

SRI P6 - Unidad de Trabajo 3

Repaso Web

SERVICIOS DE RED E
INTERNET

Cristóbal Suárez Abad
Servicios de Red e Internet – 2º ASIR

Contenido

Introducción:	0
Configurar la IP estática del servidor.....	1
Instalamos Apache:	2
Crea los sitios virtuales prueba.tudominio, test.tutominio, try.tudominio y desactiva la web por defecto.	3
Configura dichos sitios web para que su página índice por defecto sea prueba.html, test.htm y try.php respectivamente.	4
Crea una redirección de /music a <i>simpmusic.org</i> en el tercer sitio web.	10
Indica los módulos estáticos que se han incluido al compilar el servidor Apache2 e Indica los módulos dinámicos que hay habilitados.....	11
Habilita los sitios web de usuarios, crea el usuario prueba, personaliza que la carpeta donde alojar las webs sea webRoot; créale una página personal llamada home.html, y configura en el módulo que home.html sea el índice en las web de usuario y accede a ella para probar que funciona.	13
Cambia el tercer sitio virtual para que se inicie sólo cuando se visita el servidor desde el puerto 88 . Compruébalo.	17
Realiza 10 visitas a las webs creadas. Instala webalizer y analiza los logs del segundo sitio. Hazlos accesibles desde /stats . Aporta captura.....	18
Configura y activa una versión segura del primer sitio con certificados Let's Encrypt obtenidos para tal fin. Aporta captura del acceso mediante https a mismo y de los detalles del certificado mostrados por el navegador Web.	23
En el primer sitio, versión NO segura, haz una redirección permanente al sitio seguro.	27
Realiza lo necesario en el segundo sitio web para que el recurso /marineford (<i>{{siteroot}}/marineford</i>) sólo sea accesible para los usuarios luffy y zoro , con contraseñas a tu elección. Para ello usa el método de autenticación Digest. Es obligatorio usar el fichero .htaccess . Comprueba que se solicita contraseña al acceder vía Web al dicho recurso.....	28
Apéndices:	33
a) Resolver problema de bloqueo de proceso (apt update o install):.....	33
Enlaces:	34
Módulos:	35

Introducción:

Repaso de la Unidad Web. Realiza en AWS:

Crea los sitios virtuales [prueba.tudominio](#), [test.tutominio](#), [try.tudominio](#) y desactiva la web por defecto.

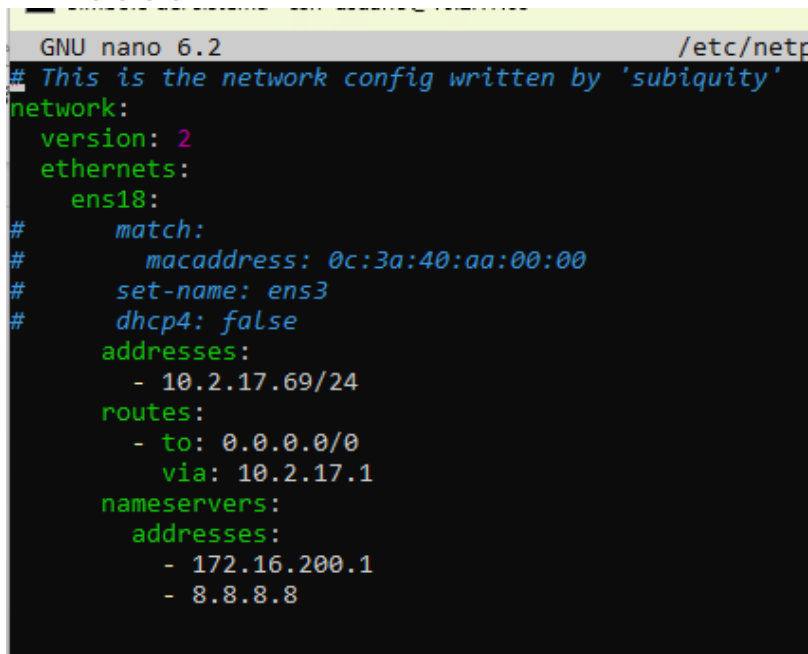
1. Configura dichos sitios web para que su **página índice** por defecto sea *prueba.html*, *test.htm* y *try.php* respectivamente.
2. Crea una redirección de */music* a [simpmusic.org](#) en el tercer sitio web.
3. Indica los módulos estáticos que se han incluido al compilar el servidor Apache2 e Indica los módulos dinámicos que hay habilitados.
4. Habilita los **sitios web de usuarios**, crea el usuario **prueba**, personaliza que la carpeta donde alojar las webs sea **webRoot**; créale una página personal llamada **home.html**, y configura en el módulo que **home.html** sea el índice en las web de usuario y accede a ella para probar que funciona.
5. Cambia el tercer sitio virtual para que se inicie sólo cuando se visita el servidor desde el **puerto 88**. Compruébalo.
6. Realiza 10 visitas a las webs creadas. Instala **webalizer** y analiza los logs del segundo sitio. Hazlos accesibles desde [/stats](#) . Aporta captura.
7. Configura y activa una versión segura del primer sitio con certificados **Let's Encrypt** obtenidos para tal fin. Aporta captura del acceso mediante https a mismo y de los detalles del certificado mostrados por el navegador Web.
8. En el primer sitio, versión NO segura, haz una redirección permanente al sitio seguro.
9. Realiza lo necesario en el segundo sitio web para que el recurso **/marineford** (**{siteroot}/marineford**) sólo sea accesible para los usuarios **luffy** y **zoro**, con contraseñas a tu elección. Para ello usa el método de [autenticación Digest](#). Es obligatorio usar el fichero [.htaccess](#).¹ Comprueba que se solicita contraseña al acceder vía Web al dicho recurso.

¹ Mira la directiva Allowoverride dentro de Directory

Configurar la IP estática del servidor.

`nano /etc/netplan/00-installer-config.yaml`

```
network:
  version: 2
  ethernets:
    ens18:
#   match:
#     macaddress: 0c:3a:40:aa:00:00
#   set-name: ens3
#   dhcp4: false
  addresses:
    - 10.2.17.69/24
  routes:
    - to: 0.0.0.0/0
      via: 10.2.17.1
  nameservers:
    addresses:
      - 172.16.200.1
      - 8.8.8.8
```

A screenshot of a terminal window with a dark background. The title bar at the top shows 'GNU nano 6.2' on the left and '/etc/netp' on the right. The main content of the terminal is a YAML configuration file for netplan. The text is color-coded: green for keywords like 'network:', 'ethernets:', 'addresses:', 'routes:', and 'nameservers:'; blue for comments starting with '#'; and black for values and list items. The configuration sets a static IP of 10.2.17.69/24 for interface ens18, adds a default route via 10.2.17.1, and sets DNS servers to 172.16.200.1 and 8.8.8.8. A comment at the top reads '# This is the network config written by \'subiquity\''.

```
GNU nano 6.2 /etc/netp
# This is the network config written by 'subiquity'
network:
  version: 2
  ethernets:
    ens18:
#   match:
#     macaddress: 0c:3a:40:aa:00:00
#   set-name: ens3
#   dhcp4: false
  addresses:
    - 10.2.17.69/24
  routes:
    - to: 0.0.0.0/0
      via: 10.2.17.1
  nameservers:
    addresses:
      - 172.16.200.1
      - 8.8.8.8
```

`netplan apply`

Instalamos Apache:

apt update

apt install apache2 -y

systemctl status apache2

Comprobar puertos:

ss -ltnp | grep 80

ss -ltnp | grep apache

Comprobar versión:

apache2 -v

Crea los sitios virtuales [prueba.tudominio](#), [test.tutominio](#), [try.tudominio](#) y desactiva la web por defecto.

