

Jenny-Vasquez /
Nginx-AccesoSeguro[Code](#) [Issues](#) [Pull requests](#) [Actions](#) [Projects](#) [Wiki](#) [Security](#)

main

Nginx-AccesoSeguro

/ README.md



Jenny-Vasquez Update README.md

4c0478c · now



133 lines (106 loc) · 4.07 KB

Preview

Code

Blame

Raw



Nginx-Autenticacion

Previamente la configuracion de nuestra maquina debe estar correcta, para ello hemos realizado los siguientes pasos.

Configuración de Máquina Virtual con Debian, Nginx y FTPS

Hemos configurado automáticamente una máquina virtual basada en Debian utilizando **Vagrant**. La configuración incluye:

- Instalación de **Nginx** y configuración personalizada para un sitio web.
- Implementación de un servidor FTPS seguro con **vsftpd**.
- Clonación de un repositorio Git en nuestro caso <https://github.com/Jenny-Vasquez/Practica2.git>

1. Instalación y Configuración de Nginx

1. **Vagrant** instalado en tu sistema.
2. **VirtualBox** u otro proveedor compatible con Vagrant.
3. Acceso a Internet para descargar la caja base y dependencias.

4. Un repositorio Git accesible para la clonación (en este caso: <https://github.com/Jenny-Vasquez/Practica2.git>).
5. La configuración del servidor se ajustó de la siguiente forma:

```
server{  
    listen 80;  
    listen [::]:80;  
    server_name taylorweb;  
  
    root /var/www/taylorweb/html/Practica2;  
    index index.html index.htm index.nginx-debian.html;  
  
    location / {  
        try_files $uri $uri/ =404;  
    }  
}
```



6. Se verificó que la configuración estuviera correcta ejecutando:

```
sudo nginx -t
```



```
vagrant@bookworm:~$ cd /etc/nginx/sites-available/  
vagrant@bookworm:/etc/nginx/sites-available$ sudo nginx -t  
nginx: the configuration file /etc/nginx/nginx.conf syntax is ok  
nginx: configuration file /etc/nginx/nginx.conf test is successful  
vagrant@bookworm:/etc/nginx/sites-available$
```

2. Configuración del Cortafuegos

1. Se instaló y configuró el cortafuegos UFW para proteger la máquina virtual:

```
sudo apt update  
sudo apt install ufw
```



2. Se realizaron las siguientes configuraciones:

- Permitir SSH:

```
sudo ufw allow ssh
```



- Permitir tráfico seguro por HTTPS (Nginx Full):

```
sudo ufw allow 'Nginx Full'
```



- Bloquear tráfico no seguro:

```
sudo ufw delete allow 'Nginx HTTP'
```



```
vagrant@bookworm:/etc/nginx/sites-available$ sudo ufw status
Status: inactive
vagrant@bookworm:/etc/nginx/sites-available$ sudo ufw allow ssh
Rules updated
Rules updated (v6)
vagrant@bookworm:/etc/nginx/sites-available$ sudo ufw allow 'Nginx Full'
Rules updated
Rules updated (v6)
vagrant@bookworm:/etc/nginx/sites-available$ sudo ufw delete allow 'Nginx HTTP'
Could not delete non-existent rule
Could not delete non-existent rule (v6)
vagrant@bookworm:/etc/nginx/sites-available$
```

3. Se activó el cortafuegos:

```
sudo ufw enable
```



```
vagrant@bookworm:/etc/nginx/sites-available$ sudo ufw enable
Command may disrupt existing ssh connections. Proceed with operation (y|n)? y
Firewall is active and enabled on system startup
vagrant@bookworm:/etc/nginx/sites-available$
```

