

Abstract geometric lines in the top left corner, consisting of several overlapping, irregular polygons and lines in a light beige color.

PRÁCTICA 4

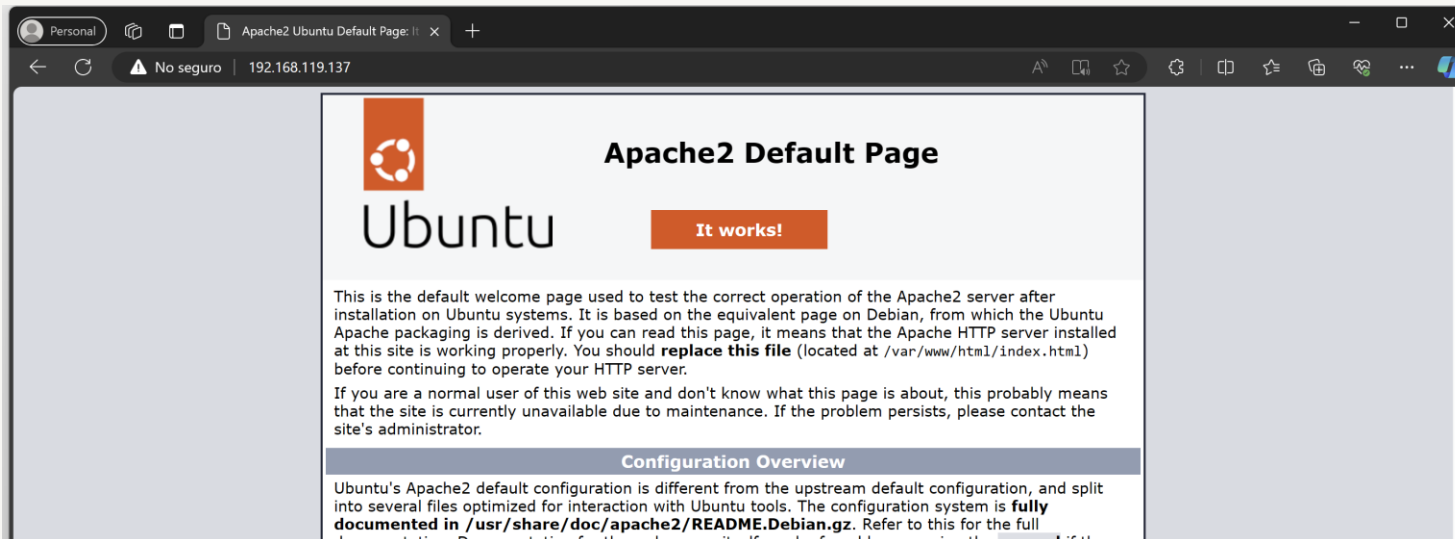
ADMINISTRACIÓN DE SISTEMAS

Paloma Pérez de Madrid Laguna - [http](http://)

1. INSTALAR EL SERVIDOR APACHE EN UNA DISTRIBUCIÓN UBUNTU SERVER 22.

```
root@server:~# apt install apache2
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
  apache2-bin apache2-data apache2-utils libapr1 libaprutil1 libaprutil1-dbd-sqlite3
Paquetes sugeridos:
  apache2-doc apache2-suexec-pristine | apache2-suexec-custom
```

En VM Ubuntu



Verificamos el funcionamiento de Apache buscando la dirección IP de nuestra máquina, apareciendo así la página de bienvenida de Apache

2. VERIFICAR SU CONFIGURACIÓN

Verificar su configuración (archivo `apache2.conf` y directorios `*-enabled`) y modificar alguna de sus directivas para comprobar su funcionamiento (establecer uno o varios puertos de escucha, cambiar la página de inicio predeterminada, utilizar la opción `index` en algún subdirectorio y ver su efecto, apuntar con un `Alias` a otro directorio, usar `Redirect` para redirigir a otro sitio web, etc).

`/etc/apache2/apache2.conf`

```
# Include module configuration:
IncludeOptional mods-enabled/*.load
IncludeOptional mods-enabled/*.conf

# Include list of ports to listen on
Include ports.conf

# Sets the default security model of the Apache2 HTTPD server. It does
# not allow access to the root filesystem outside of /usr/share and /var/www.
# The former is used by web applications packaged in Debian,
# the latter may be used for local directories served by the web server. If
# your system is serving content from a sub-directory in /srv you must allow
# access here, or in any related virtual host.
<Directory />
    Options FollowSymLinks
    AllowOverride None
    Require all denied
</Directory>
|
<Directory /usr/share>
    AllowOverride None
    Require all granted
</Directory>

"/etc/apache2/apache2.conf" 227L, 7224B escritos
```

Directorios `*-enabled`

```
root@server:/etc/apache2# ls
apache2.conf  conf-enabled  magic          mods-enabled  sites-available
conf-available  envvars      mods-available  ports.conf    sites-enabled
```

Sites-enabled: Archivos de configuración de host virtuales que se procesarán
Ahora mismo solo hay el archivo por defecto:
`000-default.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/html

    # 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
</VirtualHost>

#000-default.conf# 311, 1332B
```

2. VERIFICAR SU CONFIGURACIÓN

Directorios *-enabled

```
root@server:/etc/apache2# ls
apache2.conf  conf-enabled  magic          mods-enabled  sites-available
conf-available  envvars      mods-available  ports.conf    sites-enabled
```

mods-enabled: configuraciones concretas (autenticación, seguridad, ...)