Comprobamos que sitios web están activos y los desactivamos.

```
Tu Nombre  jueves  6 noviembre 2025 15:45
[root@server2asir usuario]$cd /etc/apache2/
Tu Nombre  jueves  6 noviembre 2025 15:46
[root@server2asir apache2]$ls -l sites-enabled/
total 0
lrwxrwxrwx 1 root root 35 nov  6 15:44 000-default.conf -> ../sites-available/000-
default.conf
Tu Nombre  jueves  6 noviembre 2025 15:46
[root@server2asir apache2]$_
```

a2dissite 000-default.conf

systemctl reload apache2

```
ERROR: Site sites-enabled/000-default does not exist.
Tu Nombre  jueves  6 noviembre 2025 15:47
[root@server2asir apache2]$a2dissite 000-default.conf
Site 000-default disabled.
To activate the new configuration, you need to run:
  systemctl reload apache2
Tu Nombre  jueves  6 noviembre 2025 15:48
[root@server2asir apache2]$_
```

Configura dichos sitios web para que su página índice por defecto sea prueba.html, test.htm y try.php respectivamente.

Generamos los archivos de configuración de cada uno de los sitios virtuales:

```
Símbolo del sistema - ssh usuario@10.2.17.69
Tu Nombre jueves 6 noviembre 2025 15:48
[root@server2asir apache2]$cd sites-available/
Tu Nombre jueves 6 noviembre 2025 15:49
[root@server2asir sites-available]$ls -l
total 12
-rw-r--r-- 1 root root 1332 mar 18 2024 000-default.conf
-rw-r--r-- 1 root root 6338 mar 18 2024 default-ssl.conf
Tu Nombre jueves 6 noviembre 2025 15:49
[root@server2asir sites-available]$cp 000-default.conf prueba.initiald.conf
Tu Nombre jueves 6 noviembre 2025 15:49
[root@server2asir sites-available]$cp 000-default.conf test.initiald.conf
Tu Nombre jueves 6 noviembre 2025 15:49
[root@server2asir sites-available]$cp 000-default.conf try.initiald.conf
Tu Nombre jueves 6 noviembre 2025 15:49
[root@server2asir sites-available]$ls -l
total 24
-rw-r--r-- 1 root root 1332 mar 18 2024 000-default.conf
-rw-r--r-- 1 root root 6338 mar 18 2024 default-ssl.conf
-rw-r--r-- 1 root root 1332 nov 6 15:49 prueba.initiald.conf
-rw-r--r-- 1 root root 1332 nov 6 15:49 test.initiald.conf
-rw-r--r-- 1 root root 1332 nov 6 15:49 try.initiald.conf
Tu Nombre jueves 6 noviembre 2025 15:49
[root@server2asir sites-available]$_
```

- Configuración inicial básica de “prueba.initiald”.

```
GNU nano 6.2 prueba.initiald.conf
<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
    DocumentRoot /var/www/prueba.initiald
    DirectoryIndex prueba.html
    ServerName www.prueba.initiald.com
```

- Configuración inicial básica de “test.initiald”.

```
GNU nano 6.2 test.initiald.conf
<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
    DocumentRoot /var/www/test.initiald
    DirectoryIndex test.htm_
    ServerName www.test.initiald.com
```

- Configuración inicial básica de “try.initiald”.

```
GNU nano 6.2 try.initiald.conf
<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
    DocumentRoot /var/www/try.initiald_
    DirectoryIndex try.php
    ServerName www.try.initiald.com
```

- Ejemplo:

ServerAdmin webmaster@localhost
DocumentRoot /var/www/prueba.initiald
DirectoryIndex prueba.html
ServerName www.prueba.initiald.com

Creamos los directorios:

```
[root@server2asir sites-available]$cd /var/www/
Tu Nombre  jueves  6 noviembre 2025 16:05
[root@server2asir www]$mkdir prueba.initiald test.initiald try.initiald
Tu Nombre  jueves  6 noviembre 2025 16:06
[root@server2asir www]$ls -l
total 16
drwxr-xr-x 2 root root 4096 nov  6 15:44 html
drwxr-xr-x 2 root root 4096 nov  6 16:06 prueba.initiald
drwxr-xr-x 2 root root 4096 nov  6 16:06 test.initiald
drwxr-xr-x 2 root root 4096 nov  6 16:06 try.initiald
Tu Nombre  jueves  6 noviembre 2025 16:06
```

- Creamos en cada uno de ellos sus páginas índices:
 - o prueba.html:

```
Tu Nombre  jueves  6 noviembre 2025 16:06
[root@server2asir www]$nano prueba.initiald/prueba.html
```

```
GNU nano 6.2 prueba.initiald/prueba.html
<!DOCTYPE html>
<html>
<head>
  <title>prueba.initiald</title>
</head>
<body>
  <h1>Bienvenido a la página de prueba de InitialD.</h1>
</body>
</html>
```

<!DOCTYPE html>

<html>

<head>

<title>prueba.initiald</title>

</head>

<body>

<h1>Bienvenido a la página de prueba de InitialD.</h1>

</body>

</html>

- test.htm

```
Tu Nombre  jueves  6 noviembre 2025 16:14  
[root@server2asir www]$nano test.initiald/test.htm_
```

```
<!DOCTYPE html>  
<html>  
<head>  
  <title>test.initiald</title>  
</head>  
<body>  
  <h1>Esta es la pagina de test de InitialD.</h1>  
</body>  
</html>
```

```
GNU nano 6.2 test.initiald/test.htm  
<!DOCTYPE html>  
<html>  
<head>  
  <title>test.initiald</title>  
</head>  
<body>  
  <h1>Esta es la página de test de InitialD.</h1>  
</body>  
</html>
```

- try.php

```
Tu Nombre  jueves  6 noviembre 2025 16:16  
[root@server2asir www]$nano try.initiald/try.php_
```

```
GNU nano 6.2 try.initiald/try.php  
<?php  
  echo "página "try" de InitialD.";
```

```
<?php  
  echo "Página try de InitialD.";
```