4. El estado se verificó con:

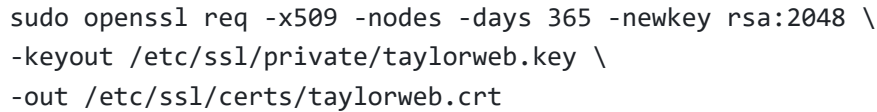
```
sudo ufw status
```



```
vagrant@bookworm:/etc/nginx/sites-available$ sudo ufw enable
Command may disrupt existing ssh connections. Proceed with operation
(y|n)? y
Firewall is active and enabled on system startup
vagrant@bookworm:/etc/nginx/sites-available$ sudo ufw status
Status: active

To Action From
--
22/tcp ALLOW Anywhere
Nginx Full ALLOW Anywhere
22/tcp (v6) ALLOW Anywhere (v6)
Nginx Full (v6) ALLOW Anywhere (v6)
```

3. Habilitación de HTTPS con Certificado Autofirmado

[illegible]

```
sudo chmod 600 /etc/ssl/private/taylorweb.key
sudo chmod 600 /etc/ssl/certs/taylorweb.crt
```

[illegible]

```
server {  
    listen 443 ssl; # Puerto HTTPS  
    server_name taylorweb;  
  
    root /var/www/taylorweb/html/Practica2;  
    index index.html index.htm;  
  
    ssl_certificate /etc/ssl/certs/taylorweb.crt;  
    ssl_certificate_key /etc/ssl/private/taylorweb.key;  
  
    ssl_protocols TLSv1.2 TLSv1.3;  
  
    location / {  
        try_files $uri $uri/ =404;  
    }  
}
```



4. Se verificó la configuración nuevamente:

```
sudo nginx -t
```



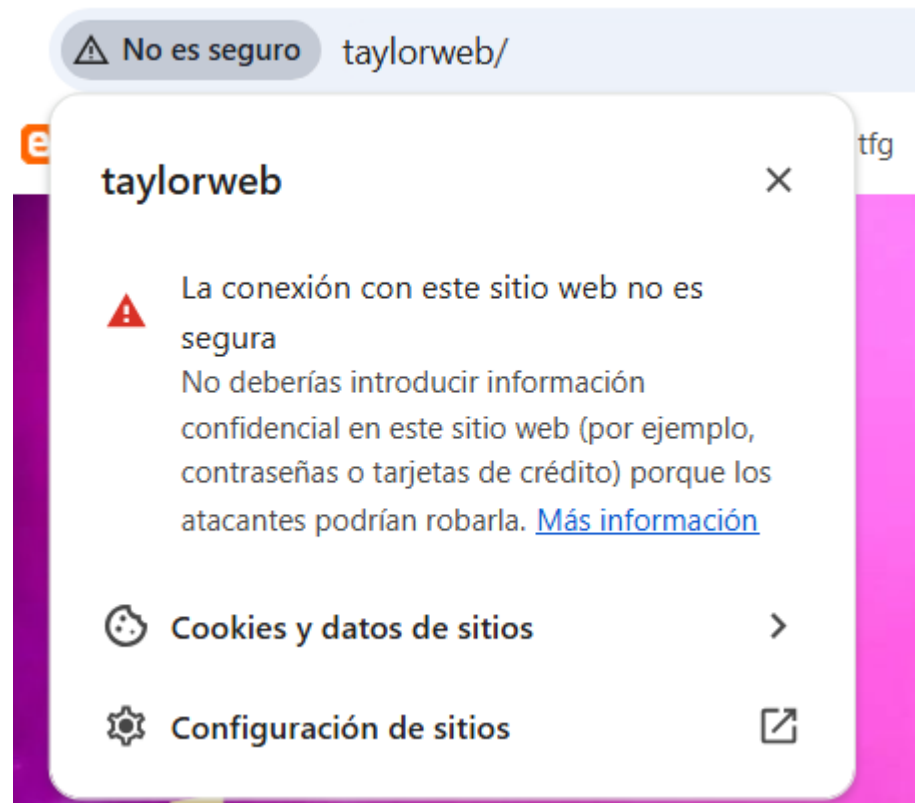
```
vagrant@bookworm:/etc/nginx/sites-available$ sudo nano /etc/nginx/sites-available/taylorweb  
vagrant@bookworm:/etc/nginx/sites-available$ sudo nginx -t  
nginx: the configuration file /etc/nginx/nginx.conf syntax is ok  
nginx: configuration file /etc/nginx/nginx.conf test is successful
```

Resultados

El servidor está configurado para usar HTTPS, pero como el certificado SSL es **autofirmado**, los navegadores mostrarán una advertencia indicando que la conexión no es completamente segura.

