

Tarea 02 de DAW. José Luis Comesaña

Enunciado.

Una empresa quiere mostrar y operar con su negocio a través de Internet. Así quiere:

- ✓ Una página web visible a cualquiera en Internet que publicite su negocio: quienes somos -que contiene un 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.

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:
 - 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**.
5. Permitir el protocolo HTTPS en el **virtualhost empresa-tarea-daw02**
6. Configurar los archivos de registro como sigue:
 - a. Identificación log de acceso: **empresa-tarea-daw02-access.log**
 - b. Identificación log de error: **empresa-tarea-daw02-error.log**
 - c. 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 raíz del directorio **todo-empresa-tarea-daw02** que contenga el texto 'ACCESO NO LIMITADO'.
 - ➔ Uno de nombre **index.html** en la raíz 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. Adjuntar los ficheros configurados.
 - ➔ Apoyar la documentación con capturas de pantalla. En alguna de ellas, se debe ver la plataforma con vuestra foto del perfil (la foto que os aparece arriba a la izquierda).

Criterios de puntuación. Total 10 puntos.

La valoración de cada apartado es:

1. 1 punto.
2. 1 punto.

3. 1 punto.
4. 2 puntos.
5. 3 puntos.
6. 1 punto.
7. 1 punto.

Recursos necesarios para realizar la Tarea.

- ✓ 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.

Consejos y 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 comiences 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.

Resolución de la tarea

Para la realización del **punto 1** iremos a la carpeta `/var/www/` y creamos un directorio al que denominaremos "`todo-empresa-tarea-daw02`", para ello abrimos el terminal de Linux y nos logamos como `root` tecleando:

```
sudo su
```

Introducimos la contraseña de superusuario root y ya estamos logados para poder realizar todas las tareas de configuración del virtualhost. Ahora creamos el directorio:

```
mkdir /var/www/todo-empresa-tarea-daw02
```

Y creamos el fichero de configuración para el virtualhost que nos solicita este punto de la tarea:

```
gedit /etc/apache2/sites-available/empresa-tarea-daw02
```

Y tecleamos las siguientes líneas dentro de él:

```
<VirtualHost *:80>
    DocumentRoot /var/www/todo-empresa-tarea-daw02/
    ServerName www.empresa-tarea-daw02.local
    ServerAlias empresa-tarea-daw02.local
</VirtualHost>
```

Grabamos el fichero y procedemos ahora a activar los VirtualHosts recién creados mediante los comandos:

```
a2ensite empresa-tarea-daw02.local
```

Como no hemos dado de alta el dominio en un servidor DNS, para probarlo podemos editar el fichero `/etc/hosts` para que las peticiones a ese dominio vaya a nuestro servidor:

```
gedit /etc/hosts
```

Y dentro del fichero pondremos:

```
127.0.0.1 www.empresa-tarea-daw02.local
```

El **punto 2** de la tarea que indica que debemos hacer accesible a través de internet a las URL que identifican a la empresa, ya lo tenemos hecho mediante las órdenes `ServerName` y `ServerAlias` del apartado anterior.

Ahora, para el **punto 3**, necesitamos indicar que podríamos utilizar un fichero de vídeo de tipo `flv`, para lo que editamos el fichero `mime.conf` del servidor, tecleando:

```
gedit /etc/apache2/mods-available/mime.conf
```

Y vemos que posee una línea donde pone:

```
TypesConfig /etc/mime.types
```

Lo cual indica que los tipos de archivos conocidos se encuentran en ese fichero, por lo que lo editamos tecleando:

```
gedit /etc/mime.types
```

Y dentro del fichero buscamos si ya existe una referencia al tipo de ficheros `flv`, encontrando:

```
video/x-flv flv
```

Que nos dice que los ficheros de tipo `flv` ya están reconocidos por el servidor como ficheros de vídeo. Si no existiera dicha línea seríamos nosotros los que tendríamos que teclearla.