```
root@server:/etc/apache2/mods-enabled# ls
access_compat.load  authn_file.load  autoindex.load  env.load  mpm_event.load  setenvif.conf
alias.conf          authz_core.load  deflate.conf     filter.load  negotiation.conf  setenvif.load
alias.load          authz_host.load  deflate.load     mime.conf   negotiation.load  status.conf
auth_basic.load     authz_user.load  dir.conf        mime.load   reqtimeout.conf   status.load
authn_core.load     autoindex.conf   dir.load        mpm_event.conf  reqtimeout.load
```

conf-enabled: configuraciones globales que afectan a todos los host virtuales

```
root@server:/etc/apache2/conf-enabled# ls
charset.conf  localized-error-pages.conf  other-vhosts-access-log.conf  security.conf  serve-cgi-bin.conf
root@server:/etc/apache2/conf-enabled#
```

2. VERIFICAR SU CONFIGURACIÓN

Modificación de los archivos de *-enabled

Establecer varios puertos de escucha
(apache2.conf)

```
Include ports.conf
```

ports.conf → Listen puerto 8080

```
Listen 80
Listen 8080
|
<IfModule ssl_module>
    Listen 443
</IfModule>

<IfModule mod_gnutls.c>
    Listen 443
</IfModule>

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

Cambiar Página predeterminada

- Añadimos la directiva DirectoryIndex (primero buscará indexPaloma.html)

```
<Directory /var/www/>
    Options Indexes FollowSymLinks
    AllowOverride None
    Require all granted
    DirectoryIndex indexPaloma.html index.html
</Directory>
```

- Creamos /var/www/html/indexPaloma.html
- Para comprobar que funciona → IP en el navegador de la máquina principal



The screenshot shows a web browser window with the address bar displaying '192.168.119.137'. The page content is a contact form titled 'Servidor Paloma de Ubuntu'. The form includes a 'Contacto' section with a message: 'Por favor, contactanos si tienes alguna pregunta o comentario:'. Below this are three input fields: 'Nombre' (with placeholder 'Tu nombre'), 'Correo electrónico' (with placeholder 'tucorreo@ejemplo.com'), and 'Mensaje'. A blue 'Enviar' button is at the bottom of the form. Below the form is a link that says 'Iniciar Sesión'.

2. VERIFICAR SU CONFIGURACIÓN

Modificación de los archivos de *-enabled

Utilizar opción indexes en algún directorio

- Creamos un subdirectorio
/var/www/html/paloma.com/
- Creo diferentes archivos (que no sean HTML) para poder hacer un Index.

```
root@server:/var/www/html/paloma.com# ls
archivoPaloma.PDF  archivoPaloma.txt  hola.py  pagWeb
```

(los HTML irán en pagWeb)

- Creamos una directiva en apache2.conf de paloma.com

```
<Directory /var/www/html/paloma.com>
Options Indexes
AllowOverride None
Require all granted
</Directory>
```

- Borramos el indexPaloma.html como DirectoryIndex en las directivas superiores

```
<Directory /var/www/>
Options Indexes FollowSymLinks
AllowOverride None
Require all granted
DirectoryIndex index.html
</Directory>
```

← ↻ ⚠ No seguro | 192.168.119.137/paloma.com/

Index of /paloma.com

	Name	Last modified	Size	Description
🔙	Parent Directory		-	
📄	archivoPaloma.PDF	2024-03-14 06:08	28	
📄	archivoPaloma.txt	2024-03-14 06:07	52	
📄	hola.py	2024-03-14 06:08	35	
📁	pagWeb/	2024-03-14 05:57	-	

Apache/2.4.52 (Ubuntu) Server at 192.168.119.137 Port 80

3. CONFIGURACIÓN DE SERVIDORES VIRTUALES

Crear varios directorios bajo el directorio /var/projects, que servirán de punto de entrada para nuestros servidores virtuales (ubicados en /var/projects/server1, /var/projects/server2, /var/projects/miempresa.com, /var/projects/otraempresa.com, ...). Añadir en estos directorios al menos una página de inicio (index.html) con algún texto significativo (“Servidor de miempresa.com”, “Servidor web 1”, ...).

```
root@server:~# mkdir /var/projects
root@server:~# mkdir /var/projects/server1
root@server:~# mkdir /var/projects/server2
root@server:~# mkdir /var/projects/miempresa.com
root@server:~# mkdir /var/projects/otraempresa.com
root@server:~#
```

```
root@server:/var/projects/server1# ls
index.html
```

```
root@server:/var/projects/miempresa.com# ls
index.html
```

```
root@server:/var/projects/otraempresa.com# ls
index.html
```

```
root@server:/var/projects/server2# ls
index.html
```

3. CONFIGURACIÓN DE SERVIDORES VIRTUALES

Las tres configuraciones que se indican a continuación pueden realizarse de forma independiente (no es necesario combinarlas).

Nota: Usaremos archivos .conf en sites-available para los servidores virtuales, con enlaces simbólicos desde sites-enabled (a2ensite/a2dissite)

Servidores virtuales basados en puerto.

