Actividades.

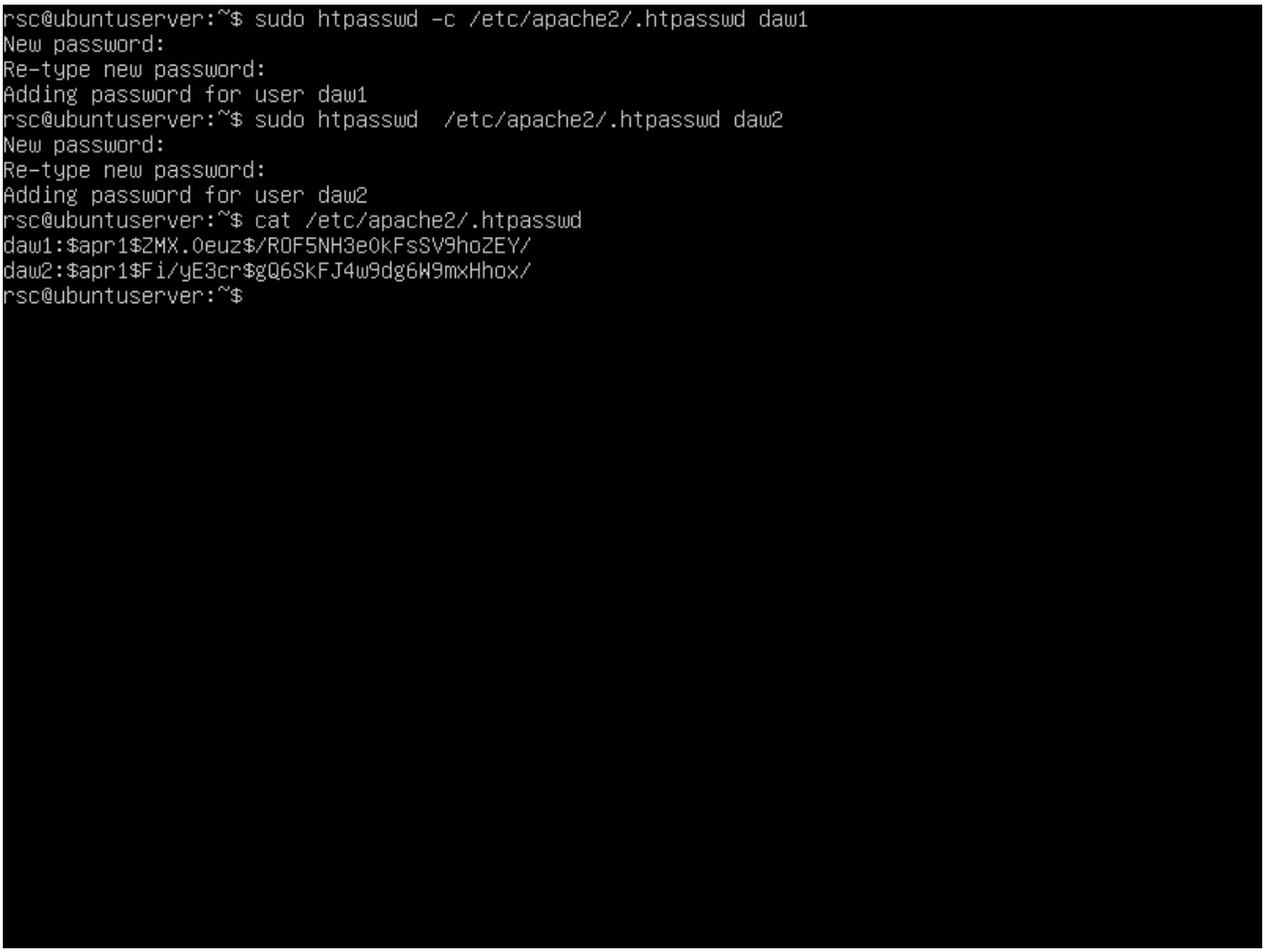
2. Crear el subdirectorio todo-daw02/delimitado teniendo en cuenta que:

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

✓ El subdirectorio todo-daw02/delimitado permite el acceso solamente al usuario admin.