El **punto 4** nos pide que creamos un subdirectorio dentro de `todo-empresa-tarea-daw02` para restringir el acceso a todos los usuarios que no tengan el rol de `admin`:

```
mkdir /var/www/todo-empresa-tarea-daw02/delimitado
```

Modificamos el fichero de configuración virtualhost anterior para que permita el uso del fichero htaccess en el directorio que deseamos restringir su acceso:

```
gedit /etc/apache2/sites-available/empresa-tarea-daw02
```

Y le añadimos:

```
<Directory /var/www/todo-empresa-tarea-daw02/delimitado>
  AllowOverride All
</Directory>
```

Y a continuación creamos un fichero `.htaccess` en el directorio que deseamos controlar:

```
gedit /var/www/todo-empresa-tarea-daw02/delimitado/.htaccess
```

Y tecleamos:

```
AuthType Basic
AuthName "Area restringida para administradores"
AuthUserFile /etc/apache2/todo-empresa-tarea-daw02/passwd
AuthGroupFile /etc/apache2/todo-empresa-tarea-daw02/roles
Require group admin
```

Como le indicamos que se restringe el acceso sólo a los pertenecientes al grupo `admin`, hemos de crear dicho grupo en el lugar indicado, en este caso en el fichero `roles` que ubicaremos en `/etc/apache2/todo-empresa-tarea-daw02/`, por lo que tecleamos:

```
gedit /etc/apache2/todo-empresa-tarea-daw02/roles
```

Y dentro del fichero ponemos:

```
admin: root joseluis
```

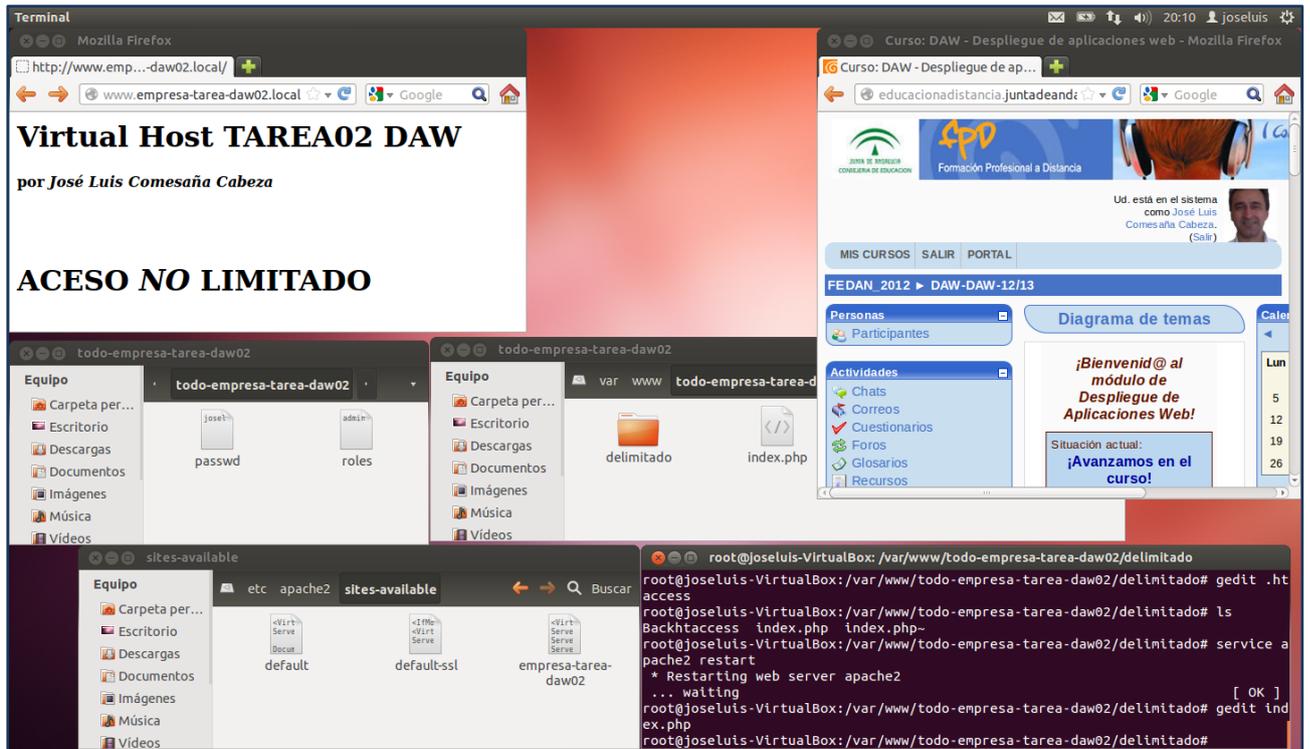
Con lo que asignamos al grupo `admin` los usuarios `root` y `joseluis`