Configurar la escucha del servidor web en tres puertos (80, 2020 y 2080). Cada uno de ellos permitirá acceder a un servidor virtual diferente (los puntos de entrada que hemos creado previamente). El primero de ellos (en el puerto 80) puede utilizar la configuración del servidor principal. Los otros tendrán que configurarse como servidores virtuales.

Creamos archivos serverX.conf en /etc/apache2/sites-available

```
<VirtualHost *:80>
    ServerAdmin webmaster@localhost
    ServerName www.server1.com
    ServerAlias server1.com
    DocumentRoot /var/projects/server1

    <Directory /var/projects/server1>
        Require all granted
        Options Indexes FollowSymLinks
    </Directory>

    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>
```

server1.conf → copiamos el archivo de 000-default.conf y le pasamos la configuración de server1 (nuestro servidor principal)

3. CONFIGURACIÓN DE SERVIDORES VIRTUALES

Las tres configuraciones que se indican a continuación pueden realizarse de forma independiente (no es necesario combinarlas).

Nota: Usaremos archivos .conf en sites-available para los servidores virtuales, con enlaces simbólicos desde sites-enabled (a2ensite/a2dissite)

Servidores virtuales basados en puerto.

En ambos casos hemos añadido las directivas Require y Options

- Require all granted → permite que cualquier usuario tenga acceso completo al directorio y a sus archivos sin ninguna restricción adicional
- FollowSymLinks → permite que Apache siga enlaces simbólicos dentro del directorio especificado. (importante para poder crear un enlace simbólico a la carpeta site-enable)

Creamos archivos serverX.conf en /etc/apache2/sites-available

```
<VirtualHost *:2020>
    ServerName www.server2.com
    ServerAlias server2.com
    DocumentRoot /var/projects/server2

    <Directory /var/projects/server2>
        Require all granted
        # Options Indexes FollowSymLinks
        Options FollowSymLinks
        # DirectoryIndex /var/projects/server2/index.html
    </Directory>
</VirtualHost>
```

server2conf

Desactivamos archivo de configuración predeterminado

```
root@server:/etc/apache2/sites-available# a2dissite 000-default.conf
Site 000-default disabled.
To activate the new configuration, you need to run:
    systemctl reload apache2
```

3. CONFIGURACIÓN DE SERVIDORES VIRTUALES

Las tres configuraciones que se indican a continuación pueden realizarse de forma independiente (no es necesario combinarlas).

Nota: Usaremos archivos .conf en sites-available para los servidores virtuales, con enlaces simbólicos desde sites-enabled (a2ensite/a2dissite)

Servidores virtuales basados en puerto

Creamos los enlaces a site-enable

```
root@server:/etc/apache2/sites-available# systemctl reload apache2
root@server:/etc/apache2/sites-available# a2ensite server1.conf
Site server1 already enabled
root@server:/etc/apache2/sites-available# a2ensite server2.conf
Enabling site server2.
To activate the new configuration, you need to run:
    systemctl reload apache2
root@server:/etc/apache2/sites-available# systemctl restart apache2
```

Para comprobar su funcionamiento desde la máquina principal (Windows), debemos añadir desde el modo administración la IP de nuestra máquina y añadir los host que acabamos de crear

```
C:\Windows\System32> notepad drivers\etc\hosts
```

```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#       102.54.94.97       rhino.acme.com          # source server
#       38.25.63.10       x.acme.com              # x client host


# localhost name resolution is handled within DNS itself.
#       127.0.0.1         localhost
#       ::1               localhost

192.168.119.137 www.server1.com www.server2.com server1.com server2.com
```

3. CONFIGURACIÓN DE SERVIDORES VIRTUALES

Las tres configuraciones que se indican a continuación pueden realizarse de forma independiente (no es necesario combinarlas).

Nota: Usaremos archivos .conf en sites-available para los servidores virtuales, con enlaces simbólicos desde sites-enabled (a2ensite/a2dissite)

Servidores virtuales basados en puerto

```
Listen 80
Listen 8080
Listen 2020
Listen 2080
```

En /etc/apache2/ports.conf indicamos que también escuche el puerto del servidor2

Tercer Servidor (miempresa.com) :

```
<VirtualHost *:2080>
    ServerName www.miempresa.com
    ServerAlias miempresa.com
    DocumentRoot /var/projects/miempresa.com

    <Directory /var/projects/miempresa.com>
        Require all granted
        Options FollowSymLinks
    </Directory>
</VirtualHost>
```



Server1 - CEU San Pablo

[Acerca de](#) [Contacto](#) [Iniciar Sesión](#)

Acerca de

Bienvenido al servidor Server1, un espacio dedicado a los estudiantes del CEU San Pablo.

