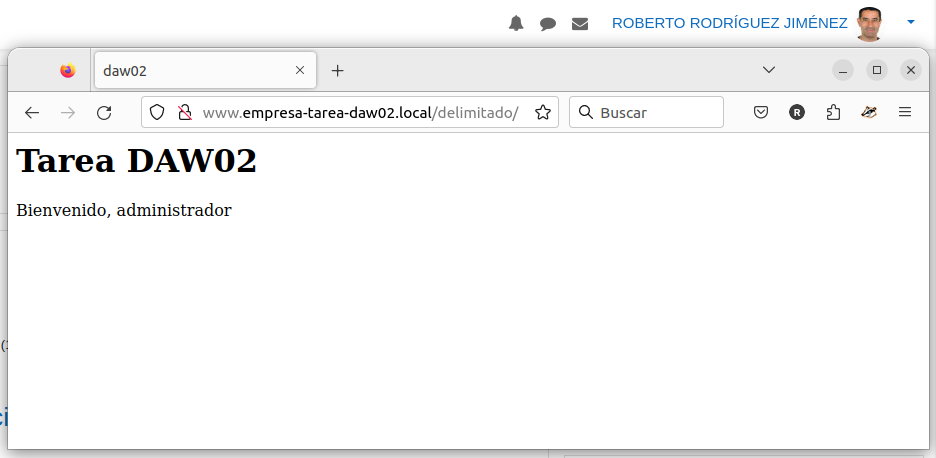


**Problema**  
He tenido problemas con AuthGroupFile al no estar habilitado el módulo authz\_groupfile.   
Se ha solucionado habilitándolo con a2enmod authz\_groupfile.



Vista de zona restringida





### Permitir el protocolo HTTPS en el virtual host empresa-tarea-daw02

Comprobamos que no tenemos acceso al servidor mediante https

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Creamos el directorio en el que se van a guardar los archivos

Texto

Descripción generada automáticamente

Ya tenemos la clave y el archivo *csr* que tenemos que mandar a la AC para que lo firme.

Captura de pantalla de un celular

Descripción generada automáticamente

Pedimos el certificado con la auto firma

Texto

Descripción generada automáticamente

Modificamos el archivo de configuración

Texto

Descripción generada automáticamente

El sitio se muestra correctamente con el certificado propio

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

### Configurar los archivos de registro como sigue:

1. Identificación log de acceso: empresa-tarea-daw02-access.log
2. Identificación log de error: empresa-tarea-daw02-error.log
3. Alias logformat: combined

Incluímos el código en el archivo de configuración *empresa-tarea-daw02.conf*.

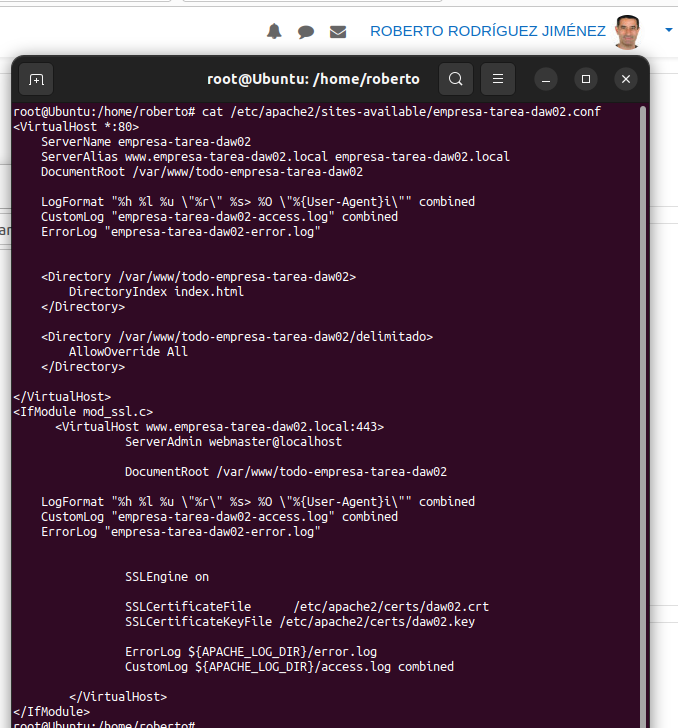
    LogFormat "%h %l %u \"%r\" %s> %O \"%{User-Agent}i\"" combined

