

TAREAS quincena 5. https, autenticación, Awstats

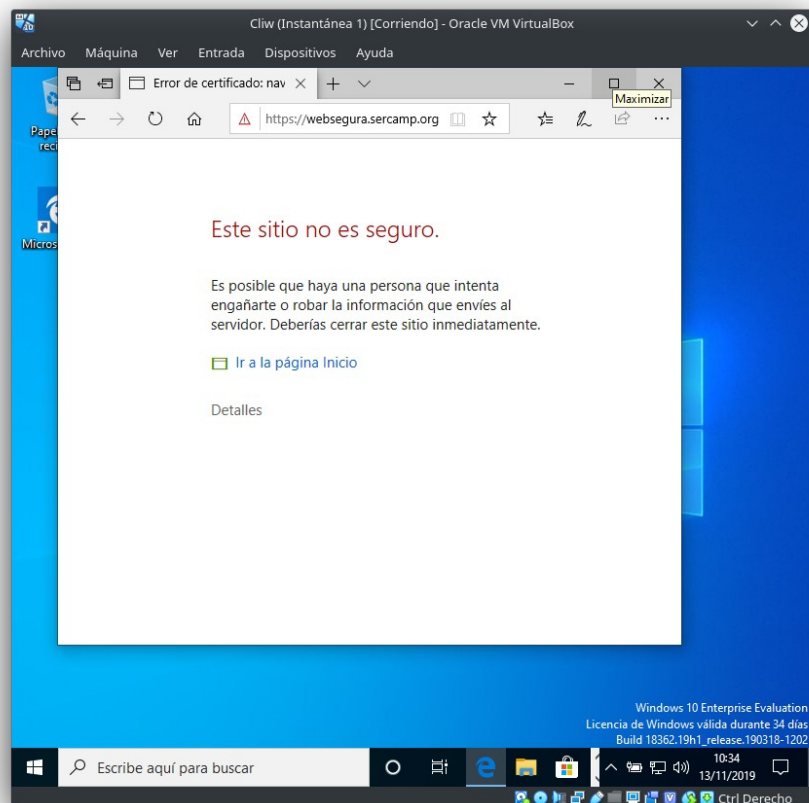
TAREA 1. - instala un servidor https en una máquina virtual. Sigue las instrucciones del documento Apache (puntos 3 y 4 para esta quincena)

Para entregar:

- Captura de pantalla de la alerta de seguridad que nos indica que el certificado no está emitido por una CA en la que confiamos.

En el cliente tecleamos desde el navegador

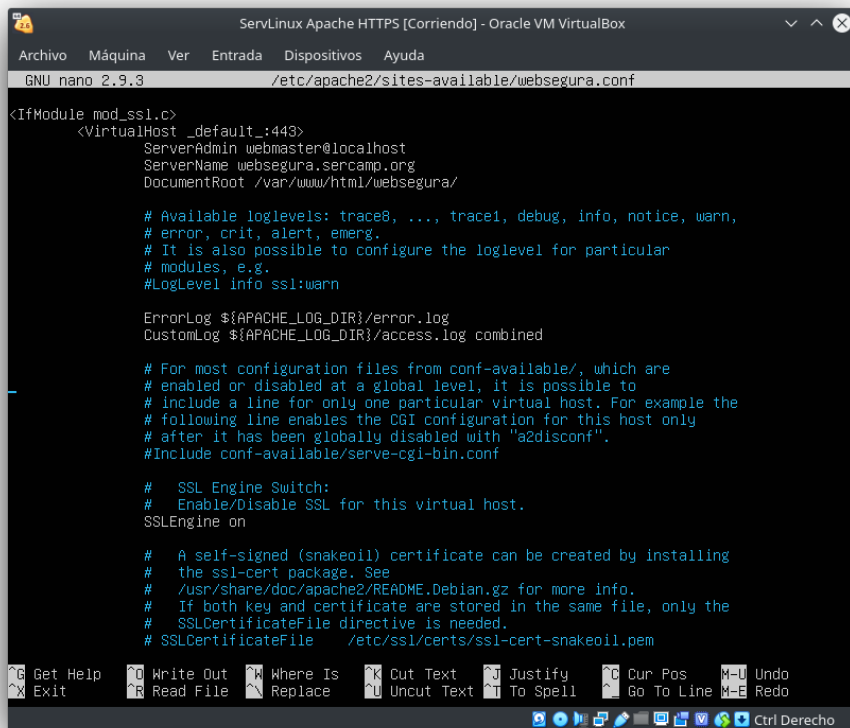
'<https://websegura.sercamp.org>'.