Paso 1:

> Crear los usuarios y password con htpassword



Paso 2:

> Añadir un nuevo directory al archivo daw02-ssl.conf

```
#   o StdEnvVars:
#         This exports the standard SSL/TLS related `SSL_*' environment variables.
#         Per default this exportation is switched off for performance reasons,
#         because the extraction step is an expensive operation and is usually
#         useless for serving static content. So one usually enables the
#         exportation for CGI and SSI requests only.
#   o OptRenegotiate:
#         This enables optimized SSL connection renegotiation handling when SSL
#         directives are used in per-directory context.
#SSLOptions +FakeBasicAuth +ExportCertData +StrictRequire
<FilesMatch "\.(cgi|shtml|phtml|php)$">
                SSLOptions +StdEnvVars
</FilesMatch>
<Directory /usr/lib/cgi-bin>
                SSLOptions +StdEnvVars
</Directory>

<Directory "/var/www/html/todo-daw02/public_html/delimitado">
        AuthType Basic
        AuthName "Contenido Restringido, solo admin"
        AuthUserFile /etc/apache2/.htpasswd
        Require valid-user
</Directory>
#   SSL Protocol Adjustments:
#   The safe and default but still SSL/TLS standard compliant shutdown
#   approach is that mod_ssl sends the close notify alert but doesn't wait for
#   the close notify alert from client. When you need a different shutdown
#   approach you can use one of the following variables:
#   o ssl-unclean-shutdown:
#         This forces an unclean shutdown when the connection is closed, i.e. no
#         SSL close notify alert is send or allowed to received.  This violates
#         the SSL/TLS standard but is needed for some brain-dead browsers. Use
#         this when you receive I/O errors because of the standard approach where
#         mod_ssl sends the close notify alert.
#   o ssl-accurate-shutdown:
#         This forces an accurate shutdown when the connection is closed, i.e. a
"/etc/apache2/sites-available/daw02-ssl.conf" 139L, 6566B                     102,51-65     81%
```

Paso 3:

> Comprobar con apachectl configtest si esta bien la sintaxis del archivo anterior

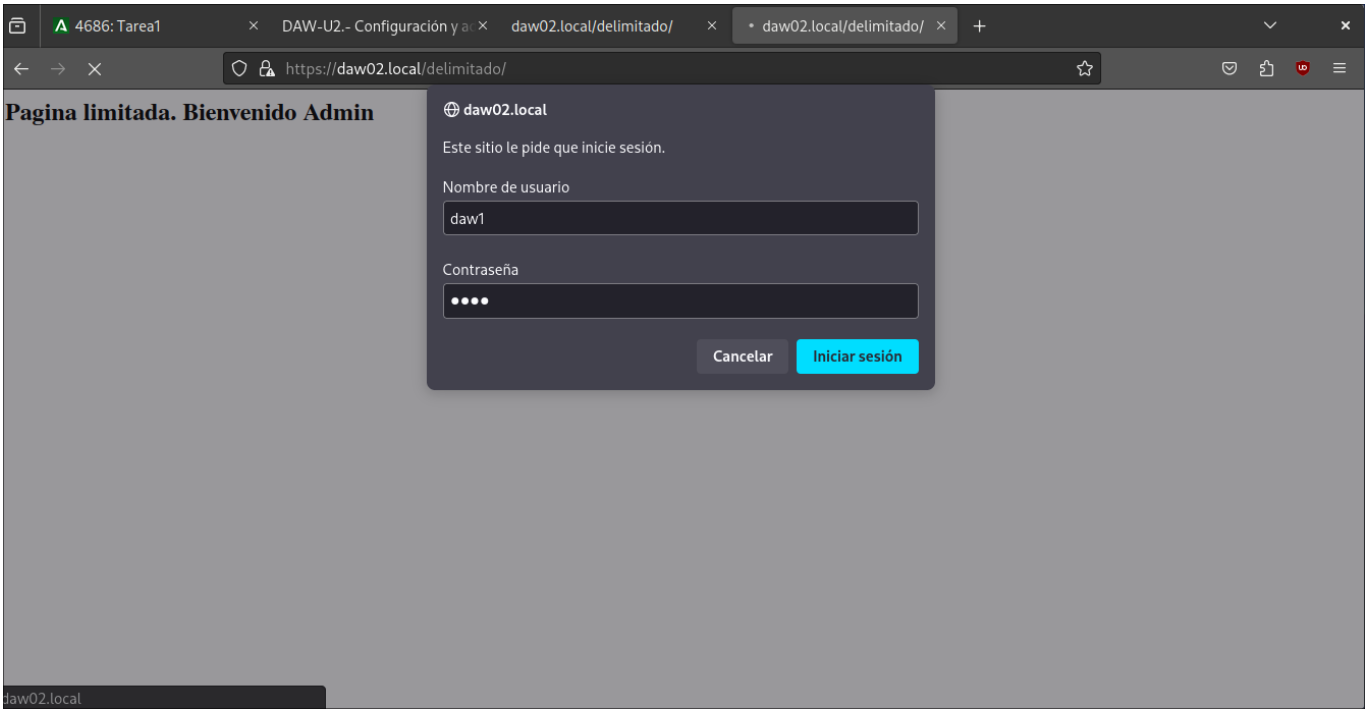
Paso 4:

> Le damos permisos a la nueva carpeta.

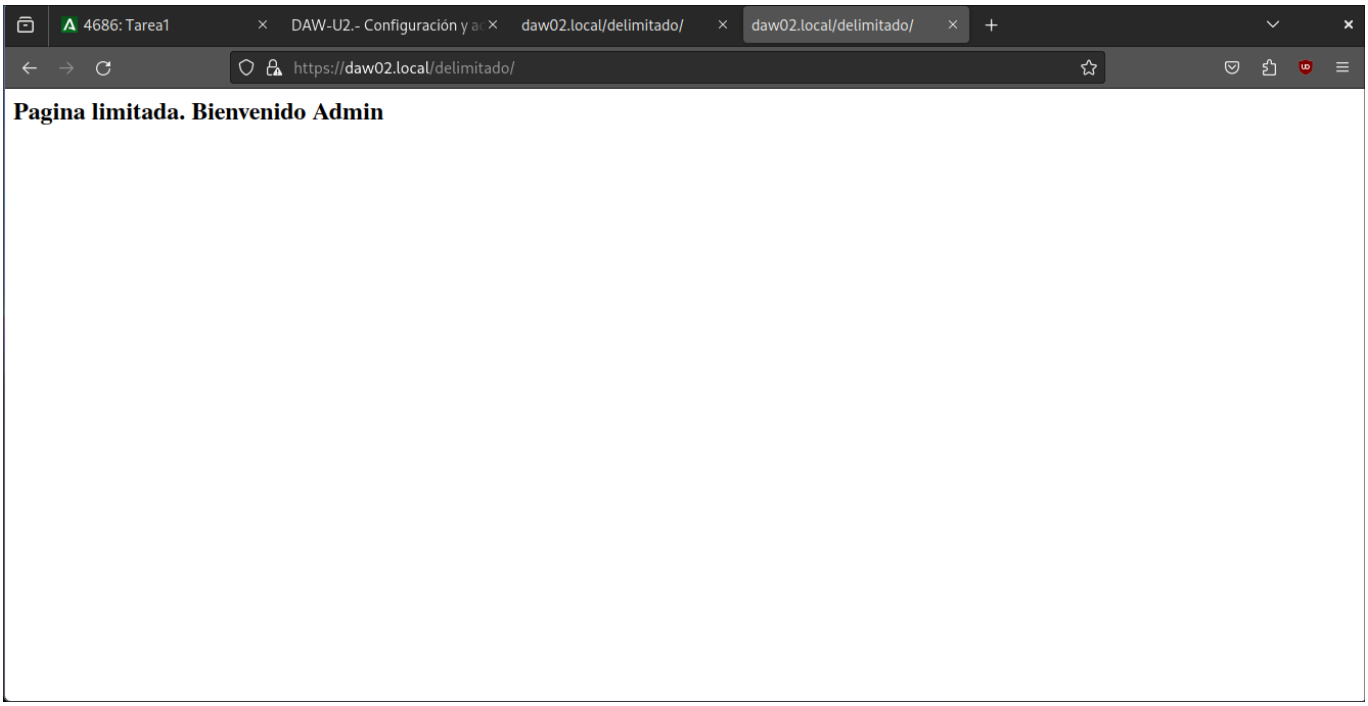
```
rsc@ubuntuserver:~$ ls -l /var/www/html/todo-daw02/
total 4
drwxr-xr-x 3 755 www-data 4096 oct 26 08:56 public_html
rsc@ubuntuserver:~$ ls -l /var/www/html/todo-daw02/public_html/
total 8
drwxr-xr-x 2 root root     4096 oct 26 08:56 delimitado
-rw-r--r-- 1  755 www-data  205 oct 19 07:06 index.html
rsc@ubuntuserver:~$
```

Paso 5:

> Entramos a la nueva web de delimitado



> Una vez hecho el login



Configurar los archivos de registro como sigue:

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

✓ Identificación log de error: daw02-error.log.