    CustomLog "empresa-tarea-daw02-access.log" combined

    ErrorLog "empresa-tarea-daw02-error.log"

Podemos ver la salida del archivo con el log de acceso con el comando  
 tail -f /etc/apache2/empresa-tarea-daw02-access.log





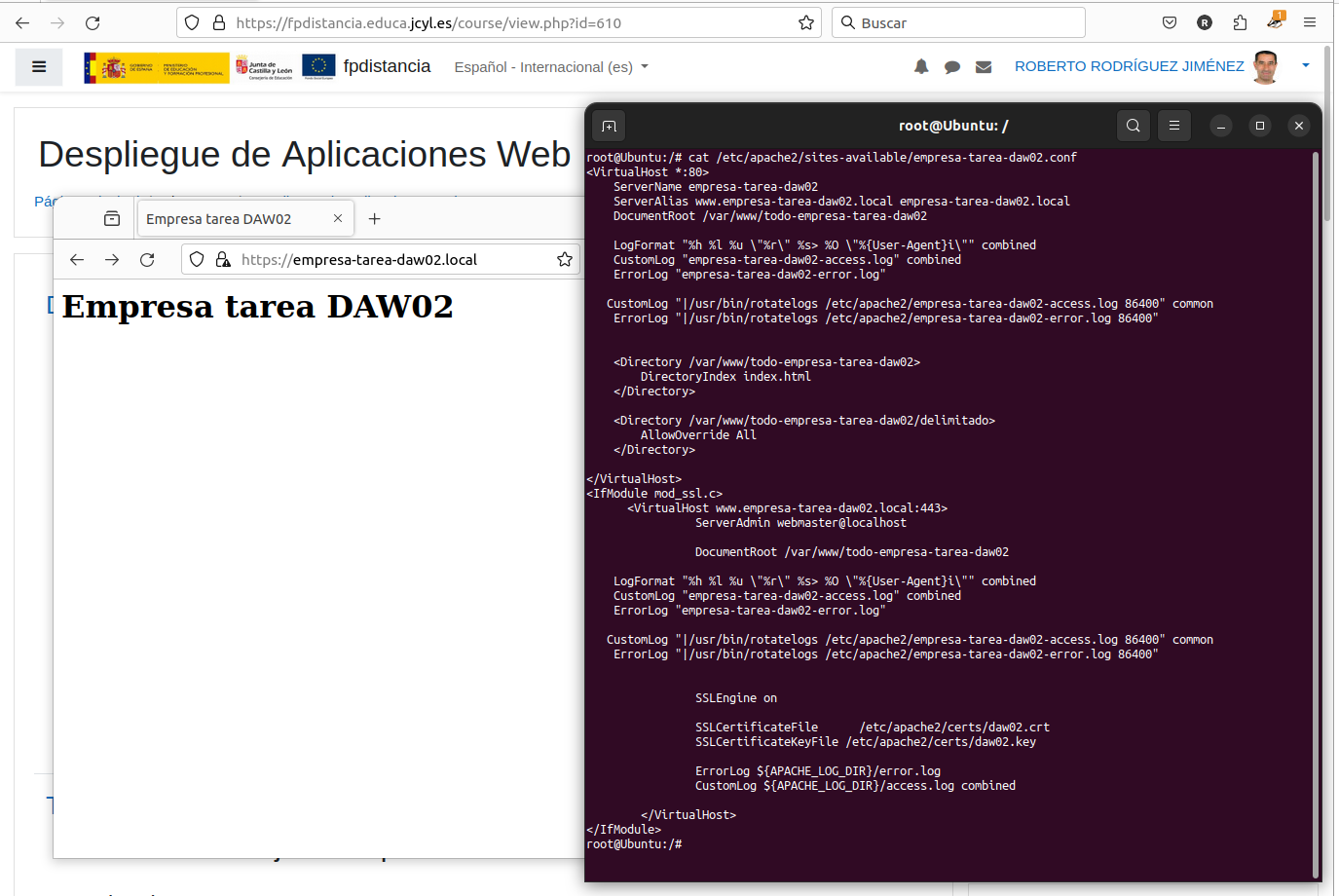
### Rotar logs por intervalo temporal: cada 24horas.