TAREAS quincena 5. https, autenticación, Awstats

- Captura de las modificaciones realizadas en los diferentes archivos de configuración

Configuración de Websegura.



```
GNU nano 2.9.3 /etc/apache2/sites-available/websegura.conf

<IfModule mod_ssl.c>
<VirtualHost _default_:443>
    ServerAdmin webmaster@localhost
    ServerName websegura.sercamp.org
    DocumentRoot /var/www/html/websegura/

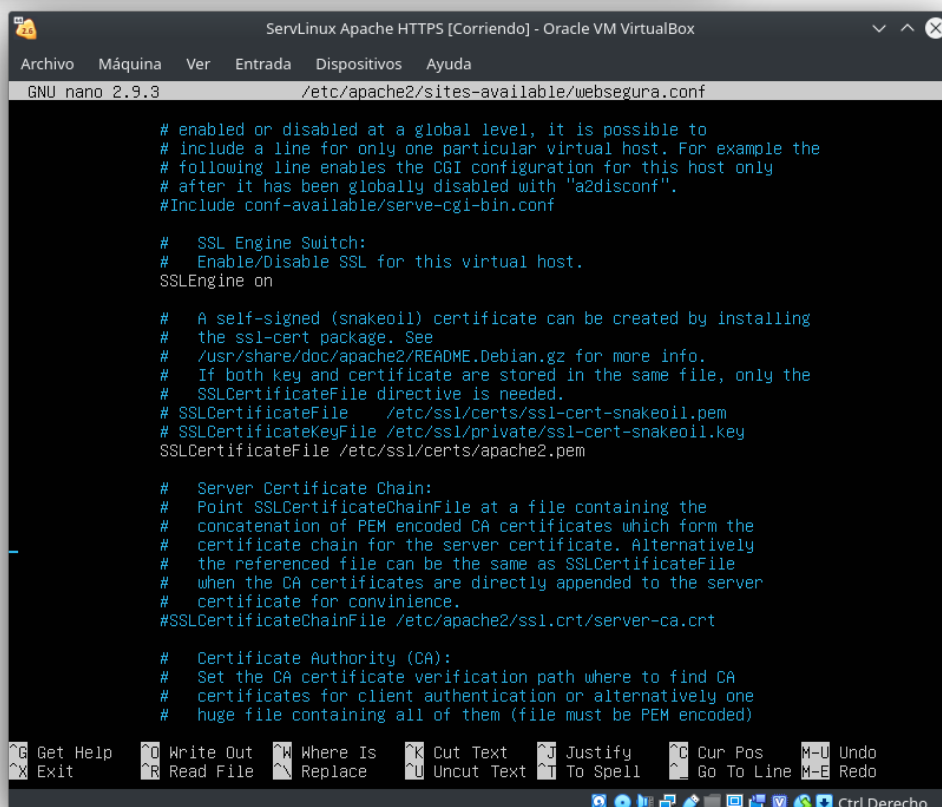
    # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
    # error, crit, alert, emerg.
    # It is also possible to configure the loglevel for particular
    # modules, e.g.
    #LogLevel info ssl:warn

    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined

    # For most configuration files from conf-available/, which are
    # enabled or disabled at a global level, it is possible to
    # include a line for only one particular virtual host. For example the
    # following line enables the CGI configuration for this host only
    # after it has been globally disabled with "a2disconf".
    #Include conf-available/serve-cgi-bin.conf

    #
    # SSL Engine Switch:
    # Enable/Disable SSL for this virtual host.
    SSLEngine on

    #
    # A self-signed (snakeoil) certificate can be created by installing
    # the ssl-cert package. See
    # /usr/share/doc/apache2/README.Debian.gz for more info.
    # If both key and certificate are stored in the same file, only the
    # SSLCertificateFile directive is needed.
    # SSLCertificateFile /etc/ssl/certs/ssl-cert-snakeoil.pem
```



```
GNU nano 2.9.3 /etc/apache2/sites-available/websegura.conf

    # enabled or disabled at a global level, it is possible to
    # include a line for only one particular virtual host. For example the
    # following line enables the CGI configuration for this host only
    # after it has been globally disabled with "a2disconf".
    #Include conf-available/serve-cgi-bin.conf

    #
    # SSL Engine Switch:
    # Enable/Disable SSL for this virtual host.
    SSLEngine on

    #
    # A self-signed (snakeoil) certificate can be created by installing
    # the ssl-cert package. See
    # /usr/share/doc/apache2/README.Debian.gz for more info.
    # If both key and certificate are stored in the same file, only the
    # SSLCertificateFile directive is needed.
    # SSLCertificateFile /etc/ssl/certs/ssl-cert-snakeoil.pem
    # SSLCertificateKeyFile /etc/ssl/private/ssl-cert-snakeoil.key
    # SSLCertificateFile /etc/ssl/certs/apache2.pem

    #
    # Server Certificate Chain:
    # Point SSLCertificateChainFile at a file containing the
    # concatenation of PEM encoded CA certificates which form the
    # certificate chain for the server certificate. Alternatively
    # the referenced file can be the same as SSLCertificateFile
    # when the CA certificates are directly appended to the server
    # certificate for convenience.
    # SSLCertificateChainFile /etc/apache2/ssl.crt/server-ca.crt

    #
    # Certificate Authority (CA):
    # Set the CA certificate verification path where to find CA
    # certificates for client authentication or alternatively one
    # huge file containing all of them (file must be PEM encoded)
```