Contacto

Para cualquier consulta, puedes contactarnos a través del siguiente correo electrónico: info@server1.com

Iniciar Sesión

Usuario:

Contraseña:

Iniciar Sesión

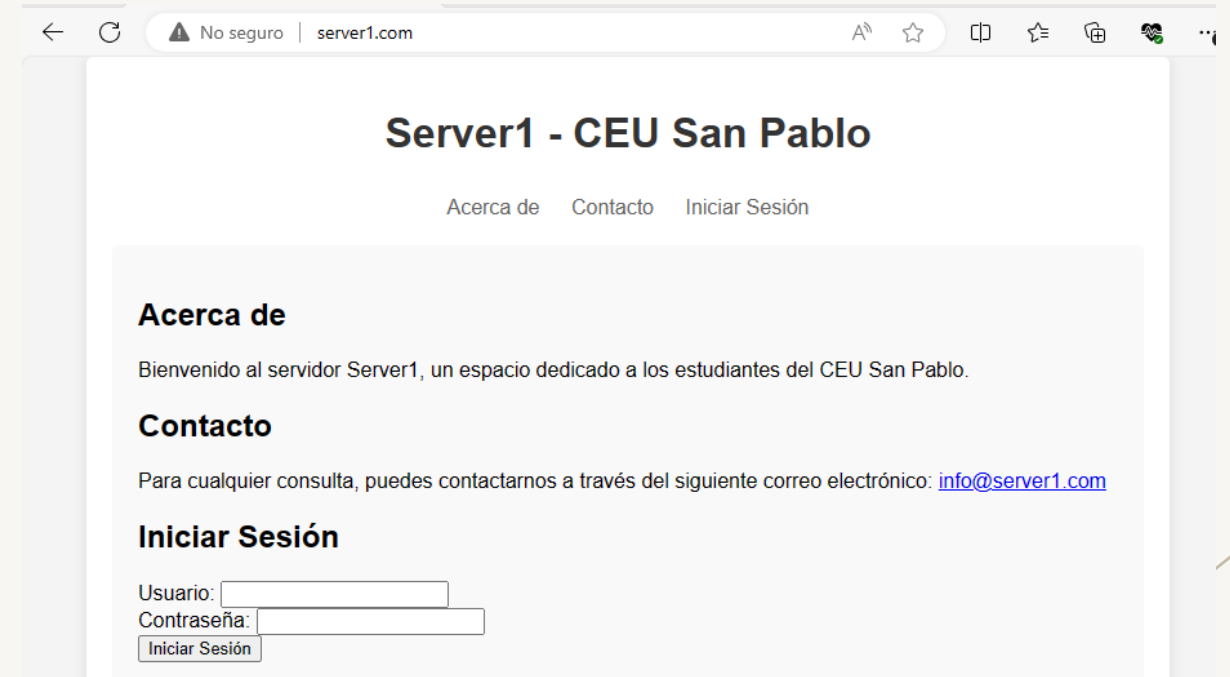
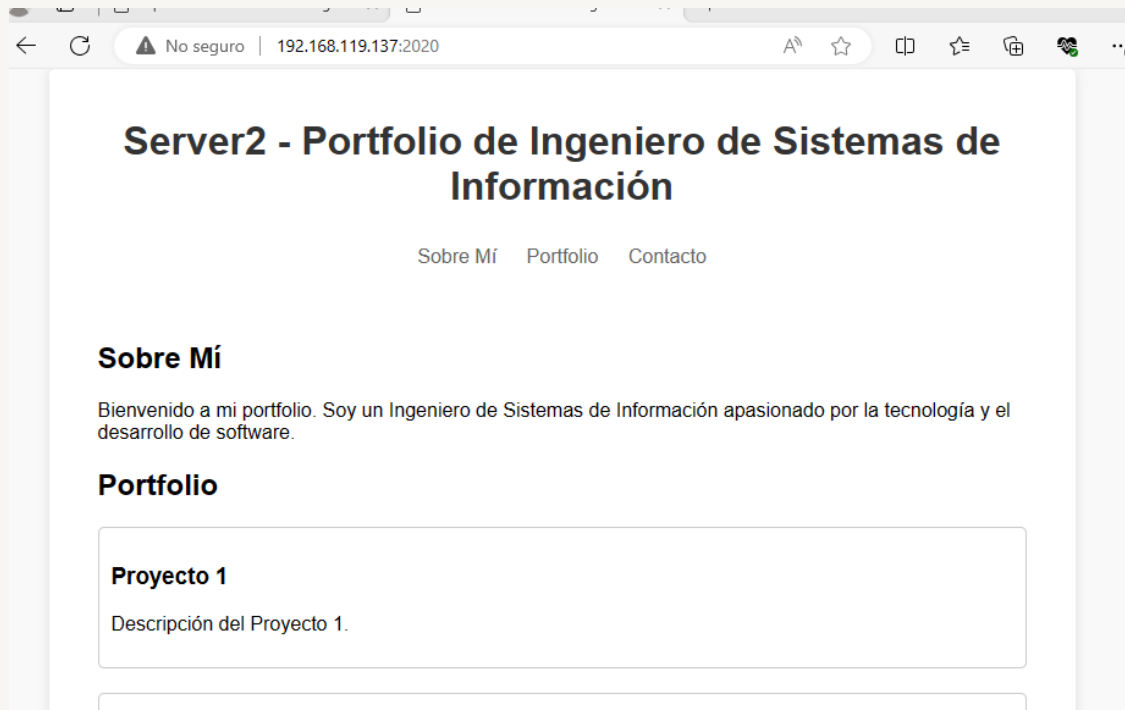
Server1 - CEU San Pablo © 2024

3. CONFIGURACIÓN DE SERVIDORES VIRTUALES

Las tres configuraciones que se indican a continuación pueden realizarse de forma independiente (no es necesario combinarlas).

