

Servidor multisitio por puerto y Enjaular usuario ubuntu

Despliegue de aplicaciones web

David Aparicio Sir

Contenido

Servidor multisitio por puerto y Enjaular usuario ubuntu	1
Configurar sitios	3
Copiamos la configuracion inicial /etc/apache2/sites-available/000-default.config	3
Configuramos el fichero anteriormente copiado	3
Configuramos el servicio apache2 para escuchar por el puerto 81	3
Activamos el sitio puerto81	4
Abrimos el puerto 81 en el cortafuegos	4
Comprobamos que funciona	5
Enjaular usuario	5
Cambiamos el propietario del directorio home del usuario daw202 que es /var/www/puerto81 al usuario root y grupo root	5
Cambiaremos los permisos para que nadie pueda escribir (555)	5
Cambiamos los permisos y propietario del directorio /var/www/puerto81/public_html al usuario daw202 y grupo www-data permisos para que el propietario como el grupo tenga permisos totales y el publico solo pueda ver y ejecutar con bit pegajoso y recursividad (2775)	5
Creamos el grupo de usuarios enjaulados para simplificar la creacion de proximos usuarios .5	
Añadimos el usuario al nuevo grupo	5
Editar /etc/ssh/sshd_config	6
Comprobacion	7

Creamos el usuario puerto81 con home en /var/www/puerto81 y password paso

```
miadmin@das-used:/etc/apache2/sites-available$ sudo useradd -m -d /var/www/puerto81 -g www-data daw202
miadmin@das-used:/etc/apache2/sites-available$ sudo passwd daw202
New password:
Retype new password:
passwd: password updated successfully
```

Creamos el directorio /var/www/puerto81/public_html

```
miadmin@das-used:/etc/apache2$ sudo mkdir /var/www/puerto81/public_html
```

```
miadmin@das-used:/etc/apache2/sites-available$ ls -l /var/www
total 8
drwxrwsr-x 8 operadorweb www-data 4096 oct 12 08:32 html
drwxr-x--- 2 daw202          www-data 4096 oct 27 15:14 puerto81
```

Configurar sitios

Copiamos la configuracion inicial /etc/apache2/sites-available/000-default.config

```
miadmin@das-used:/etc/apache2/sites-available$ sudo cp 000-default.conf puerto81.conf
```

Configuramos el fichero anteriormente copiado

```
GNU nano 6.2                                puerto81.conf
<VirtualHost *:81>
# 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/puerto81/public_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
# following line enables the CGI configuration for this host only
[ Wrote 31 lines ]
^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location   M-U Undo
^X Exit      ^R Read File  ^\ Replace    ^U Paste      ^J Justify    ^_ Go To Line  M-E Redo
```

Establecemos la escucha de todas las direcciones por el puerto 81 y la raiz de documentos a /var/www/puerto81

Configuramos el servicio apache2 para escuchar por el puerto 81

Habilitamos el sitio puerto81 en el fichero /etc/apache2/ports.conf incluimos la sentencia Listen 81

```
GNU nano 6.2 ports.conf *
# If you just change the port or add more ports here, you will likely also
# have to change the VirtualHost statement in
# /etc/apache2/sites-enabled/000-default.conf

Listen 80
Listen 81
<IfModule ssl_module>
    Listen 443
</IfModule>

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

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

[ Read 15 lines ]
^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location   M-U Undo
^X Exit      ^R Read File  ^R Replace    ^U Paste      ^J Justify    ^_/ Go To Line  M-E Redo
```