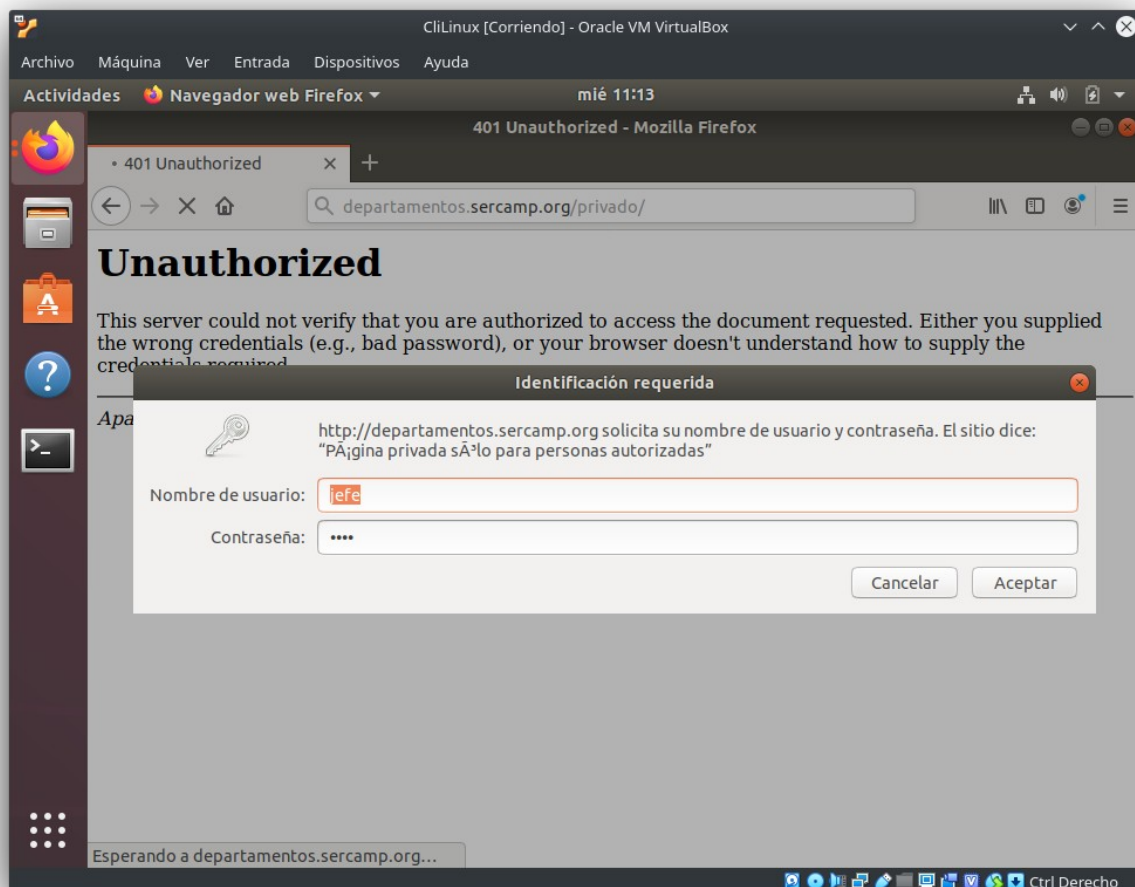
TAREAS quincena 5. https, autenticación, Awstats