Tenemos creado el grupo, pero no los usuarios, por lo que el siguiente paso será crear sus contraseñas de paso, para lo cual usaremos el mandato `htpasswd`, con el parámetro `-c` si lo vamos a crear por primera vez (*no posee usuarios creados*) o sin dicho parámetro para ir añadiendo nuevos miembros:

```
htpasswd -c /etc/apache2/todo-empresa-tarea-daw02/passwd joseluis
```

Introduzco la contraseña que quiera asignarle y me lo solicita nuevamente para confirmarla.

Reiniciamos el servidor con `service apache2 restart` y ya estamos preparados para probarlo, pero antes, como ambas carpetas están vacías, crearemos un `index.html` para cada una, quedando como nuestro a continuación:

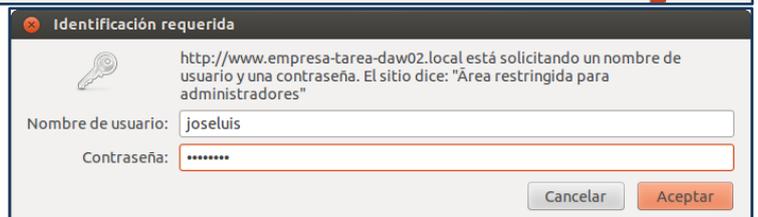


Escritorio con página principal de ACCESO NO LIMITADO

Quando intentamos acceder a "limitado" nos pide usuario/contraseña, y si nos equivocamos nos muestra una pantalla de error:



Quando introducimos el par usuario/contraseña de forma adecuada:



Conseguimos que nos muestre la página de forma correcta:



El **punto 5** nos pide que permitamos acceder al servidor creado, con HTTPS, para lo que instalaremos el openssl con:

```
apt-get install openssl
```

Y lo activamos con:

```
a2enmod ssl
```

Reiniciamos el servidor web apache:

```
service apache2 restart
```

Creamos ahora una carpeta, en la de apache por ejemplo, que contendrá los certificados, y a la que vamos a llamar `ssl`:

```
mkdir /etc/apache2/ssl
```

Nos situamos en la nueva carpeta

```
cd /etc/apache2/ssl
```

Lo primero es crear la clave privada del servidor. Lo hacemos mediante la generación aleatoria de una cadena de texto, tecleando:

```
openssl genrsa -des3 -out server.key 1024
```

Nos pide una frase de paso que debemos recordar (yo he puesto *cual es mi edad*), ya que la solicitará siempre que reiniciemos el servidor. Si quisiéramos deshabilitar el hecho de que la pida siempre (*no es recomendable*), teclearíamos:

```
openssl rsa -in server.key -out server.pem
```

Ahora generaremos el archivo `csr` mediante la orden:

```
openssl req -new -key server.key -out server.csr
```

Lo cual solicitará una serie de datos que hemos de introducir, teniendo especial atención en poner la web exacta del dominio que queremos activar con ssl. En nuestro caso, cuando nos pregunta “Common Name” teclearemos `www.empresa-tarea-daw02.local`

Algunos campos pueden tener valores por defecto, pero si deseamos dejar el campo en blanco tendremos que poner sólo un punto.

Con esto ya podemos emitir certificados para nuestro sitio, por lo que vamos a generar uno autofirmado, ya que no poseemos ninguno de una autoridad certificada. Tecleamos:

```
openssl x509 -req -days 365 -in server.csr -signkey server.key -out server.crt
```

Hemos puesto que caduque al año, pero podríamos haber puesto cualquier cantidad de días.

Ya tenemos listos los certificados, por lo que pasaremos ahora a crear el virtualhost que lo contendrá y la carpeta donde lo ubicaremos, por lo que tecleamos:

```
mkdir /var/www/todo-empresa-tarea-daw02-ssl
```

Creamos un fichero `index.html` igual que hicimos para el virtualhost anterior, pero le ponemos un mensaje que nos indique que estamos ante una web segura.