Rotamos los archivos log con *rotatelogs*.

Añadimos las líneas al archivo de configuración del host virtual.

   CustomLog "|/usr/bin/rotatelogs /etc/apache2/empresa-tarea-daw02-access.log 86400" common

   ErrorLog "|/usr/bin/rotatelogs /etc/apache2/empresa-tarea-daw02-error.log 86400"



## Código

Durante el ejercicio he ido creando un archivo *sh* para poder utilizarlo en diferentes máquinas virtuales, ya que no siempre he usado el mismo equipo.

#!/bin/bash

DOMINIO="empresa-tarea-daw02";

# Eliminar archivos, si los hubiera

rm /etc/apache2/sites-available/$DOMINIO.conf

rm /etc/apache2/sites-enabled/$DOMINIO.conf

rm -rd /var/www/todo-$DOMINIO

# Eliminar las líneas de hosts

sed '/empresa-tarea/d' -i /etc/hosts

clear

# 1.- Configurar un virtual host basado en el nombre denominado empresa-tarea-daw02

# que permita el acceso de la página web de la empresa en internet al directorio

# del servidor web: todo-empresa-tarea-daw02

# Crear el archivo de configuración empresa-tarea-daw02

echo -e "<VirtualHost \*:80>

    ServerName ${DOMINIO}

    ServerAlias www.empresa-tarea-daw02.local

    DocumentRoot /var/www/todo-${DOMINIO}

    <Directory /var/www/todo-${DOMINIO}>

        DirectoryIndex index.html

    </Directory>

</VirtualHost>" >> /etc/apache2/sites-available/${DOMINIO}.conf

# Habilitar el sitio

a2ensite empresa-tarea-daw02.conf

# Comprobar que el servidor esté creado

# apachectl -S

# Crear index.html

mkdir /var/www/todo-${DOMINIO}

echo "<html>

    <head>

        <title>Empresa tarea DAW02</title>

    </head>

    <body>

        <h1>Empresa tarea DAW02</h1>

          <p>ACCESO NO LIMITADO</p>

    </body>

</html>" >> /var/www/todo-${DOMINIO}/index.html

# Agregar el dominio al archivo hosts

cp /etc/hosts /etc/hosts\_ORIGIN

sed "3 a 10.0.2.15 ${DOMINIO}" -i /etc/hosts

sed "4 a 10.0.2.15 www.${DOMINIO}.local" -i /etc/hosts

# Resetear apache

systemctl restart apache2

# 2.- Hacer accesibles a través de internet las siguientes URL que identifican

# a la empresa: www.empresa-tarea-daw.local y empresa-tarea-daw-local

# Insertar el alias en el archivo de configuración

sed '/ServerAlias/d' -i /etc/apache2/sites-available/$DOMINIO.conf

sed '/ServerName/ a     ServerAlias www.empresa-tarea-daw02.local empresa-tarea-daw02.local' -i /etc/apache2/sites-available/empresa-tarea-daw02.conf

# Insertar el dominio en hosts

sed '/daw02.local/ a 10.0.2.15 empresa-tarea-daw02.local' -i /etc/hosts

systemctl restart apache2

# 3.- Configurar en el servidor el tipo MIME posible que permite la identificación

# correcta del vídeo de presentación formto flv situado dentro del directorio

# videos y de nombre de entrada .flv.

sed '/AddType application\/x-bzip2 .bz2/ a \\tAddType video/flv .flv' -i /etc/apache2/mods-available/mime.conf

sed '/AddType video\/flv .flv/ a \\tAddType video/x-flv .flv' -i /etc/apache2/mods-available/mime.conf

# 4.- Crear el subdirectorio todo-empresa-tarea-daw02/delimitado teniendo en cuenta que:

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

#   b. El subdirectorio todo-empresa-tarea-daw02/delimitado permite el acceso solamente al personal de la empresa que tenga el rol:admin