Nota: Usaremos archivos .conf en sites-available para los servidores virtuales, con enlaces simbólicos desde sites-enabled (a2ensite/a2dissite)

Servidores virtuales basados en puerto



3. CONFIGURACIÓN DE SERVIDORES VIRTUALES

Las tres configuraciones que se indican a continuación pueden realizarse de forma independiente (no es necesario combinarlas).

Nota: Usaremos archivos .conf en sites-available para los servidores virtuales, con enlaces simbólicos desde sites-enabled (a2ensite/a2dissite)

Servidores virtuales basados en dirección IP.

Asocie una segunda dirección IP al interface eth0 de su equipo. Verifique con un comando ping lanzado desde el exterior que la nueva dirección IP está visible en la red. A continuación, configure un servidor virtual asociado a la nueva dirección IP (use como punto de entrada uno de los directorios creados previamente). Los accesos por la dirección inicial seguirán siendo atendidos por el servidor principal. En ambos casos se utilizará el puerto 80

```
root@server:~# vim /etc/netplan/00-installer-config.yaml
root@server:~# netplan apply
```

```
network:
  version: 2
  ethernets:
    eth0:
      addresses:
        - 192.168.119.137/24 # Dirección IP principal
        - 192.168.119.200/24 # Segunda dirección IP
      gateway4: 192.168.119.1 # Puerta de enlace predeterminada
      nameservers:
        addresses: [8.8.8.8, 8.8.4.4] # Servidores DNS
```

3. CONFIGURACIÓN DE SERVIDORES VIRTUALES

Las tres configuraciones que se indican a continuación pueden realizarse de forma independiente (no es necesario combinarlas).

Nota: Usaremos archivos .conf en sites-available para los servidores virtuales, con enlaces simbólicos desde sites-enabled (a2ensite/a2dissite)

Verifique con un comando ping lanzado desde el exterior que la nueva dirección IP está visible en la red

```
root@server:~# ip addr show eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:4f:4d:2f brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    altname ens33
    inet 192.168.119.137/24 brd 192.168.119.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet 192.168.119.200/24 brd 192.168.119.255 scope global secondary eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe4f:4d2f/64 scope link
        valid_lft forever preferred_lft forever
```

Máquina Ubuntu

Máquina Principal (Windows, exterior)

```
C:\Users\ppere>ping 192.168.119.200
```

```
Haciendo ping a 192.168.119.200 con 32 bytes de datos:
Respuesta desde 192.168.119.200: bytes=32 tiempo=1ms TTL=64
Respuesta desde 192.168.119.200: bytes=32 tiempo=1ms TTL=64
Respuesta desde 192.168.119.200: bytes=32 tiempo=2ms TTL=64
Respuesta desde 192.168.119.200: bytes=32 tiempo=1ms TTL=64
```

```
Estadísticas de ping para 192.168.119.200:
```

```
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
              (0% perdidos),
```

```
Tiempos aproximados de ida y vuelta en milisegundos:
```

```
    Mínimo = 1ms, Máximo = 2ms, Media = 1ms
```

```
C:\Users\ppere>ping 192.168.119.137
```

```
Haciendo ping a 192.168.119.137 con 32 bytes de datos:
Respuesta desde 192.168.119.137: bytes=32 tiempo=3ms TTL=64
Respuesta desde 192.168.119.137: bytes=32 tiempo=1ms TTL=64
Respuesta desde 192.168.119.137: bytes=32 tiempo=2ms TTL=64
Respuesta desde 192.168.119.137: bytes=32 tiempo=2ms TTL=64
```

```
Estadísticas de ping para 192.168.119.137:
```

```
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
              (0% perdidos),
```

```
Tiempos aproximados de ida y vuelta en milisegundos:
```

```
    Mínimo = 1ms, Máximo = 3ms, Media = 2ms
```

3. CONFIGURACIÓN DE SERVIDORES VIRTUALES

Las tres configuraciones que se indican a continuación pueden realizarse de forma independiente (no es necesario combinarlas).

A continuación, configure un servidor virtual asociado a la nueva dirección IP (use como punto de entrada uno de los directorios creados previamente). Los accesos por la dirección inicial seguirán siendo atendidos por el servidor principal. En ambos casos se utilizará el puerto 80

```
root@server:/etc/apache2/sites-available# vim miempresa.com.conf
root@server:/etc/apache2/sites-available# systemctl restart apache2
root@server:/etc/apache2/sites-available# a2ensite miempresa.com.conf
Enabling site miempresa.com.
To activate the new configuration, you need to run:
    systemctl reload apache2
root@server:/etc/apache2/sites-available# systemctl restart apache2
```

```
<VirtualHost 192.168.119.200:80>
    ServerName www.miempresa.com
    ServerAlias miempresa.com
    DocumentRoot /var/projects/miempresa.com

    <Directory /var/projects/miempresa.com>
        Require all granted
        Options Indexes FollowSymLinks
    </Directory>
</VirtualHost>
```

/etc/apache2/sites-available/miempresa.com.conf
(Lo añadimos al archivo hosts de Windows)

3. CONFIGURACIÓN DE SERVIDORES VIRTUALES

Las tres configuraciones que se indican a continuación pueden realizarse de forma independiente (no es necesario combinarlas).