✓ Alias logformat: combined

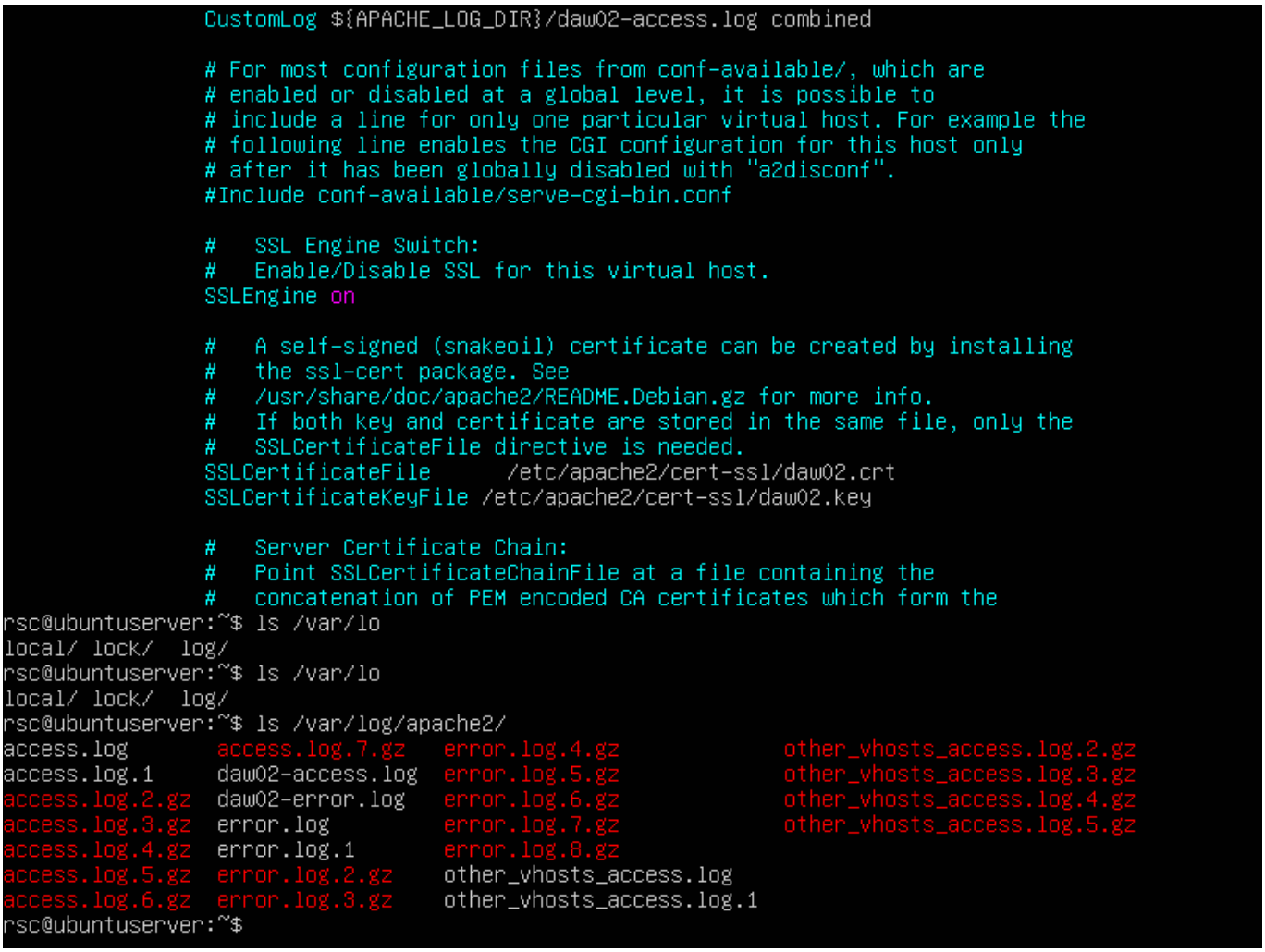
Paso 1:

> Añadimos los logs para daw02 en el archivo -ssl.conf del sitio y reiniciamos el apache.

```
<IfModule mod_ssl.c>
        <VirtualHost *:443>
                DocumentRoot /var/www/html/todo-daw02/public_html
                ServerName daw02.local
                ServerAlias www.daw02.local
                # 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}/daw02-error.log
                CustomLog ${APACHE_LOG_DIR}/daw02-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/apache2/cert-ssl/daw02.crt
                SSLCertificateKeyFile /etc/apache2/cert-ssl/daw02.key

                #   Server Certificate Chain:
                #   Point SSLCertificateChainFile at a file containing the
                #   concatenation of PEM encoded CA certificates which form the
-- INSERTAR --                                                    13,37-51 Comienzo
```

Paso 2:

> Comprobamos que han sido creados.



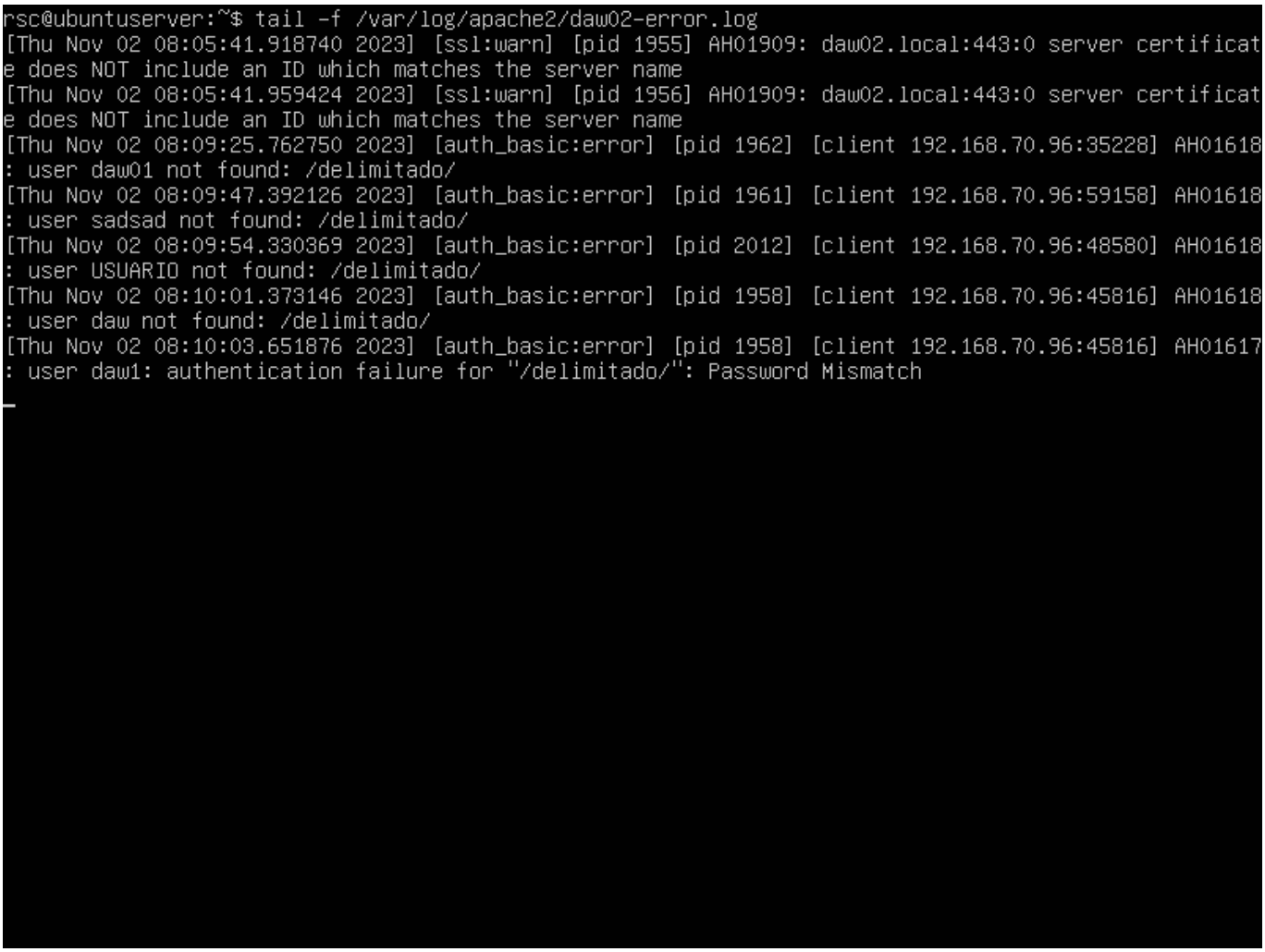
Paso 3:

> Ahora vamos comprobando el log de access en tiempo real con tail -f.

```
                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/apache2/cert-ssl/daw02.crt
                SSLCertificateKeyFile /etc/apache2/cert-ssl/daw02.key

                #   Server Certificate Chain:
                #   Point SSLCertificateChainFile at a file containing the
                #   concatenation of PEM encoded CA certificates which form the
rsc@ubuntuserver:~$ ls /var/lo
local/ lock/  log/
rsc@ubuntuserver:~$ ls /var/lo
local/ lock/  log/
rsc@ubuntuserver:~$ ls /var/log/apache2/
access.log       access.log.7.gz   error.log.4.gz            other_vhosts_access.log.2.gz
access.log.1     daw02-access.log  error.log.5.gz            other_vhosts_access.log.3.gz
access.log.2.gz  daw02-error.log   error.log.6.gz            other_vhosts_access.log.4.gz
access.log.3.gz  error.log         error.log.7.gz            other_vhosts_access.log.5.gz
access.log.4.gz  error.log.1       error.log.8.gz
access.log.5.gz  error.log.2.gz    other_vhosts_access.log
access.log.6.gz  error.log.3.gz    other_vhosts_access.log.1
rsc@ubuntuserver:~$ tail -f /var/log/apache2/daw02-access.log
192.168.70.96 - - [02/Nov/2023:08:08:23 +0000] "GET / HTTP/1.1" 200 2547 "-" "Mozilla/5.0 (X11; Linu
x x86_64; rv:109.0) Gecko/20100101 Firefox/119.0"
192.168.70.96 - - [02/Nov/2023:08:08:23 +0000] "GET /favicon.ico HTTP/1.1" 404 418 "https://daw02.lo
cal/" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/119.0"
192.168.70.96 - - [02/Nov/2023:08:08:23 +0000] "GET / HTTP/1.1" 200 1048 "-" "Mozilla/5.0 (X11; Linu
x x86_64; rv:109.0) Gecko/20100101 Firefox/119.0"
192.168.70.96 - - [02/Nov/2023:08:08:23 +0000] "GET / HTTP/1.1" 200 516 "-" "Mozilla/5.0 (X11; Linux
 x86_64; rv:109.0) Gecko/20100101 Firefox/119.0"
192.168.70.96 - - [02/Nov/2023:08:08:34 +0000] "GET /jaksfja.html HTTP/1.1" 404 950 "-" "Mozilla/5.0
 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/119.0"
```

Paso 4:

> Comprobamos el log de error en tiempo real con tail -f.