Activamos las páginas:

a2ensite prueba.initiald.conf

a2ensite test.initiald.conf

a2ensite try.initiald.conf

Y recargamos las configuración

systemctl reload apache2

systemctl status apache2

En esta ocasión, en el archivo “C:\Windows\System32\drivers\etc\hosts” debemos introducir la resolución de direcciones:

```
# REDES - Practica 6 WEB
10.2.17.69 www.prueba.initiald.com
10.2.17.69 www.test.initiald.com
10.2.17.69 www.try.initiald.com
```

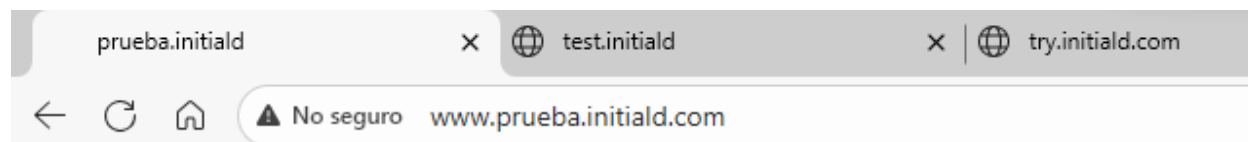
10.2.17.69 www.prueba.initiald.com

10.2.17.69 www.test.initiald.com

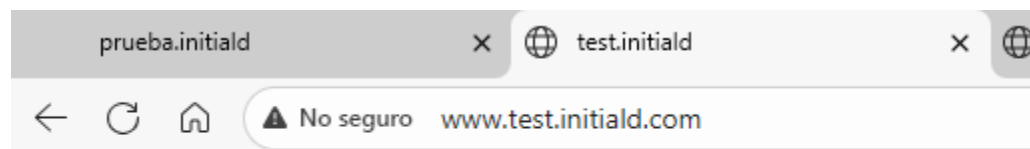
10.2.17.69 www.try.initiald.com

NOTA: para que se vea la PHP necesitas instalar un módulo.

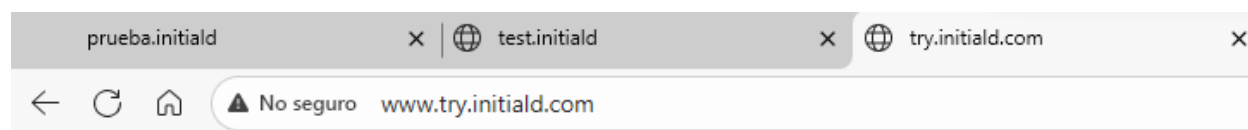
apt install php libapache2-mod-php -y



Bienvenido a la pagina de prueba de InitialD.



Esta es la pagina de test de InitialD.

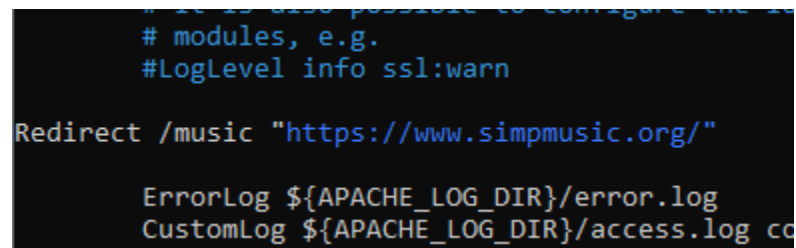


página try de InitialD.

Crea una redirección de */music* a [simpmusic.org](https://www.simpmusic.org/) en el tercer sitio web.

nano try.initiald.conf

Redirect /music "https://www.simpmusic.org/"

A screenshot of a terminal window showing the nano text editor editing the file try.initiald.conf. The editor's content includes a comment about modules, a LogLevel setting, a Redirect directive for /music to https://www.simpmusic.org/, and the start of ErrorLog and CustomLog directives. The text is displayed in a monospaced font with syntax highlighting: comments are green, directives are blue, and file paths are yellow.

```
# It is also possible to configure the 1
# modules, e.g.
#LogLevel info ssl:warn

Redirect /music "https://www.simpmusic.org/"

ErrorLog ${APACHE_LOG_DIR}/error.log
CustomLog ${APACHE_LOG_DIR}/access.log co
```

Y hacemos “**systemctl reload apache2**”.

Si ponemos ahora <http://www.try.initiald.com/music> en el navegador, nos redirigirá a el enlace de “simpmusic”.

Indica los módulos estáticos que se han incluido al compilar el servidor Apache2 e
Indica los módulos dinámicos que hay habilitados.

Módulos estáticos: “**apache2 -l**” o “**apachectl -l**”.

```
Tu Nombre  jueves  6 noviembre 2025 16:44
[root@server2asir apache2]$apache2 -l
Compiled in modules:
  core.c
  mod_so.c
  mod_watchdog.c
  http_core.c
  mod_log_config.c
  mod_logio.c
  mod_version.c
  mod_unixd.c
Tu Nombre  jueves  6 noviembre 2025 16:54
[root@server2asir apache2]$_
```

```
Tu Nombre  viernes  7 noviembre 2025 17:53
[root@server2asir usuario]$apachectl -l
Compiled in modules:
  core.c
  mod_so.c
  mod_watchdog.c
  http_core.c
  mod_log_config.c
  mod_logio.c
  mod_version.c
  mod_unixd.c
Tu Nombre  viernes  7 noviembre 2025 17:54
```

Módulos dinámicos habilitados: **apachectl -M**

```
Tu Nombre viernes 7 noviembre 2025 18:07
root@server2asir apache2]$apachectl -M
AH00558: apache2: Could not reliably determine
'Name' directive globally to suppress this message
Loaded Modules:
core_module (static)
so_module (static)
watchdog_module (static)
http_module (static)
log_config_module (static)
logio_module (static)
version_module (static)
unixd_module (static)
access_compat_module (shared)
alias_module (shared)
auth_basic_module (shared)
auth_digest_module (shared)
authn_core_module (shared)
authn_file_module (shared)
authz_core_module (shared)
authz_host_module (shared)
authz_user_module (shared)
autoindex_module (shared)
deflate_module (shared)
dir_module (shared)
env_module (shared)
filter_module (shared)
mime_module (shared)
mpm_prefork_module (shared)
negotiation_module (shared)
```

También podríamos hacer un “**ls -l**” en las carpetas “**mods-available**” y “**mods-enabled**” para ver que mods están disponibles y habilitados.

Habilita los sitios web de usuarios, crea el usuario prueba, personaliza que la carpeta donde alojar las webs sea webRoot; créale una página personal llamada home.html, y configura en el módulo que home.html sea el índice en las web de usuario y accede a ella para probar que funciona.

a) Crea el usuario prueba:

adduser prueba

```
[root@server2asir apache2]$adduser prueba
Adding user `prueba' ...
Adding new group `prueba' (1001) ...
Adding new user `prueba' (1001) with group `prueba' ...
Creating home directory `/home/prueba' ...
Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for prueba
Enter the new value, or press ENTER for the default
    Full Name []:
    Room Number []:
    Work Phone []:
    Home Phone []:
    Other []:
Is the information correct? [Y/n] y
Tu Nombre  jueves  6 noviembre 2025 16:55
[root@server2asir apache2]$
```

b) Personaliza que la carpeta donde alojar las webs sea webRoot.

