WEB APPLICATIONS DEPLOYMENT

TERM 1

ASSESSABLE ACTIVITY

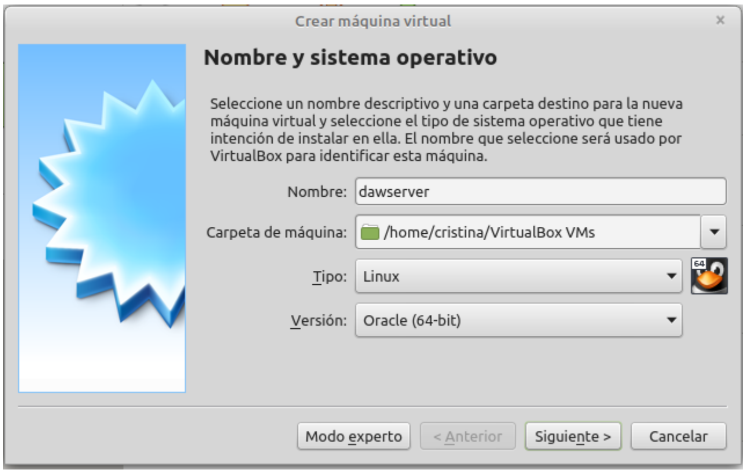
2021-2022

CRISTINA CHIARRI

1 CREATING A VIRTUAL MACHINE

1.1 Create the virtual machine

As you can see below, we create with VirtualBox a virtual machine called dawserver with a 25GB hard drive dynamically allocated



Nombre y sistema operativo

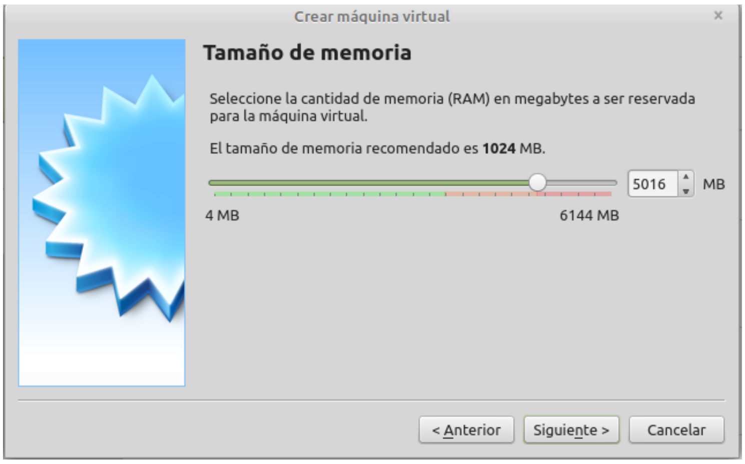
Seleccione un nombre descriptivo y una carpeta destino para la nueva máquina virtual y seleccione el tipo de sistema operativo que tiene intención de instalar en ella. El nombre que seleccione será usado por VirtualBox para identificar esta máquina.

Nombre: dawserver

Carpeta de máquina: /home/cristina/VirtualBox VMs

Tipo: Linux

Versión: Oracle (64-bit)



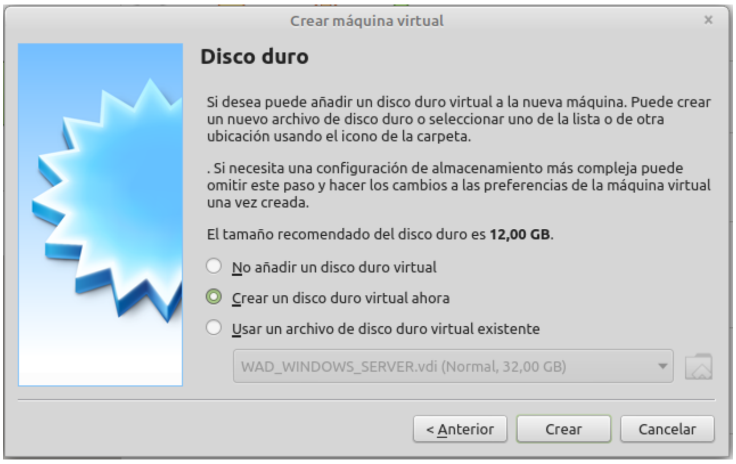
Tamaño de memoria

Seleccione la cantidad de memoria (RAM) en megabytes a ser reservada para la máquina virtual.