Ahora nos dirigimos a `/etc/apache2/sites-available` y copiamos el contenido del virtualhost del punto anterior “`empresa-tarea-daw02`” y lo llamamos “`empresa-tarea-daw02-ssl`” para lo que tecleamos:

```
cd /etc/apache2/sites-available
cp empresa-tarea-daw02 empresa-tarea-daw02-ssl
```

Y editamos su contenido con `gedit` para cambiarlo por:

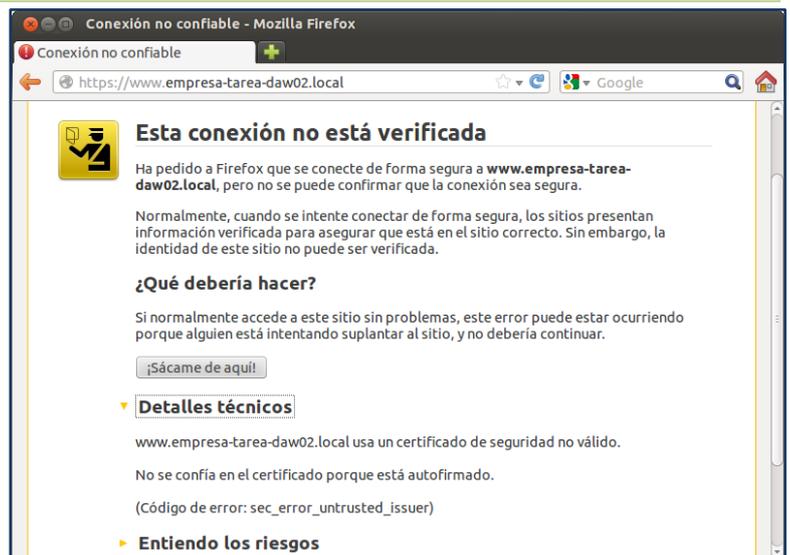
```
<VirtualHost *:443>
  ServerAdmin webmaster@empresa-tarea-daw02.local
  ServerName www.empresa-tarea-daw02.local
  ServerAlias empresa-tarea-daw02.local
  DocumentRoot /var/www/todo-empresa-tarea-daw02-ssl/
  SSLEngine on
  SSLCertificateFile /etc/apache2/ssl/server.crt
  SSLCertificateKeyFile /etc/apache2/ssl/server.pem
</VirtualHost>
```

Ya lo tenemos listo y sólo queda recargar y reiniciar apache para que entre en funcionamiento la nueva configuración:

```
service apache2 reload
service apache2 restart
```

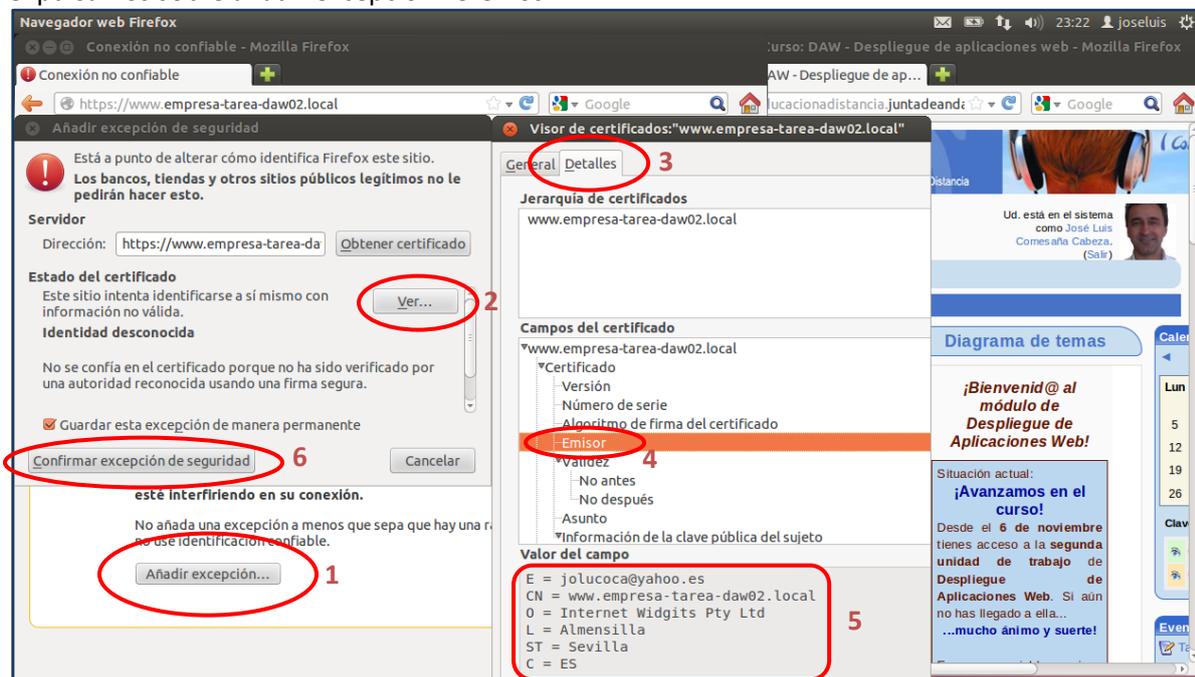
Ahora para comprobar que todo ha salido bien, nos dirigiremos al navegador y en su barra de direcciones teclearemos:

```
https://www.empresa-tarea-daw02.local
```