Primero debemos activar el módulo “**userdir**”.

sudo a2enmod userdir

sudo systemctl restart apache2

```
Tu Nombre  jueves  6 noviembre 2025 16:55
[root@server2asir apache2]$a2enmod userdir
Enabling module userdir.
To activate the new configuration, you need to run:
    systemctl restart apache2
Tu Nombre  jueves  6 noviembre 2025 17:01
[root@server2asir apache2]$systemctl restart apache2
Tu Nombre  jueves  6 noviembre 2025 17:01
```


Creamos la carpeta dentro del directorio de trabajo del usuario.

```
sudo mkdir /home/prueba/webRoot
```

```
sudo chown -R prueba:prueba /home/prueba/webRoot
```

```
Tu Nombre jueves 6 noviembre 2025 17:04
[root@server2asir apache2]$sudo mkdir /home/prueba/webRoot
Tu Nombre jueves 6 noviembre 2025 17:04
[root@server2asir apache2]$ls -l /home/prueba/webRoot/
total 0
Tu Nombre jueves 6 noviembre 2025 17:05
[root@server2asir apache2]$ls -l /home/prueba/
total 4
drwxr-xr-x 2 root root 4096 nov  6 17:04 webRoot
Tu Nombre jueves 6 noviembre 2025 17:05
[root@server2asir apache2]$sudo chown -R prueba:prueba /home/prueba/webRoot
Tu Nombre jueves 6 noviembre 2025 17:05
[root@server2asir apache2]$ls -l /home/prueba/
total 4
drwxr-xr-x 2 prueba prueba 4096 nov  6 17:04 webRoot
Tu Nombre jueves 6 noviembre 2025 17:05
[root@server2asir apache2]$
```

Le configuramos un archivo “prueba.html”.

```
Tu Nombre jueves 6 noviembre 2025 17:34
[root@server2asir apache2]$nano /home/prueba/webRoot/home.html
```

```
<!DOCTYPE html>
<HTML>
  <head>
    <title>Web del usuario Prueba</title>
  </head>
  <body>
    <div id="una capa">
      <h1>Hola mundo, soy Prueba!</h1>
      <p>Este es un ejemplo del uso de HTML para crear un documento web que nuest>
    </div>
  </body>
</HTML>
```

Modificamos el archivo del módulo para que “**home.html**” sea el índice en las webs de usuario y también para que sepa que tiene que buscarlo en la carpeta webRoot.

nano mods-available/userdir.conf

```
Tu Nombre  jueves  6 noviembre 2025 17:19
[root@server2asir apache2]$ nano mods-available/userdir.conf
```

En nuestro caso, comentamos las líneas que tienen “**public_html**” y las reemplazamos con “**webRoot**”. Además, debemos introducir la línea “**DirectoryIndex home.html**”.

```
GNU nano 6.2      mods-available/userdir.conf
<IfModule mod_userdir.c>
#   UserDir public_html
   UserDir webRoot
   UserDir disabled root

#   <Directory /home/*/public_html>
   <Directory /home/*/webRoot>
       DirectoryIndex home.html
       AllowOverride FileInfo AuthConfig Limit Indexes
       Options MultiViews Indexes SymLinksIfOwnerMatch IncludesNoExec
       Require method GET POST OPTIONS
   </Directory>
</IfModule>

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
```

NOTA: hay que darle permisos al usuario de apache2 para que pueda ejecutar en el directorio de trabajo del usuario:

chmod o+x /home/prueba/

chmod o+x /home/prueba/webRoot/

chown -R www-data:www-data /home/prueba/webRoot/*

```

[root@server2asir apache2]$ls -l /home/prueba/webRoot/
total 4
-rw-r--r-- 1 www-data www-data 311 nov  6 17:19 home.html
  Tu Nombre  jueves  6 noviembre 2025 17:37
[root@server2asir apache2]$chmod o+x /home/prueba/webRoot/
  Tu Nombre  jueves  6 noviembre 2025 17:38
[root@server2asir apache2]$chmod o+x /home/prueba/
  Tu Nombre  jueves  6 noviembre 2025 17:38
[root@server2asir apache2]$ls -l /home/prueba/
total 4
drwxr-xr-x 2 prueba prueba 4096 nov  6 17:34 webRoot
  Tu Nombre  jueves  6 noviembre 2025 17:39
[root@server2asir apache2]$ls -l /home/prueba/webRoot/
total 4
-rw-r--r-- 1 www-data www-data 311 nov  6 17:19 home.html
  Tu Nombre  jueves  6 noviembre 2025 17:39
[root@server2asir apache2]$chmod o+x /home/prueba/webRoot/*
  Tu Nombre  jueves  6 noviembre 2025 17:40
[root@server2asir apache2]$ls -l /home/prueba/webRoot/
total 4
-rw-r--r-x 1 www-data www-data 311 nov  6 17:19 home.html
  Tu Nombre  jueves  6 noviembre 2025 17:40
[root@server2asir apache2]$_

```

Accedemos usando la virgullita: <http://www.try.initiald.com/~prueba/>

<http://www.prueba.initiald.com/~prueba/>

<http://www.test.initiald.com/~prueba/>



Hola mundo, soy Prueba!

Este es un ejemplo del uso de HTML para crear un documento web que nuestro navegador es capaz de interpretar.

Cambia el tercer sitio virtual para que se inicie sólo cuando se visita el servidor desde el **puerto 88**. Compruébalo.

nano sites-available/try.initiald.conf

```
GNU nano 6.2 sites-available/try.initiald.conf *
<VirtualHost *:88>
    # The ServerName directive sets the request scheme, hostna
    # the server name to identify itself. This is used when a
```

Y ahora el archive “ports.conf” de la configuración general de Apache.

nano ports.conf

```
# /etc/apache2/ports.conf

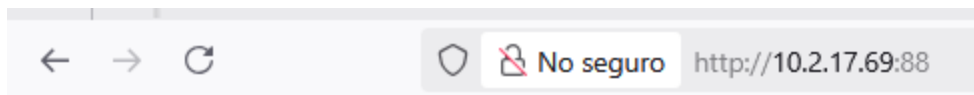
Listen 80
Listen 88_
# IfModule ssl_module
```

Se añade, no se reemplaza.

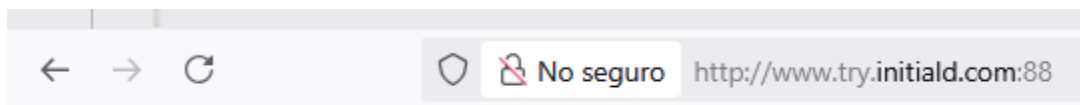
systemctl restart apache2

Abrir puerto 88:

sudo ufw allow 88/tcp



página try de InitialD.



página try de InitialD.

Realiza 10 visitas a las webs creadas. Instala **webalizer** y analiza los logs del segundo sitio. Hazlos accesibles desde [/stats](#) . Aporta captura.