5. Rotar logs por intervalo temporal: cada 48 horas

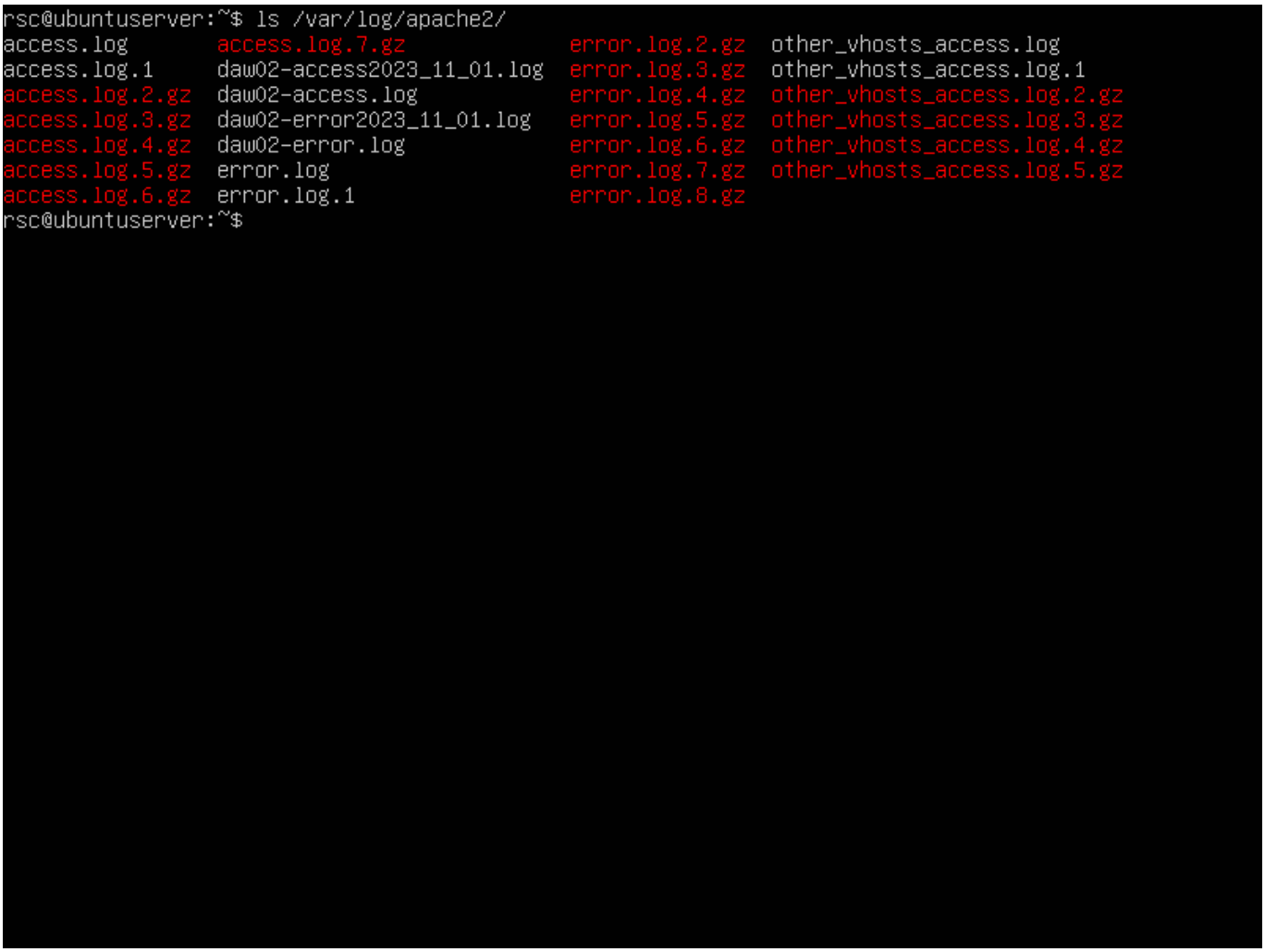
Paso 1:

> Modificamos el -ssl.conf

```
<IfModule mod_ssl.c>
        <VirtualHost *:443>
                DocumentRoot /var/www/html/todo-daw02/public_html
                ServerName daw02.local
                ServerAlias www.daw02.local
                # 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}/daw02-error.log
                #CustomLog ${APACHE_LOG_DIR}/daw02-access.log combined

                CustomLog "|/bin/rotatelogs ${APACHE_LOG_DIR}/daw02-access%Y_%m_%d.log 172800" combi
ned
                ErrorLog "|/bin/rotatelogs ${APACHE_LOG_DIR}/daw02-error%Y_%m_%d.log 172800"

                # 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/apache2/cert-ssl/daw02.crt
                SSLCertificateKeyFile /etc/apache2/cert-ssl/daw02.key
"/etc/apache2/sites-available/daw02-ssl.conf" 142L, 6751B                     16,60-74 Comienzo
```

Paso 2::

> vemos los archivos creados nuevos.


rsc@ubuntuserver:~$ ls /var/log/apache2/
access.log
access.log.1
access.log.2.gz
access.log.3.gz
access.log.4.gz
access.log.5.gz
access.log.6.gz
access.log.7.gz
daw02-access2023_11_01.log
daw02-access.log
daw02-error2023_11_01.log
daw02-error.log
error.log
error.log.1
error.log.2.gz
error.log.3.gz
error.log.4.gz
error.log.5.gz
error.log.6.gz
error.log.7.gz
error.log.8.gz
other_vhosts_access.log
other_vhosts_access.log.1
other_vhosts_access.log.2.gz
other_vhosts_access.log.3.gz
other_vhosts_access.log.4.gz
other_vhosts_access.log.5.gz
rsc@ubuntuserver:~$