Y aparece lo siguiente:

Si pulsamos sobre añadir excepción veremos:



Y cuando pulsamos sobre “Confirmar excepción de seguridad” nos aparece:



Ahora, para el **punto 6** nos dirigimos a la carpeta donde tenemos configurado el virtualhost y editamos su fichero de configuración tecleando:

```
cd /etc/apache2/sites-available
gedit empresa-tarea-daw02
```

Y añadimos al final del mismo, pero dentro de las etiquetas VirtualHost, las siguientes líneas:

```
LogFormat "%h %l %u %t \"%r\" %>s %b" combined
CustomLog empresa-tarea-daw02-access.log combined
ErrorLog "empresa-tarea-daw02-error.log"
```

Con la primera línea asignamos el alias `combined` a `logformat`, con el que generaremos registros en el formato

<code>%h</code>	host
<code>%l</code>	identificación_cliente
<code>%u</code>	usuario
<code>%t</code>	fecha_y_hora
<code>\"%r\"</code>	cliente, recurso, protocolo
<code>%>s</code>	Código de estado que el servidor envía de vuelta al cliente. Si el código comienza por 2 fue respondido con éxito, por 3 identifican una redirección, por 4 se trata de un error del cliente y por 5 es un error del servidor.
<code>%b</code>	Tamaño del objeto retornado por el cliente.

Si cuando nos tenga que presentar los datos, alguno de ellos no existe, pondrá un guión en el lugar que le corresponda.

Con la segunda línea conseguimos indicar que el fichero de registro de acceso se guardará en el directorio del servidor por defecto, con el nombre de `empresa-tarea-daw02-access.log` y con el contenido que se adapte al formato establecido en la línea anterior:

La tercera línea se usa para indicar dónde se ha de guardar el registro de errores, en este caso, en el fichero `empresa-tarea-daw02-error.log` situado en el directorio por defecto del servidor.

Para realizar el **punto 7** y último, a lo introducido en el punto anterior, añadiremos:

```
CustomLog "|/usr/sbin/rotateCustom /etc/apache2/empresa-tarea-daw02-access.log 86400" combined
ErrorLog "|/usr/sbin/rotateError /etc/apache2/empresa-tarea-daw02-error.log 86400" combined
```

Con lo que le indicamos que el fichero del registro de acceso `empresa-tarea-daw02-access.log` que se encuentra situado en `/etc/apache2` lo almacene cada 24 horas (*86400 segundos*) en el fichero `rotateCustom` que se encuentra en `/usr/sbin` utilizando para ello el alias `combined`

Con la segunda línea, decimos que el fichero de registro de errores `empresa-tarea-daw02-error.log` que se encuentra en `/etc/apache2` lo almacene cada 24 horas (*86400 segundos*) en el fichero `rotateError` que se encuentra en `/usr/sbin` utilizando para ello el alias `combined`

NOTA Cuando reiniciaba o recargaba apache me aparecía un error, el cual conseguí arreglar creando un fichero de nombre `httpd.conf` (*que no existía*), en `/etc/apache2/` y le introduce `ServerName localhost` como único valor.