Hay que instalarlo donde está el servidor apache2

apt -y install webalizer

Creamos copia solo para “test.initiald”.

cp /etc/webalizer/webalizer.conf.sample /etc/webalizer/webalizer.test.initiald.conf

nano /etc/webalizer/webalizer.test.initiald.conf

Introducimos:

LogFile /var/log/apache2/test.initiald-access.log

OutputDir /var/www/test.initiald/stats

ReportTitle Webalizer para www.test.initiald.com

HostName www.test.initiald.com

```
OutputDir       /var/www/test.initiald/stats_
```

```
# is being read.
```

```
LogFile         /var/log/apache2/test.initiald-access.log
```

```
# LogType defines the log type being processed.  Normally, t
```

```
ReportTitle     Webalizer para www.test.initiald.com_
```

```
HostName        www.test.initiald.com_
```

```
# HTMLExtension allows you to specify th
```

Ahora debemos modificar el archivo de configuración del virtualhost para crear “logs” específicos de la página, en vez de los generales de Apache.

```
ErrorLog ${APACHE_LOG_DIR}/test.initiald.error.log
CustomLog /var/log/apache2/test.initiald-access.log combined
```

También debemos crear un Alias para poder entrar.

Alias /stats/ "/var/www/test.initiald/stats/"

<Directory "/var/www/test.initiald/stats/">

Options Indexes FollowSymLinks

AllowOverride None

Require all granted

</Directory>

```
Alias /stats/ "/var/www/test.initiald/stats/"

<Directory "/var/www/test.initiald/stats/">
Options Indexes FollowSymLinks
AllowOverride None
Require all granted
</Directory>
```

Y también hacer un **systemctl restart apache2**.

También creamos el directorio:

mkdir /var/www/test.initiald/stats

Vamos a usar el siguiente comando para configurar que Webalizer realice un análisis todos los días.

crontab -e

Elegimos un editor de texto. En nuestro caso el primero, nano.

E introducimos la siguiente línea de código.

```
0 6 * * * /usr/bin/webalizer -c /etc/webalizer/webalizer.test.initiald.conf </dev/null  
2<&1
```

```
[root@server2asir apache2]$ crontab -e
no crontab for root - using an empty one

Select an editor. To change later, run 'select-editor'.
 1. /bin/nano          <---- easiest
 2. /usr/bin/vim.basic
 3. /usr/bin/vim.tiny
 4. /bin/ed

Choose 1-4 [1]: 1

# m h dom mon dow   command
0 6 * * * /usr/bin/webalizer -c /etc/webalizer/webalizer.test.initiald.conf </dev/null 2<&1_
```

Una vez que guardemos y salgamos de “**nano**”, nos debe aparecer este mensaje:

```
no crontab for root - using an empty one
crontab: installing new crontab
```

Esto significa que el “crontab” se ha instalado con éxito.

Comando para hacer 10 visitas en la página web.

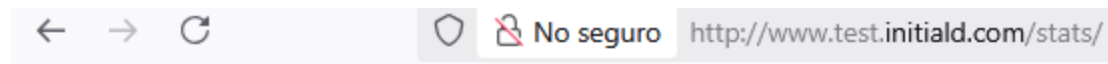
```
for i in {1..10}; do curl -s http://www.test.initiald.com > /dev/null; done
```

Forzar a webalizer a que analice los blogs.









```
sudo webalizer -c /etc/webalizer/webalizer.test.initiald.conf
```

```
Tu Nombre jueves 6 noviembre 2025 18:23
[root@server2asir apache2]$sudo webalizer -c /etc/webalizer/webalizer.test.initiald.conf
Webalizer V2.23-08 (Linux 5.15.0-94-generic x86_64) locale: es7XU
Utilizando histórico /var/log/apache2/test.initiald-access.log (clf)
Creando informe en /var/www/test.initiald/stats
El nombre de máquina en el informe es 'www.test.initiald.com'
Leyendo archivo... webalizer.hist
Generando informe de Noviembre 2025
Guardando información de archivo...
Generando informe resumido
24 registros en 1 segundos, 24/sec
Tu Nombre jueves 6 noviembre 2025 18:23
```

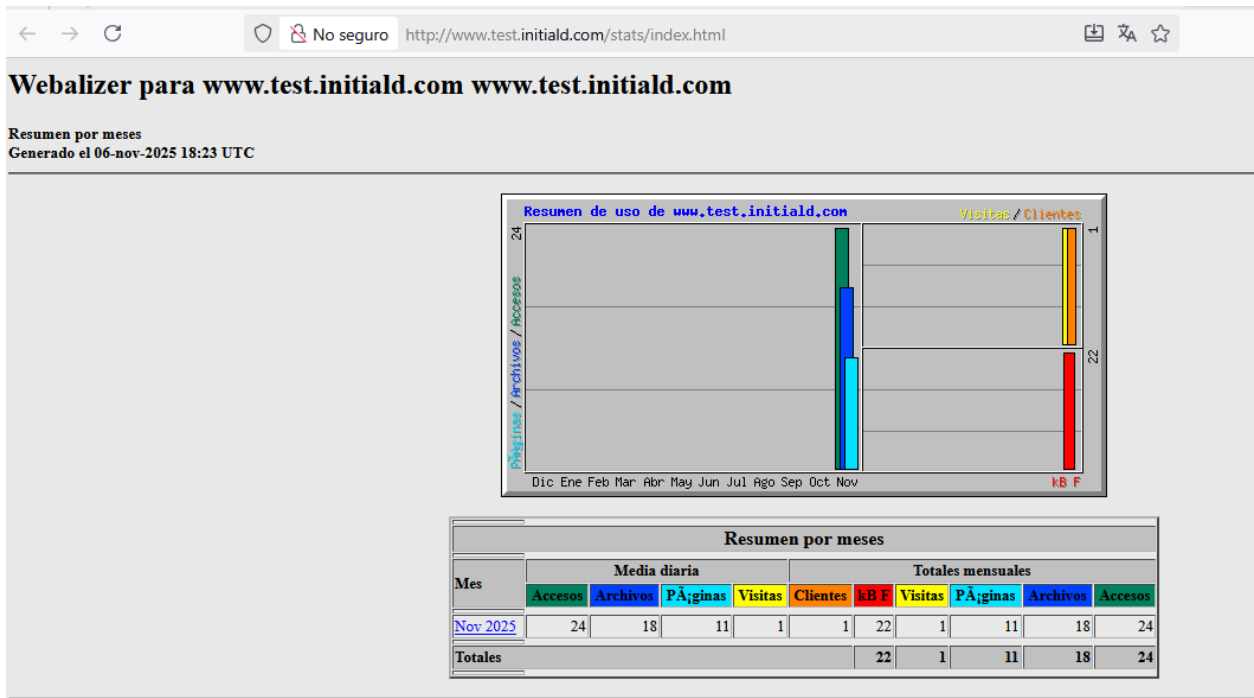
<http://www.test.initiald.com/stats/>



Index of /stats

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory		-	
 ctry_usage_202511.png	2025-11-06 18:22	2.6K	
 daily_usage_202511.png	2025-11-06 18:22	2.6K	
 hourly_usage_202511.png	2025-11-06 18:22	1.7K	
 index.html	2025-11-06 18:22	3.6K	
 usage.png	2025-11-06 18:22	2.2K	
 usage_202511.html	2025-11-06 18:22	33K	
 webalizer.hist	2025-11-06 18:22	3.3K	

Apache/2.4.52 (Ubuntu) Server at www.test.initiald.com Port 80



Configura y activa una versión segura del primer sitio con certificados Let's Encrypt obtenidos para tal fin. Aporta captura del acceso mediante https a mismo y de los detalles del certificado mostrados por el navegador Web.