Activamos el sitio puerto81

```
miadmin@das-used:/etc/apache2/sites-available$ sudo a2ensite puerto81
Enabling site puerto81.
To activate the new configuration, you need to run:
    systemctl reload apache2
miadmin@das-used:/etc/apache2/sites-available$ sudo service apache2 restart
miadmin@das-used:/etc/apache2/sites-available$ sudo service apache2 status
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset: enabled)
   Active: active (running) since Thu 2022-10-27 15:17:48 UTC; 5s ago
     Docs: https://httpd.apache.org/docs/2.4/
   Process: 1313 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
  Main PID: 1318 (apache2)
    Tasks: 6 (limit: 2238)
   Memory: 10.1M
      CPU: 63ms
   CGroup: /system.slice/apache2.service
           └─1318 /usr/sbin/apache2 -k start
             └─1319 /usr/sbin/apache2 -k start
               └─1320 /usr/sbin/apache2 -k start
                 └─1321 /usr/sbin/apache2 -k start
                   └─1322 /usr/sbin/apache2 -k start
                     └─1323 /usr/sbin/apache2 -k start

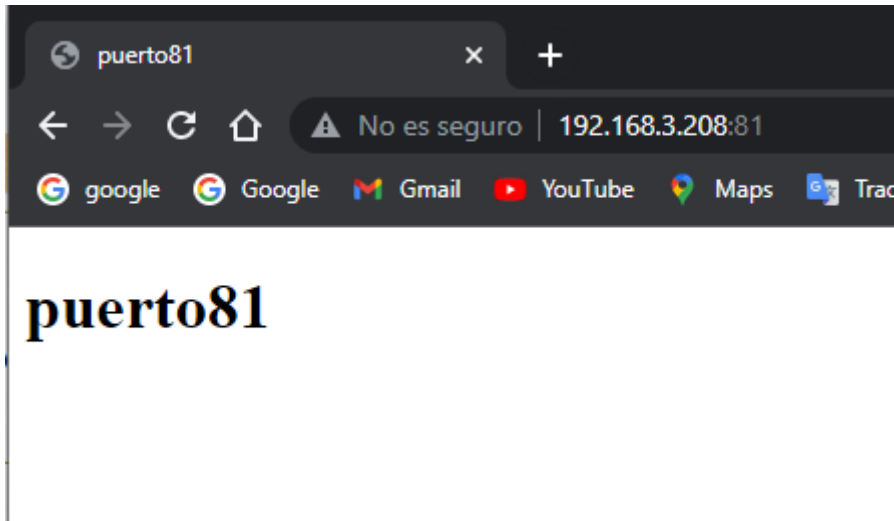
oct 27 15:17:48 das-used systemd[1]: apache2.service: Deactivated successfully.
oct 27 15:17:48 das-used apachectl[1310]: AH00558: apache2: Could not reliably determine the server's fully qualified domain name, please see the README file for details on how to set the 'ServerName' directive correctly to avoid this warning.
oct 27 15:17:48 das-used systemd[1]: Stopped The Apache HTTP Server.
oct 27 15:17:48 das-used systemd[1]: Starting The Apache HTTP Server...
oct 27 15:17:48 das-used apachectl[1317]: AH00558: apache2: Could not reliably determine the server's fully qualified domain name, please see the README file for details on how to set the 'ServerName' directive correctly to avoid this warning.
oct 27 15:17:48 das-used systemd[1]: Started The Apache HTTP Server.
```

Abrimos el puerto 81 en el cortafuegos

```
rule added (v6)
miadmin@das-used:/etc/apache2$ sudo ufw status
Status: active

To Action From
--
9003 ALLOW Anywhere
80 ALLOW Anywhere
22 ALLOW Anywhere
81 ALLOW Anywhere
9003 (v6) ALLOW Anywhere (v6)
80 (v6) ALLOW Anywhere (v6)
22 (v6) ALLOW Anywhere (v6)
81 (v6) ALLOW Anywhere (v6)
```

Comprobamos que funciona



Enjaular usuario

Enajularemos el usuario daw202

Cambiamos el propietario del directorio home del usuario daw202 que es /var/www/puerto81 al usuario root y grupo root

```
miadmin@das-used:/etc/apache2$ sudo chown root:root /var/www/puerto81
```

Cambiaremos los permisos para que nadie pueda escribir (555)

```
miadmin@das-used:/etc/apache2$ sudo chmod 555 /var/www/puerto81
```

Cambiamos los permisos y propietario del directorio /var/www/puerto81/public_html al usuario daw202 y grupo www-data permisos para que el propietario como el grupo tenga permisos totales y el publico solo pueda ver y ejecutar con bit pegajoso y recursividad (2775)

```
miadmin@das-used:/etc/apache2$ sudo chown -R daw202:www-data /var/www/puerto81/public_html/
```

```
miadmin@das-used:/etc/ssh$ sudo chmod -R 2775 /var/www/puerto81/public_html/
```

Creamos el grupo de usuarios enjaulados para simplificar la creacion de proximos usuarios

```
miadmin@das-used:/etc/apache2$ sudo groupadd ftpusers
```

Añadimos el usuario al nuevo grupo

```
miadmin@das-used:/etc/apache2$ sudo usermod -g ftpusers daw202
```