El tamaño de memoria recomendado es **1024** MB.

5016 MB

4 MB 6144 MB



Disco duro

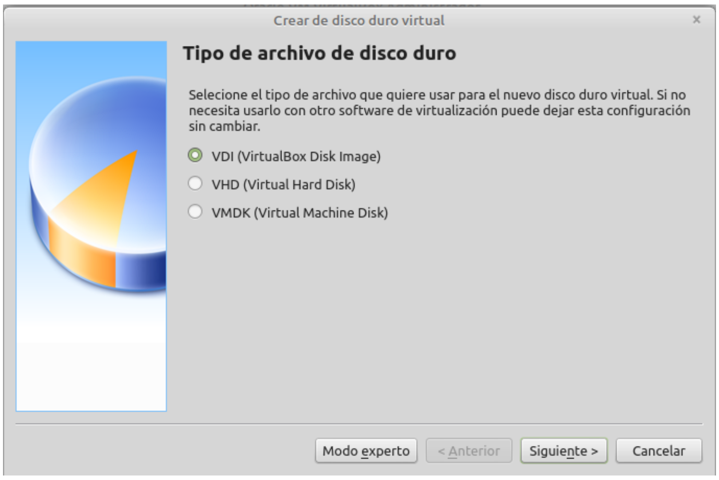
Si desea puede añadir un disco duro virtual a la nueva máquina. Puede crear un nuevo archivo de disco duro o seleccionar uno de la lista o de otra ubicación usando el icono de la carpeta.

. Si necesita una configuración de almacenamiento más compleja puede omitir este paso y hacer los cambios a las preferencias de la máquina virtual una vez creada.

El tamaño recomendado del disco duro es **12,00 GB**.

○ No añadir un disco duro virtual
● Crear un disco duro virtual ahora
○ Usar un archivo de disco duro virtual existente

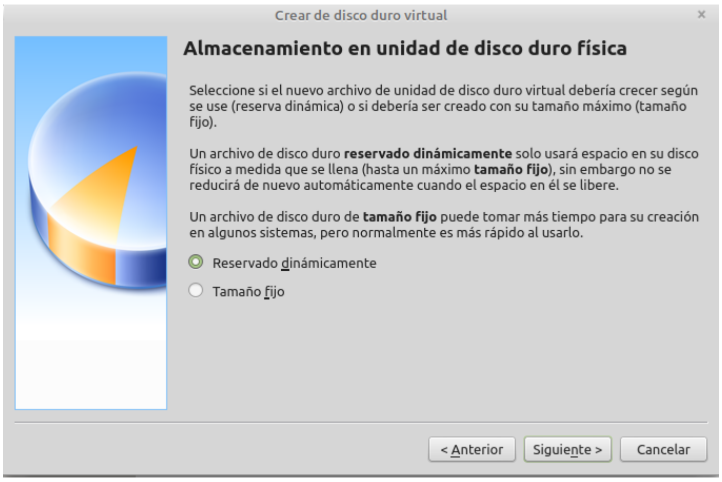
WAD_WINDOWS_SERVER.vdi (Normal, 32,00 GB)



Tipo de archivo de disco duro

Selecione el tipo de archivo que quiere usar para el nuevo disco duro virtual. Si no necesita usarlo con otro software de virtualización puede dejar esta configuración sin cambiar.