TAREA 2. - Acceso autenticado a nuestro servidor web. Sigue las instrucciones del documento Apache (puntos 3 y 4 para esta quincena)

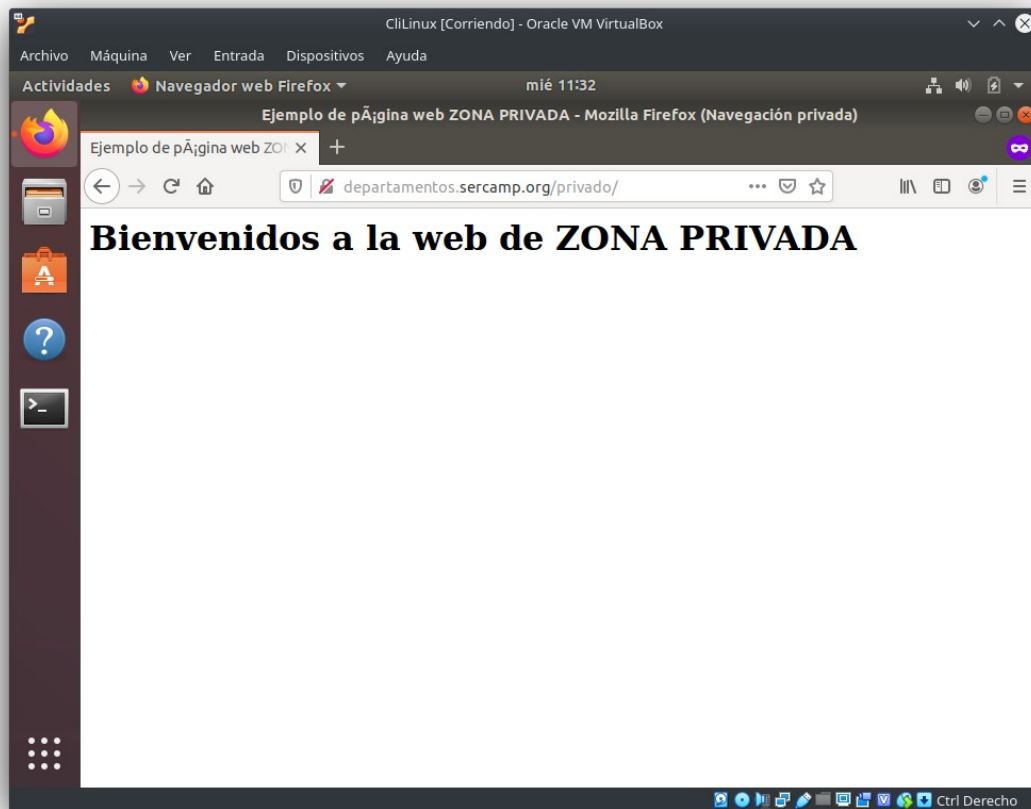
Crea una carpeta a la que sólo darás acceso a usuarios autenticados empleando la autenticación básica proporcionada por Apache.

Para entregar:

- Captura de pantalla accediendo a <http://departamentos.sercamp.org/privado> veremos que nos pide un usuario y contraseña y tras introducir el usuario y contraseña correcto nos dará acceso a la carpeta: **privado**.