Nos posicionamos en la carpeta de “**mods-available**” de apache2.

cd mods-available/

Ejecutamos: **a2enmod ssl**

systemctl restart apache2

```
Símbolo del sistema - ssh usuario@10.2.17.69
Tu Nombre  jueves  6 noviembre 2025 18:23
[root@server2asir apache2]$cd mods-available/
Tu Nombre  jueves  6 noviembre 2025 18:29
[root@server2asir mods-available]$a2enmod ssl
Considering dependency setenvif for ssl:
Module setenvif already enabled
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for ssl:
Enabling module socache_shmcb.
Enabling module ssl.
See /usr/share/doc/apache2/README.Debian.gz on how to configure SSL and create self-signed certificates.
To activate the new configuration, you need to run:
    systemctl restart apache2
Tu Nombre  jueves  6 noviembre 2025 18:30
[root@server2asir mods-available]$_
```

-rw-r--r--	1	root	root	78	mar 18	2024	socache_shmcb.load
-rw-r--r--	1	root	root	66	mar 18	2024	speling.load
-rw-r--r--	1	root	root	3110	mar 18	2024	ssl.conf
-rw-r--r--	1	root	root	97	mar 18	2024	ssl.load
-rw-r--r--	1	root	root	749	mar 18	2024	status.conf
-rw-r--r--	1	root	root	64	mar 18	2024	status.load

Ahora vamos al directorio “**/etc/ssl/private/**”.

Vamos a generar nuestro propio certificado:

openssl genrsa 2048 > prueba.initiald.ssl.key

```
Tu Nombre  jueves  6 noviembre 2025 18:32
[root@server2asir private]$openssl genrsa 2048 > prueba.initiald.ssl.key
Tu Nombre  jueves  6 noviembre 2025 18:33
[root@server2asir private]$ls -l
total 8
-rw-r--r-- 1 root root 1704 nov  6 18:33 prueba.initiald.ssl.key
-rw-r----- 1 root ssl-cert 1704 nov  6 15:44 ssl-cert-snakeoil.key
Tu Nombre  jueves  6 noviembre 2025 18:33
[root@server2asir private]$_
```

Ahora vamos al directorio **/etc/ssl/certs/**

Allí ejecutamos el siguiente comando para generar el **“.pem”**

openssl req -new -key ../private/prueba.initiald.ssl.key -x509 -days 365 -out

/etc/ssl/certs/prueba.initiald.ssl.pem

```
Tu Nombre  jueves  6 noviembre 2025 18:36
[root@server2asir certs]$openssl req -new -key ../private/prueba.initiald.ssl.key
-x509 -days 365 -out /etc/ssl/certs/prueba.initiald.ssl.pem
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:ES
State or Province Name (full name) [Some-State]:Huelva
Locality Name (eg, city) []:La Palma del Condado
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Mi Casa
Organizational Unit Name (eg, section) []:Mi cuarto
Common Name (e.g. server FQDN or YOUR name) []:initiald
Email Address []:pakkieressaberexojajaja
Tu Nombre  jueves  6 noviembre 2025 18:37
[root@server2asir certs]$
```

Antes de nada. La configuración de los permisos de los archivos **“.pem”** y **“.key”**.

El archivo **“.pem”** puede quedarse con la configuración que aparece en la imagen, que es con la que viene por defecto.

Usaríamos:

chown root:root /etc/ssl/certs/NOMBRE_ARCHIVO.pem

chmod 644 /etc/ssl/certs/NOMBRE_ARCHIVO.pem

```
[root@server2asir apache2]$ls -l /etc/ssl/certs/ | grep initial
lrwxrwxrwx 1 root root    23 nov  7 12:26 40af839b.0 -> prueba.initiald.ssl.pem
-rw-r--r-- 1 root root 1489 nov  6 18:37 prueba.initiald.ssl.pem
```

Pero el archivo “.key” se guarda por defecto con una configuración que puede dar problemas.

```
[root@server2asir apache2]$ls -l /etc/ssl/private/prueba.initiald.ssl.key
-rw-r--r-- 1 root root 1704 nov  6 18:33 /etc/ssl/private/prueba.initiald.ssl.key
Tu Nombre viernes 7 noviembre 2025 18:42
```

Para cambiarla usamos los siguientes comandos:

chown root:ssl-cert /etc/ssl/private/NOMBRE_ARCHIVO.key

chmod 640 /etc/ssl/private/NOMBRE_ARCHIVO.key

```
[root@server2asir apache2]$ls -l /etc/ssl/private/prueba.initiald.ssl.key
-rw-r----- 1 root ssl-cert 1704 nov  6 18:33 /etc/ssl/private/prueba.initiald.ssl.key
Tu Nombre viernes 7 noviembre 2025 18:48
```

Ahora volvemos a /etc/apache2/sites-available/ y creamos una copia del “default-ssl.conf”.

cp sites-available/default-ssl.conf sites-available/prueba.initiald-ssl.conf

nano sites-available/prueba.initiald-ssl.conf

Ahora modificamos el archivo. Mantén el cabecero igual y modifica solo lo que has introducido en el archivo “prueba.initiald.conf”.

```
GNU nano 6.2 sites-available/prueba.initiald-ssl.conf
<IfModule mod_ssl.c>
    <VirtualHost _default_:443>
        ServerAdmin webmaster@localhost

        DocumentRoot /var/www/prueba.initiald
        DirectoryIndex prueba.html
        ServerName www.prueba.initiald.com
        # Available loglevels: trace8, ..., trace1, debug, info, notice, warn, error, crit,
        # ...
```

Buscamos la línea de certificados y especificamos la ruta donde están los dos certificados (key y pem) que hemos creado previamente.

