Servidor virtual HTTPS en Linux

Objetivos

- Crear un certificado digital autofirmado con *openssi* para el dominio **seguro.africalinux.org**
- Crear y habilitar un servidor virtual https para el dominio seguro.africalinux.org

Actividades:

1. Configura el servidor DNS para que resuelva el nombre **seguro.africalinux.org**. La dirección IP asociada al nombre será la IP del Servidor Linux.

```
/etc/bind/db.africalinux.org
  GNU nano 4.8
 BIND data file for local loopback interface
$ORIGIN africalinux.org.
$TTL
        2D
        ΙN
                SOA
                         africa–server1
                                         root (
                          2020121401
                                          ; Serial
                          604800
                                            Refresh
                           86400
                                          ; Retry
                         2419200
                                          ; Expire
                                          ; Negative Cache TTL
                          604800 )
africalinux.org.
                         ΙN
                                 NS
                                          africa-server1
africa–server1
                         ΙN
                                          192.168.1.200
                         ΙN
                                CNAME
www
                                          africa–server1
web
                         ΙN
                                CNAME
                                          africa–server1
                         ΙN
                                CNAME
                                          africa-server1_<
seguro
```

```
GNU nano 4.8
                                           /etc/bind/db.192.168.1
 BIND data file for local loopback interface
$ORIGIN 1.168.192.in–addr.arpa.
        604800
$TTL
        ΙN
                SOA
                         africa–server1 root (
                          2020121401
                                          ; Serial
                          604800
                                          ; Refresh
                           86400
                                          ; Retry
                         2419200
                                          ; Expire
                          604800 )
                                          ; Negative Cache TTL
                         africa-server1.africalinux.org.
        ΙN
                NS
200
         ΙN
                          africa–server1.africalinux.org.
                PTR
200
         ΙN
                          www.africalinux.org.
                 PTR
200
         ΙN
                          web.africalinux.org.
                 PTR
200
         ΙN
                 PTR
                          seguro.africalinux.org 🤙
```

 Reiniciar el servidor para guardar cambios. sudo service bind9 restart 3. Crea el directorio /var/www/html/seguro
Este directorio será el directorio raíz

4. Crea el fichero de texto /var/www/html/seguro/index.html con el contenido que quieras.

- 5. Crea un certificado digital autofirmado usando openssl
 - 5.1 Sitúate en el directorio **home** del usuario con que has iniciado sesión.
 - 5.2 Crea una clave privada RSA de 2048 bit. openssl genrsa –out seguro.key 2048

5.3 Genera una solicitud de certificado (CSR) openssl req –new –key seguro.key –out seguro.csr

A continuación, introduce los datos del certificado.

Esta solicitud de certificado se la podrías enviar a una autoridad de certificación para que generase el certificado (CTR). En este caso lo vamos a firmar nosotros, vamos a crear un certificado autofirmado.

5.4 Crea el certificado digital autofirmado usando la clave privada.

openssl x509 –req –days 365 –in seguro.csr –signkey seguro.key –out seguro.crt

6. Copia la clave y el certificado en los directorios que utiliza por defecto Apache y configura los permisos adecuados.

sudo mv seguro.key /etc/ssl/private
atricaserver1@atrica-server1:"\$ sudo mv seguro.key /etc/ssl/private/
[sudo] password for africaserver1:

sudo mv seguro.crt /etc/ssl/certs

africaserver1@africa–server1:~\$ sudo mv seguro.crt /etc/ssl/certs/

sudo chown root:ssl-cert /etc/ssl/private/seguro.key sudo chmod 640 /etc/ssl/private/seguro.key sudo chown root:root /etc/ssl/certs/seguro.crt

africaserver1@africa–server1:~\$ sudo chown root:ssl–cert /etc/ssl/private/seguro.key africaserver1@africa–server1:~\$ sudo chmod 640 /etc/ssl/private/seguro.key africaserver1@africa–server1:~\$ sudo chown root:root /etc/ssl/certs/seguro.crt