# Crear el subdirectorio dentro de todo-empresa-tarea-daw02

mkdir /var/www/todo-$DOMINIO/delimitado

echo "<html>

    <head>

        <title>Empresa tarea DAW02</title>

    </head>

    <body>

        <h1>Empresa tarea DAW02</h1>

          <p>ACCESO LIMITADO</p>

    </body>

</html>" >> /var/www/todo-${DOMINIO}/delimitado/index.html

# Restringir el acceso a /delimitado mediante el archivo .htaccess

# - Crear un fichero para guardar las contraseñas en un lugar inaccesible desde la web

mkdir /etc/apache2/acceso

# Crear el archivo passwords con el usuario roberto (pass: 0000)

htpasswd -c /etc/apache2/acceso/passwords roberto

# Crear el archivo para especificar los grupos

echo "admin: roberto" > /etc/apache2/acceso/grupos

# Configurar el archivo .htacces en el directorio que se quiere proteger.

# Añadimos la directiva AllowOverride AuthConfig en la configuración del host.

# Crear una copia

# cp /etc/apache2/sites-available/empresa-tarea-daw02.conf /etc/apache2/sites-available/empresa-tarea-daw02.conf\_COPY

sed '/<\/Directory>/ a \

\

    <Directory \/var\/www\/todo-empresa-tarea-daw02\/delimitado>\

        AllowOverride AuthConfig\

    </Directory>\

    ' -i /etc/apache2/sites-available/empresa-tarea-daw02.conf

# Crear el archivo .htaccess

echo "AuthType Basic

AuthName \"Area con autenticación\"

AuthBasicProvider file

AuthUserFile acceso/passwords

AuthGroupFile acceso/grupos

#Require valid-user

#Require group admin" >> /var/www/todo-$DOMINIO/delimitado/.htaccess

# Habilitar el módulo authz\_groupfile para evitar problemas

a2enmod authz\_groupfile

systemctl restart apache2

# 5 Permitir el protocolo HTTPS en el virtualhost empresa-tarea-daw02

# Crear el directorio en el que guardar los certificados

mkdir /etc/apache2/certs

openssl req -new -nodes -keyout /etc/apache2/certs/daw02.key -out /etc/apache2/certs/daw.csr

# Realizar la autofirma

openssl x509 -in /etc/apache2/certs/daw02.csr -out /etc/apache2/certs/daw02.crt -req -signkey /etc/apache2/certs/daw02.key -days 365

# Modificar el archivo de configuración

echo -e "<IfModule mod\_ssl.c>

      <VirtualHost www.empresa-tarea-daw02.local:443>

                ServerAdmin webmaster@localhost

                DocumentRoot /var/www/todo-empresa-tarea-daw02

                SSLEngine on

                SSLCertificateFile      /etc/apache2/certs/daw02.crt

                SSLCertificateKeyFile  /etc/apache2/certs/daw02.key

                ErrorLog \${APACHE\_LOG\_DIR}/error.log

                CustomLog \${APACHE\_LOG\_DIR}/access.log combined

        </VirtualHost>

</IfModule>"  >> /etc/apache2/sites-available/$DOMINIO.conf

# Hbilitar el módulo ssl

a2enmod ssl

systemctl restart apache2

# 6.- Confifurar los archivos de registro como sigue:

# Mostrar el archivo log: tail -f nombre-archivo.log

sed '/DocumentRoot/ a \

    \

    LogFormat "%h %l %u \\"%r\\" %s> %O \\"%{User-Agent}i\\"" combined\

    CustomLog "empresa-tarea-daw02-access.log" combined\

    ErrorLog "empresa-tarea-daw02-error.log"\

' -i /etc/apache2/sites-available/empresa-tarea-daw02.conf

# 7.- Rotar logs por intervalos de 24 horas.

sed '/ErrorLog "empresa-tarea-daw02-error.log"/ a \

    \

   CustomLog "|\/usr\/bin\/rotatelogs \/etc\/apache2\/empresa-tarea-daw02-access.log 86400" common\

    ErrorLog "|\/usr\/bin\/rotatelogs \/etc\/apache2\/empresa-tarea-daw02-error.log 86400"\

' -i /etc/apache2/sites-available/empresa-tarea-daw02.conf

systemctl restart apache2