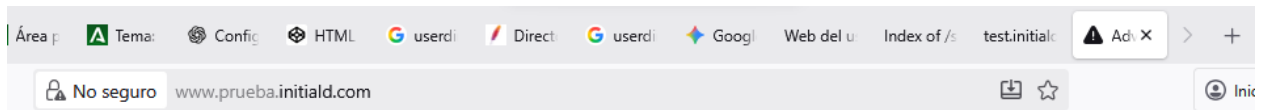
```
# SSLCertificateFile directive is needed.
SSLCertificateFile /etc/ssl/certs/prueba.initiald.ssl.pem
SSLCertificateKeyFile /etc/ssl/private/prueba.initiald.ssl_key
```

Una vez termines la configuración, debes habilitar el sitio con “**a2ensite**”. Después reiniciar el servicio.

```
[root@server2asir apache2]$ Tu Nombre jueves 6 noviembre 2025 18:44
[root@server2asir apache2]$ a2ensite prueba.initiald-ssl.conf
Enabling site prueba.initiald-ssl.
To activate the new configuration, you need to run:
    systemctl reload apache2
Tu Nombre jueves 6 noviembre 2025 18:44
[root@server2asir apache2]$ systemctl reload apache2
Tu Nombre jueves 6 noviembre 2025 18:44
[root@server2asir apache2]$ systemctl status apache2
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; enabled; ver
   Active: active (running) since Thu 2025-11-06 18:16:06 UTC; 28min
   Docs: https://httpd.apache.org/docs/2.4/
   Process: 12059 ExecReload=/usr/sbin/apachectl graceful (code=exite
   Main PID: 11700 (apache2)
   Tasks: 6 (limit: 3426)
   Memory: 11.2M
   CPU: 589ms
```

<https://www.prueba.initiald.com/>

Aceptamos los riesgos y seguimos.



Advertencia: riesgo potencial de seguridad a continuación

Firefox ha detectado una posible amenaza de seguridad y no ha cargado **www.prueba.initiald.com**. Si visita este sitio, los atacantes podrían intentar robar información como sus contraseñas, correos electrónicos o detalles de su tarjeta de crédito.

[Más información...](#)

Retroceder (recomendado)

Avanzado...

En el primer sitio, versión NO segura, haz una redirección permanente al sitio seguro.

En la configuración “http” del primer sitio ponemos²:

Redirect permanent / <https://www.prueba.initiald.com/>

```
ServerAdmin webmaster@localhost
DocumentRoot /var/www/prueba.initiald
DirectoryIndex prueba.html
ServerName www.prueba.initiald.com
Redirect permanent / https://www.prueba.initiald.com/
```

systemctl reload apache2

Y en teoría, cuando pongas en el navegador www.prueba.initiald.com te redirige a la versión https.

NOTA: ten cuidado, porque si el navegador ya conoce la “http”, puede que no haga el cambio.

² <https://linuxize.com/post/redirect-http-to-https-in-apache/>

Realiza lo necesario en el segundo sitio web para que el recurso */marineford* (*{siteroot}/marineford*) sólo sea accesible para los usuarios *luffy* y *zoro*, con contraseñas a tu elección. Para ello usa el método de [autenticación Digest](#). Es obligatorio usar el fichero [.htaccess](#).³ Comprueba que se solicita contraseña al acceder vía Web al dicho recurso.

Es como “Configurar la Zona Privada” de la práctica de IAW. Pero la configuración del VirtualHost se pone en el archivo “.htaccess”.

Instalamos el módulo:

sudo a2enmod auth_digest

systemctl restart apache2

```
Tu Nombre jueves 6 noviembre 2025 19:01
[root@server2asir apache2]$sudo a2enmod auth_digest
Considering dependency authn_core for auth_digest:
Module authn_core already enabled
Enabling module auth_digest.
To activate the new configuration, you need to run:
  systemctl restart apache2
Tu Nombre jueves 6 noviembre 2025 19:01
[root@server2asir apache2]$systemctl restart apache2
Tu Nombre jueves 6 noviembre 2025 19:01
[root@server2asir apache2]$_
```

Vamos a crear la carpeta:

sudo mkdir /var/www/test.initiald/marineford

```
Tu Nombre jueves 6 noviembre 2025 19:01
[root@server2asir apache2]$sudo mkdir /var/www/test.initiald/marineford
Tu Nombre jueves 6 noviembre 2025 19:02
[root@server2asir apache2]$ls -l /var/www/test.initiald/
total 12
drwxr-xr-x 2 root root 4096 nov  6 19:02 marineford
drwxr-xr-x 2 root root 4096 nov  6 18:23 stats
-rw-r--r-- 1 root root 142 nov  6 16:42 test.htm
Tu Nombre jueves 6 noviembre 2025 19:03
[root@server2asir apache2]$_
```

³ Mira la directiva Allowoverride dentro de Directory

Creamos un documento "html".

```
GNU nano 6.2 /var/www/test.initiald/marineford/index.html
<!DOCTYPE html>
<HTML>
  <head>
    <title>Marineford</title>
  </head>
  <body>
    <div id="una capa">
      <h1>Marineford: Fortaleza de la Justicia</h1>
      <p>El arco argumental, llamado la Guerra de Marineford, es una saga crucial</p>
    </div>
  </body>
</HTML>
```

Creamos el archivo donde se guardarán las claves.

sudo htdigest -c .test.initiald "Thousand Sunny" luffy

sudo htdigest .test.initiald "Thousand Sunny" zoro

```
Tu Nombre jueves 6 noviembre 2025 19:13
[root@server2asir apache2]$sudo htdigest -c .test.initiald "Thousand Sunny" luffy
Adding password for luffy in realm Thousand Sunny.
New password:
Re-type new password:
Tu Nombre jueves 6 noviembre 2025 19:15
[root@server2asir apache2]$sudo htdigest .test.initiald "Thousand Sunny" zoro
Adding user zoro in realm Thousand Sunny
New password:
Re-type new password:
Tu Nombre jueves 6 noviembre 2025 19:15
[root@server2asir apache2]$
```

```
Tu Nombre jueves 6 noviembre 2025 19:15
[root@server2asir apache2]$cat .test.initiald
luffy:Thousand Sunny:01516f166c151e3474a69e12d999c297
zoro:Thousand Sunny:5e3872b52c0ba20931238fd605216c06
Tu Nombre jueves 6 noviembre 2025 19:15
[root@server2asir apache2]$
```


Crea el archivo “.htaccess” dentro de la carpeta “marineford”.

nano /var/www/test.initiald/marineford/.htaccess

```
GNU nano 6.2 /var/www/test.initiald/marineford/.htaccess
AuthType Digest
AuthName "Thousand Sunny"
AuthUserFile /etc/apache2/.test.initiald
Require user luffy zoro
```

AuthType Digest

AuthName "Thousand Sunny"