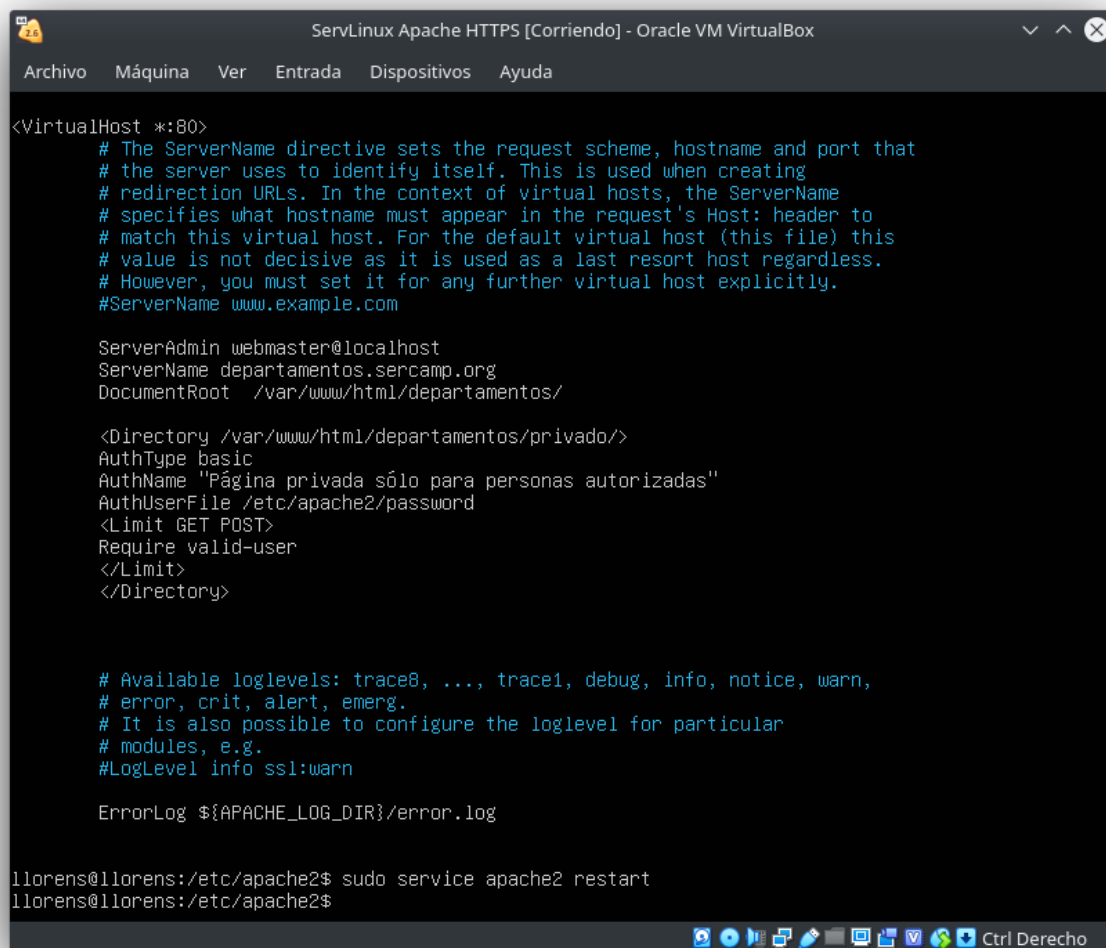


TAREAS quincena 5. https, autenticación, Awstats



TAREAS quincena 5. https, autenticación, Awstats

Configuración



```
ServLinux Apache HTTPS [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda

<VirtualHost *:80>
# The ServerName directive sets the request scheme, hostname and port that
# the server uses to identify itself. This is used when creating
# redirection URLs. In the context of virtual hosts, the ServerName
# specifies what hostname must appear in the request's Host: header to
# match this virtual host. For the default virtual host (this file) this
# value is not decisive as it is used as a last resort host regardless.
# However, you must set it for any further virtual host explicitly.
#ServerName www.example.com

ServerAdmin webmaster@localhost
ServerName departamentos.sercamp.org
DocumentRoot /var/www/html/departamentos/

<Directory /var/www/html/departamentos/privado/>
AuthType basic
AuthName "Página privada sólo para personas autorizadas"
AuthUserFile /etc/apache2/password
<Limit GET POST>
Require valid-user
</Limit>
</Directory>

# Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
# error, crit, alert, emerg.
# It is also possible to configure the loglevel for particular
# modules, e.g.
#LogLevel info ssl:warn

ErrorLog ${APACHE_LOG_DIR}/error.log

llorens@llorens:/etc/apache2$ sudo service apache2 restart
llorens@llorens:/etc/apache2$
```