Nota: Usaremos archivos .conf en sites-available para los servidores virtuales, con enlaces simbólicos desde sites-enabled (a2ensite/a2dissite)

192.168.119.200:80 , comprobación de miempresa.com mediante la IP



3. CONFIGURACIÓN DE SERVIDORES VIRTUALES

Las tres configuraciones que se indican a continuación pueden realizarse de forma independiente (no es necesario combinarlas).

Servidores virtuales basados en nombres.

Ahora todas las peticiones se recibirán por la dirección IP principal y el puerto 80. Las peticiones dirigidas a miempresa.com (puede ir o no precedido por www.) utilizarán como punto de entrada el directorio /var/projects/miempresa.com, y lo mismo para las dirigidas a otraempresa.com (a su directorio asociado). Si se reciben peticiones dirigidas a otros dominios, o a través de la dirección IP principal, se devolverá una página en blanco.

3. CONFIGURACIÓN DE SERVIDORES VIRTUALES

Las tres configuraciones que se indican a continuación pueden realizarse de forma independiente (no es necesario combinarlas).

Servidores virtuales basados en nombres.

/etc/apache2/sites-available/miempresa.com.conf

```
<VirtualHost *:80>
    ServerName www.miempresa.com
    ServerAlias miempresa.com
    DocumentRoot /var/projects/miempresa.com

    <Directory /var/projects/miempresa.com>
        Require all granted
        Options FollowSymLinks
    </Directory>
</VirtualHost>
```

/etc/apache2/sites-available/otraempresa.com.conf

```
<VirtualHost *:80>
    ServerName www.otraempresa.com
    ServerAlias otraempresa.com
    DocumentRoot /var/projects/otraempresa.com

    <Directory /var/projects/otraempresa.com>
        Require all granted
        Options Indexes FollowSymLinks
    </Directory>
</VirtualHost>
```

3. CONFIGURACIÓN DE SERVIDORES VIRTUALES

Las tres configuraciones que se indican a continuación pueden realizarse de forma independiente (no es necesario combinarlas).

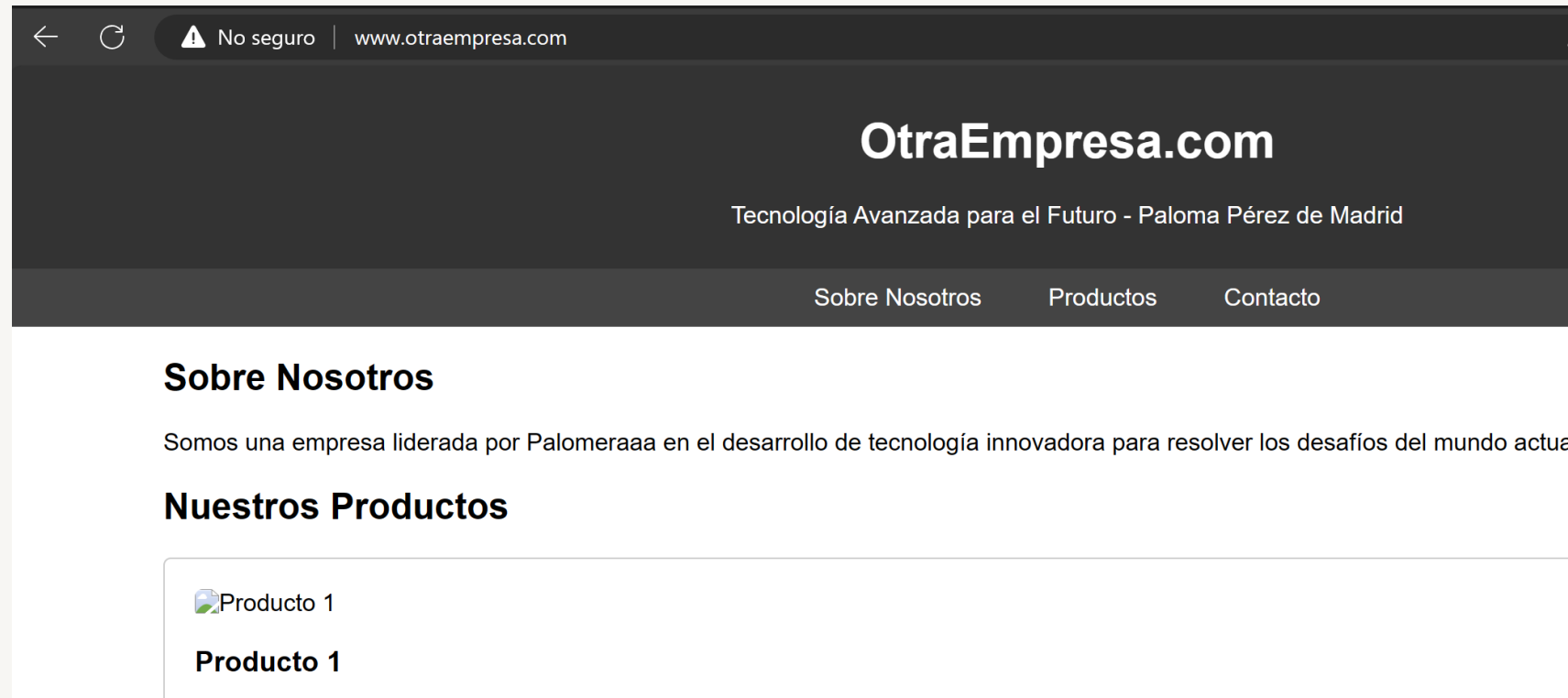
Servidores virtuales basados en nombres



3. CONFIGURACIÓN DE SERVIDORES VIRTUALES

Las tres configuraciones que se indican a continuación pueden realizarse de forma independiente (no es necesario combinarlas).