AuthUserFile /etc/apache2/.test.initiald

Require user luffy zoro

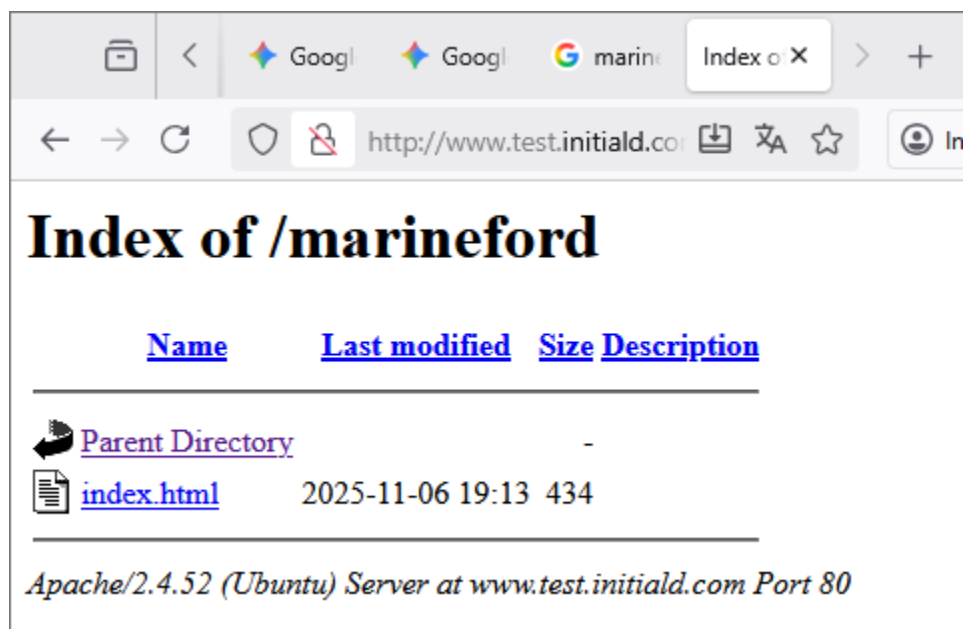
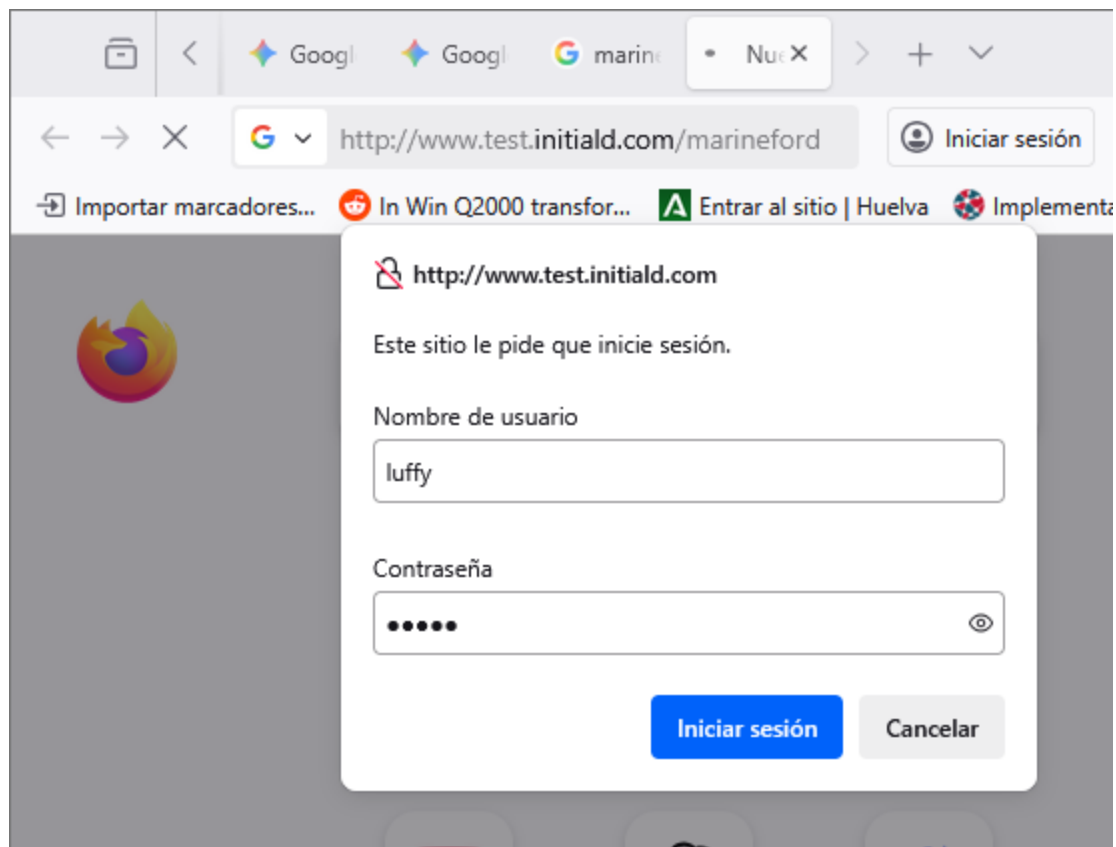
Y ahora debemos ir a la configuración del VirtualHost y permitir que en el directorio “marineford” tenga validez él “.htaccess”.

```
<Directory "/var/www/test.initiald/marineford/">
    AllowOverride All
</Directory>
```

<Directory "/var/www/test.initiald/marineford/">

AllowOverride All

</Directory>

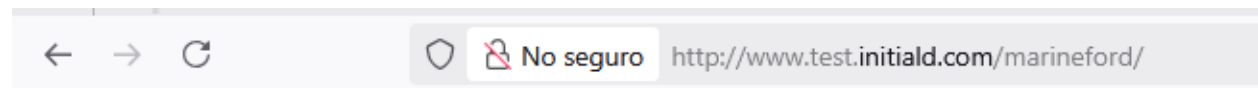


EXTRA: Si en la configuración anterior, queremos que al poner <http://www.test.initiald.com/marineford/> en el navegador cargue directamente el archivo “index.html”, debemos modificar el archivo “.htaccess”. Introducimos un:

DirectoryIndex index.html

```
AuthType Digest
AuthName "Thousand Sunny"
AuthUserFile /etc/apache2/.test.initiald
Require user luffy zoro
DirectoryIndex index.html
```

systemctl reload apache2



Marineford: Fortaleza de la Justicia

El arco argumental, llamado la Guerra de Marineford, es una saga crucial que se centra en el intento Piratas de Barbablanca. .

Apéndices:

a) Resolver problema de bloqueo de proceso (apt update o install):

Kill the offending process:

```
sudo kill 15 2004
```

If the process persists:

```
sudo kill 9 2004
```

Manually Remove the Lock Files (Last Resort):

```
sudo rm /var/lib/dpkg/lock-frontend
```

```
sudo rm /var/lib/dpkg/lock
```

Remove the apt cache lock:

```
sudo rm /var/cache/apt/archives/lock
```

Enlaces:

Directorios web por usuario

https://httpd.apache.org/docs/trunk/es/howto/public_html.html

Autenticación Digest en Apache:

<https://www.zeppelinlinux.es/autenticacion-digest-en-apache/>

Tutorial del Servidor Apache HTTP: Ficheros .htaccess

<https://httpd.apache.org/docs/trunk/es/howto/htaccess.html>

Módulos:

Para mostrar los paquetes disponibles en los repositorios de Ubuntu que permiten instalar módulos adicionales:

sudo apt search libapache2-mod

Para habilitar un módulo:

sudo a2enmod nombre_del_modulo

Para deshabilitar un módulo:

sudo a2dismod nombre_del_modulo

Para que los cambios surtan efecto se debe reiniciar el servidor.