Mensaje en el Navegador

Al acceder al sitio en un navegador mediante `https://taylorweb`, se muestra un mensaje indicando que la conexión no es completamente segura, lo que significa que los datos intercambiados entre el navegador y el sitio no están cifrados.



IMAGENES DE LA CONFIGURACIÓN

```
The programs included with the Debian GNU/Linux system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.
```

```
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent  
permitted by applicable law.
```

```
Last login: Wed Nov 20 10:06:59 2024 from 10.0.2.2
```

```
vagrant@bookworm:~$ ls -l /etc/nginx/sites-available/  
total 8
```

```
-rw-r--r-- 1 root root 2412 Mar 14 2023 default
```

```
-rwxr-xr-x 1 root root 227 Nov 20 11:06 taylorweb
```

```
vagrant@bookworm:~$ ls -l /etc/nginx/sites-enabled/  
total 0
```

```
lrwxrwxrwx 1 root root 36 Nov 20 11:06 taylorweb -> /etc/nginx/sites-available/taylorweb
```

```
vagrant@bookworm:~$
```

```
vagrant@bookworm:~$ cd /var/www/taylorweb/html/
```

```
vagrant@bookworm:/var/www/taylorweb/html$ ls -la
```

```
total 8
```

```
drwxr-xr-x 2 www-data www-data 4096 Nov 20 12:34 .
```

```
drwxr-xr-x 3 root root 4096 Nov 20 12:34 ..
```

```
vagrant@bookworm:/var/www/taylorweb/html$ sudo git clone https://github.com/Jenny-Vasquez/Practica2.git
```

```
Cloning into 'Practica2'...
```

```
remote: Enumerating objects: 49, done.
```

```
remote: Counting objects: 100% (49/49), done.
```

```
remote: Compressing objects: 100% (47/47), done.
```

```
vagrant@bookworm:/var/www/taylorweb/html$ sudo chown -R www-data:www-data /var/www/taylorweb/html/Practica2
```

```
vagrant@bookworm:/var/www/taylorweb/html$ sudo chmod -R 755 /var/www/taylorweb/html/Practica2
```

```
vagrant@bookworm:/var/www/taylorweb/html$ ^C
```

```
vagrant@bookworm:/var/www/taylorweb/html$ sudo nginx -t
```

```
sudo systemctl restart nginx
```

```
nginx: the configuration file /etc/nginx/nginx.conf syntax is ok
```

```
nginx: configuration file /etc/nginx/nginx.conf test is successful
```

```
vagrant@bookworm:/var/www/taylorweb/html$ sudo systemctl restart nginx
```

```
vagrant@bookworm:/var/www/taylorweb/html$ sudo nano /etc/hosts
```

```
vagrant@bookworm:/var/www/taylorweb/html$
```

```
GNU nano 7.2
```

```
127.0.0.1 localhost
```

```
127.0.0.2 bookworm
```

```
::1 localhost ip6-localhost ip6-loopback
```

```
ff02::1 ip6-allnodes
```

```
ff02::2 ip6-allrouters
```

```
192.168.56.11 taylorweb
```



```
PROBLEMAS  SALIDA  CONSOLA DE DEPURACIÓN  TERMINAL  PUERTOS  SEARCH ERROR

GNU nano 7.2
server {
    listen 80;
    listen [::]:80;
    server_name taylorweb; # 0 tu nombre de dominio o IP

    root /var/www/taylorweb/html/Practica2;
    index index.html index.htm index.nginx-debian.html;

    location / {
        try_files $uri $uri/ =404; # Si no se encuentra el archivo, devuelve 404
    }
}
```