Servidores virtuales basados en nombres.



4. REGISTRO DE ACCESOS AL SERVIDOR (LOGS)

Estudiar el formato de las directivas LogFormat, CustomLog, ErrorLog y LogLevel. Almacenar de forma independiente los archivos de logs del servidor virtual empresa.com configurado en el apartado anterior, y verificar la función de alguna de las opciones de LogFormat.

Log Files - Apache HTTP Server Version 2.4

- LogFormat: Define el formato del registro de acceso.
- CustomLog: Especifica la ubicación y el formato del registro de acceso personalizado.
- ErrorLog: Define la ubicación del archivo de registro de errores.
- LogLevel: Define el nivel de detalle de los mensajes de error que se registrarán.

```
root@server:/var/log# ls
alternatives.log      cloud-init.log        faillog               syslog.1              vmware-network.5.log
alternatives.log.1    cloud-init-output.log installer             syslog.2.gz           vmware-network.6.log
apache2               dist-upgrade          journal              syslog.3.gz           vmware-network.7.log
apt                   dmesg                kern.log             ubuntu-advantage.log  vmware-network.8.log
auth.log              dmesg.0              kern.log.1           ubuntu-advantage.log.1 vmware-network.9.log
auth.log.1            dmesg.1.gz           kern.log.2.gz        ubuntu-advantage-timer.log vmware-network.log
auth.log.2.gz         dmesg.2.gz           kern.log.3.gz        unattended-upgrades   vmware-vmtoolsd-root.1.log
auth.log.3.gz         dmesg.3.gz           landscape            vmware-network.1.log  vmware-vmtoolsd-root.2.log
bootstrap.log         dmesg.4.gz           lastlog              vmware-network.2.log  vmware-vmtoolsd-root.log
btmtp                 dpkg.log              private              vmware-network.3.log  vmware-vmtoolsd-root.log
btmtp.1               dpkg.log.1            syslog               vmware-network.4.log  wtmp
```

Los logs se encuentran en la carpeta /var/log

4. REGISTRO DE ACCESOS AL SERVIDOR (LOGS)

Estudiar el formato de las directivas LogFormat, CustomLog, ErrorLog y LogLevel. Almacenar de forma independiente los archivos de logs del servidor virtual empresa.com configurado en el apartado anterior, y verificar la función de alguna de las opciones de LogFormat.

Almacenamiento de archivos de logs de empresa.com

- ErrorLog → log donde guarda los errores
- CustomLog → define el archivo de registro de acceso personalizado para el servidor virtual especificado.

```
<VirtualHost 192.168.119.200:80>
  ServerName www.miempresa.com
  ServerAlias miempresa.com
  DocumentRoot /var/projects/miempresa.com

  ErrorLog ${APACHE_LOG_DIR}/miempresa_error.log
  CustomLog ${APACHE_LOG_DIR}/miempresa_access.log combined

  <Directory /var/projects/miempresa.com>
    Require all granted
  </Directory>
</VirtualHost>
```

/etc/apache2/sites-available/miempresa.com.conf

4. REGISTRO DE ACCESOS AL SERVIDOR (LOGS)

Estudiar el formato de las directivas LogFormat, CustomLog, ErrorLog y LogLevel. Almacenar de forma independiente los archivos de logs del servidor virtual empresa.com configurado en el apartado anterior, y verificar la función de alguna de las opciones de LogFormat.

Almacenamiento de archivos de logs de empresa.com → COMPROBACIÓN

1) Definir un formato de registro personalizado en el archivo de configuración de miempresa.com

```
LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\"" custom_format
```

- `%h`: La dirección IP del cliente que hizo la solicitud.
- `%l`: El identificador remoto del cliente, que generalmente es un guion (`-`) para indicar que no está disponible.
- `%u`: El usuario remoto, si está disponible.
- `%t`: La marca de tiempo de la solicitud.
- `\"%r\"`: La línea de solicitud (método, URL y versión de HTTP) entre comillas dobles.
- `%>s`: El código de estado de la respuesta HTTP.
- `%b`: El tamaño de la respuesta en bytes, excluyendo los encabezados.
- `\"%{Referer}i\"`: El referente HTTP entre comillas dobles.
- `\"%{User-Agent}i\"`: El agente de usuario (navegador web) entre comillas dobles.

4. REGISTRO DE ACCESOS AL SERVIDOR (LOGS)

Estudiar el formato de las directivas LogFormat, CustomLog, ErrorLog y LogLevel. Almacenar de forma independiente los archivos de logs del servidor virtual empresa.com configurado en el apartado anterior, y verificar la función de alguna de las opciones de LogFormat.