7. Crea el fichero /etc/apache/sites-available/seguro.conf con las siguientes directivas

```
GNU nano 4.8
                                              seguro.conf
(IfModule mod_ssl.c)
       <VirtualHost _default_:443>
               ServerName seguro.africalinux.org
               DocumentRoot /var/www/html/seguro
               ErrorLog ${APACHE_LOG_DIR}/seguro.error.log
               CustomLog ${APACHE_LOG_DIR}/seguro.acces.log combined
               <Directory /var/www/html/seguro>
                       Options Indexes FollowSymLinks
                       AllowOverride None
                       Require all granted
               </Directory>
               SSLEngine on
               SSLCertificateFile
                                                /etc/ssl/certs/seguro.crt
               SSLCertificateKeyFile
                                                /etc/ssl/private/seguro.key
       </VirtualHost>
/IfModule>
```

El log de errores será /var/log/apache2/seguro.error.log El log de accesos será /var/log/apache2/seguro.access.log, con formato combined 8. Deshabilita el servidor ssl por defecto sudo a2dissite default-ssl

```
africaserver1@africa–server1:/etc/apache2$ sudo a2dissite default–ssl
Site default–ssl disabled.
To activate the new configuration, you need to run:
systemctl reload apache2
africaserver1@africa–server1:/etc/apache2$ _
```

 Habilita el servidor virtual seguro. sudo a2ensite seguro

```
africaserver1@africa–server1:~$ sudo a2ensite seguro
[sudo] password for africaserver1:
Enabling site seguro.
To activate the new configuration, you need to run:
systemctl reload apache2
```

 Verifica que dentro del directorio /etc/apache2/sites-enabled se ha creado el enlace seguro.conf

```
africaserver1@africa-server1:/etc/apache2/sites-enabled$ sudo ln -s ../sites-available/seguro.conf s
eguro.conf
africaserver1@africa-server1:/etc/apache2/sites-enabled$ ll

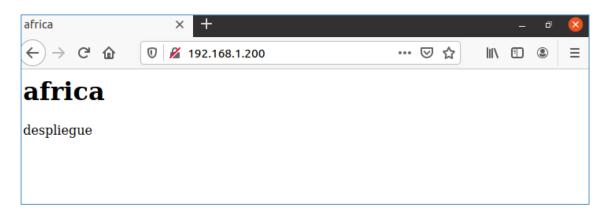
total 8

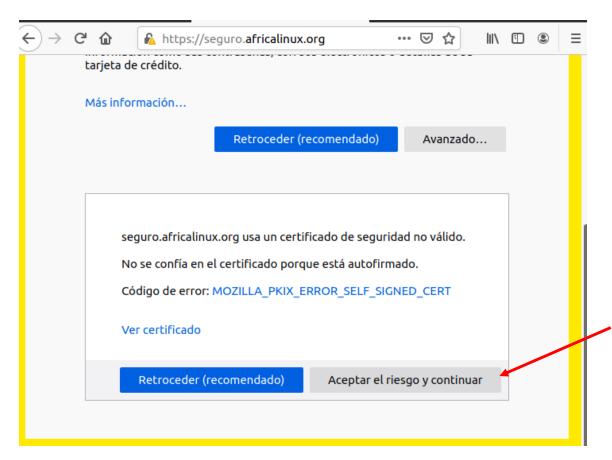
drwxr-xr-x 2 root root 4096 Feb 19 22:06 ./
drwxr-xr-x 8 root root 4096 Feb 19 21:48 ../
lrwxrwxrwx 1 root root 35 Jan 14 10:00 000-default.conf -> ../sites-available/000-default.conf
lrwxrwxrwx 1 root root 35 Feb 19 20:30 default-ssl.conf -> ../sites-available/default-ssl.conf
lrwxrwxrwx 1 root root 30 Feb 19 22:06 seguro.conf -> ../sites-available/seguro.conf
africaserver1@africa-server1:/etc/apache2/sites-enabled$ sudo service apache2 start
africaserver1@africa-server1:/etc/apache2/sites-enabled$ sudo service apache2 start

Enlace creado
```

- 11. Reinicia el servidor para que los cambios tengan efecto.
- 12. Desde el cliente abre el navegador y establece una conexión a https://seguro.africalinux.org

Si escribo http://IP-Servidor







Servidor virtual HTTPS en LINUX