Comprobamos

```
miadmin@das-used:/etc/apache2$ cat /etc/group|grep ftp
ftpusers:x:1001:
miadmin@das-used:/etc/apache2$ cat /etc/passwd|grep daw202
daw202:x:1002:1001::/var/www/puerto81:/bin/sh
miadmin@das-used:/etc/apache2$
```

[Editar /etc/ssh/sshd_config](#)

Antes de editar lo mejor que podemos hacer es hacer una copia de seguridad del fichero anterior

```
miadmin@das-used:/etc/ssh$ sudo cp sshd_config sshd_config.bak
miadmin@das-used:/etc/ssh$ ls -l
total 552
-rw-r--r-- 1 root root 505426 feb 25 2022 moduli
-rw-r--r-- 1 root root 1650 feb 25 2022 ssh_config
drwxr-xr-x 2 root root 4096 feb 25 2022 ssh_config.d
-rw-r--r-- 1 root root 3281 sep 28 15:18 sshd_config
-rw-r--r-- 1 root root 3281 oct 27 16:11 sshd_config.bak
drwxr-xr-x 2 root root 4096 feb 25 2022 sshd_config.d
-rw----- 1 root root 1381 sep 28 15:17 ssh_host_dsa_key
-rw-r--r-- 1 root root 606 sep 28 15:17 ssh_host_dsa_key.pub
-rw----- 1 root root 505 sep 28 15:17 ssh_host_ecdsa_key
-rw-r--r-- 1 root root 178 sep 28 15:17 ssh_host_ecdsa_key.pub
-rw----- 1 root root 411 sep 28 15:17 ssh_host_ed25519_key
-rw-r--r-- 1 root root 98 sep 28 15:17 ssh_host_ed25519_key.pub
-rw----- 1 root root 2602 sep 28 15:17 ssh_host_rsa_key
-rw-r--r-- 1 root root 570 sep 28 15:17 ssh_host_rsa_key.pub
-rw-r--r-- 1 root root 342 dic 7 2020 ssh_import_id
```

En el final del fichero sshd_config incluimos las siguientes sentencias

```
#Subsystem sftp /usr/lib/openssh/sftp-server
Subsystem sftp internal-sftp
# Example of overriding settings on a per-user basis
#Match User anoncvs
#    X11Forwarding no
#    AllowTcpForwarding no
#    PermitTTY no
#    ForceCommand cvs server
PasswordAuthentication yes

Match Group ftpusers
ChrootDirectory %h
ForceCommand internal-sftp -u 2
AllowTcpForwarding yes
PermitTunnel no
X11Forwarding no
```

Comprobacion

sftp://daw202@192.168.3.208 - FileZilla

ArchivoEdiciónVerTransferenciaServidorMarcadoresAyuda¡Nueva versión disponible!

Servidor: sftp://192.168.3.208Nombre de usuario: daw202Contraseña:Puerto: Conexión rápida

Estado: Connected to 192.168.3.208
Estado: Recuperando el listado del directorio...
Estado: Listing directory /
Estado: Directorio "/" listado correctamente
Estado: Recuperando el listado del directorio "/"...
Estado: Directorio "/" listado correctamente

Sitio local: E:\DAW2_22_23\DWES\20221003_DavidAparicio\nbproject\

nbproject

webroot

221025_DWES_Libro

projectoDAWCurso2223

T1 DWES

T2

T3

T4

T5

T6

T7

Sitio remoto: /

.cache

public_html

Nombre de archivo	Tamaño de...	Tipo de archivo	Última modificaci...
..			
private		Carpeta de archivos	10/10/2022 18:09:21
project.properties	141	Archivo PROPERTIES	03/10/2022 17:50:55
project.xml	333	Archivo XML	03/10/2022 17:50:55

2 archivos y 1 directorio. Tamaño total: 474 bytes

Nombre de archivo	Tamaño d...	Última modificación	Permisos
..			
.cache		27/10/2022 17:19:30	drwx-----
public_html		27/10/2022 17:23:01	drwxrwsr-x
.bash_logout	220	06/01/2022 17:23:33	-rw-r--r--
.bashrc	3.771	06/01/2022 17:23:33	-rw-r--r--
.profile	807	06/01/2022 17:23:33	-rw-r--r--

3 archivos y 2 directorios. Tamaño total: 4.798 bytes

Servidor/Archivo local	Direcci...	Archivo remoto	Tamaño	Prioridad	Estado
------------------------	------------	----------------	--------	-----------	--------

Archivos en colaTransferencias fallidasTransferencias satisfactorias

Cola: vacía