Almacenamiento de archivos de logs de empresa.com → COMPROBACIÓN

- 2) Añadimos la directiva CustomLog → especificar el archivo de registro y el formato personalizado que se utilizará para registrar los eventos de acceso para el servidor virtual asociado a miempresa.com

```
CustomLog /var/log/apache2/miempresa.com_access.log custom_format
```

- 3) Buscar miempresa.com o 192.168.119.200 desde otro navegador y comprobar que /var/log/apache2/miempresa.com_Access.log lo registra

```
0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.0.0 Safari/537.36 Edg/122.0.0.0"
192.168.119.1 - - [14/Mar/2024:18:32:12 +0000] "GET /worker2.jpg HTTP/1.1" 404 277 "http://192.168.119.200/" "Mozilla/5.
0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.0.0 Safari/537.36 Edg/122.0.0.0"
192.168.119.1 - - [14/Mar/2024:18:32:14 +0000] "GET / HTTP/1.1" 200 1548 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.0.0 Safari/537.36 Edg/122.0.0.0"
192.168.119.1 - - [14/Mar/2024:18:32:14 +0000] "GET /worker1.jpg HTTP/1.1" 404 277 "http://192.168.119.200/" "Mozilla/5.
0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.0.0 Safari/537.36 Edg/122.0.0.0"
192.168.119.1 - - [14/Mar/2024:18:32:14 +0000] "GET /worker2.jpg HTTP/1.1" 404 277 "http://192.168.119.200/" "Mozilla/5.
0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.0.0 Safari/537.36 Edg/122.0.0.0"
192.168.119.1 - - [14/Mar/2024:18:32:14 +0000] "GET /worker3.jpg HTTP/1.1" 404 277 "http://192.168.119.200/" "Mozilla/5.
0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.0.0 Safari/537.36 Edg/122.0.0.0"
192.168.119.1 - - [14/Mar/2024:18:32:17 +0000] "GET / HTTP/1.1" 200 1548 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.0.0 Safari/537.36 Edg/122.0.0.0"
@@@
"/var/log/apache2/miempresa.com_access.log" 17L, 3901B 1,1 Comienzo
```

```
vim /var/log/apache2/miempresa.com_access.log
```



5. ACCESO RESTRINGIDO POR CONTRASEÑA

Proteger el directorio *seguro* que colgará de la raíz del servidor principal (En mi caso, server1). Esté directorio contendrá una página index.html con un mensaje de bienvenida, y será necesario validarse con el usuario alumno, contraseña passceu.

1) Crear archivo .htpasswd

- Creamos la carpeta segura (#mkdir /var/www/server1/seguro)
- Creamos un usuario:
 - o Usuario: usuarioPaloma
 - o Contraseña: usuarioPaloma

```
root@server:/var/projects/server1# vi /etc/apache2/.htpasswd
root@server:/var/projects/server1# cd /etc/apache2/
root@server:/etc/apache2# sudo htpasswd -c .htpasswd usuarioPaloma
New password:
Re-type new password:
Adding password for user usuarioPaloma
```

5. ACCESO RESTRINGIDO POR CONTRASEÑA

Proteger el directorio *seguro* que colgará de la raíz del servidor principal (En mi caso, server1). Esté directorio contendrá una página index.html con un mensaje de bienvenida, y será necesario validarse con el usuario alumno, contraseña passceu.

2) Creamos .htaccess en /var/projects/server1/seguro

```
AuthType Basic
AuthName "Área Segura (PR4)"
AuthUserFile /etc/apache2/.htpasswd
Require valid-user
```

3) Añadimos la directiva AllowOverride All en el archivo de configuración de nuestro servidor principal

```
<VirtualHost *:80>
    ServerAdmin webmaster@localhost
    ServerName www.server1.com
    ServerAlias server1.com
    DocumentRoot /var/projects/server1

    <Directory /var/projects/server1>
        Require all granted
        Options Indexes FollowSymLinks
        AllowOverride all
    </Directory>

    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>
```

/etc/apache2/sites-available/server1.conf

Cuando está configurada en **None**, Apache no permite que se anulen las directivas de configuración en archivos **.htaccess**, lo que significa que cualquier directiva especificada en un archivo **.htaccess** será ignorada.

5. ACCESO RESTRINGIDO POR CONTRASEÑA

Proteger el directorio *seguro* que colgará de la raíz del servidor principal (En mi caso, server1). Esté directorio contendrá una página index.html con un mensaje de bienvenida, y será necesario validarse con el usuario alumno, contraseña passceu.

4) Crear un index.html a /var/www/server1/seguro

5) Comprobación

The screenshot shows a web browser window with the address bar displaying "192.168.119.137/seguro/". A security warning "No seguro" is visible. A modal dialog box is open, titled "Inicie sesión para obtener acceso a este sitio". It contains the text "Autorización requerida por http://192.168.119.137" and "Su conexión con este sitio no es segura". Below this, there are input fields for "Nombre de usuario" and "Contraseña". At the bottom of the dialog are two buttons: "Iniciar sesión" (blue) and "Cancelar" (gray). The background page, titled "Server1 - Zona Segura", has a header with links: "Archivos secretos", "Archivos super secretos", and "Archivos Megasecretos". Below the header, there is a section titled "Acerca de" with the text: "Bienvenido a la zona secreta del servidor Server1, un espacio dedicado a los estudiantes del CEU San Pablo."