● VDI (VirtualBox Disk Image)
○ VHD (Virtual Hard Disk)
○ VMDK (Virtual Machine Disk)



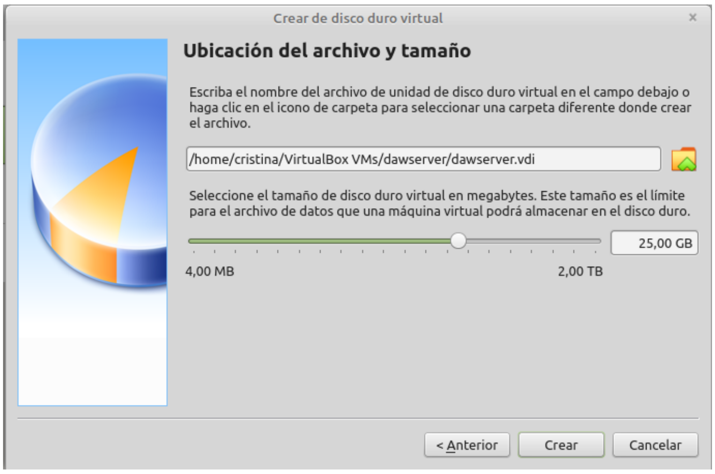
Almacenamiento en unidad de disco duro física

Seleccione si el nuevo archivo de unidad de disco duro virtual debería crecer según se use (reserva dinámica) o si debería ser creado con su tamaño máximo (tamaño fijo).

Un archivo de disco duro **reservado dinámicamente** solo usará espacio en su disco físico a medida que se llena (hasta un máximo **tamaño fijo**), sin embargo no se reducirá de nuevo automáticamente cuando el espacio en él se libere.

Un archivo de disco duro de **tamaño fijo** puede tomar más tiempo para su creación en algunos sistemas, pero normalmente es más rápido al usarlo.

● Reservado dinámicamente
○ Tamaño fijo



Ubicación del archivo y tamaño

Escriba el nombre del archivo de unidad de disco duro virtual en el campo debajo o haga clic en el icono de carpeta para seleccionar una carpeta diferente donde crear el archivo.

/home/cristina/VirtualBox VMs/dawserver/dawserver.vdi

Seleccione el tamaño de disco duro virtual en megabytes. Este tamaño es el límite para el archivo de datos que una máquina virtual podrá almacenar en el disco duro.

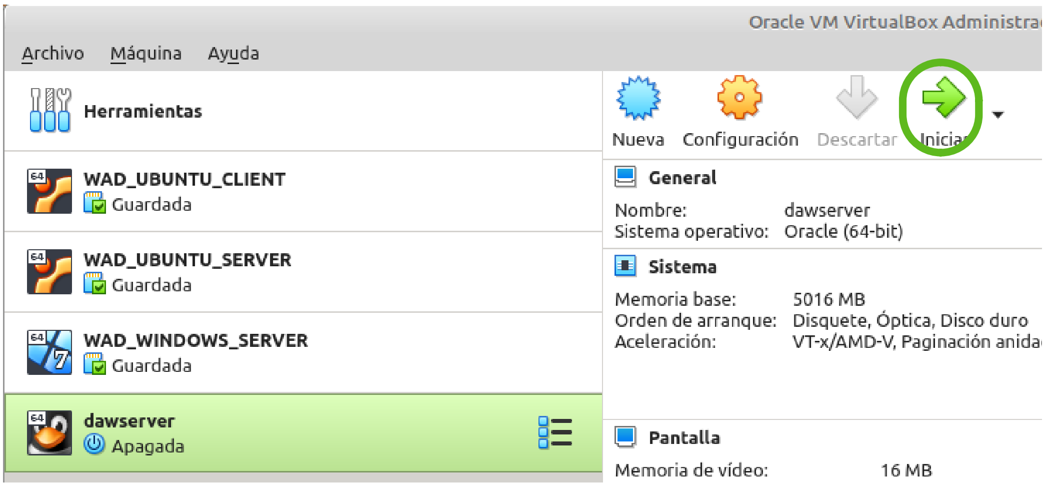
25,00 GB

4,00 MB 2,00 TB

1.2 OS installation

Once the virtual machine is created we have to choose the ISO or VDI file to install the OS selected. I am going to use an iso for **Ubuntu 20.04.3 LTS** distribution.

We start the virtual machine and select the iso file.



WAD_UBUNTU_CLIENT Guardada

WAD_UBUNTU_SERVER Guardada

WAD_WINDOWS_SERVER Guardada

dawserver Apagada

General

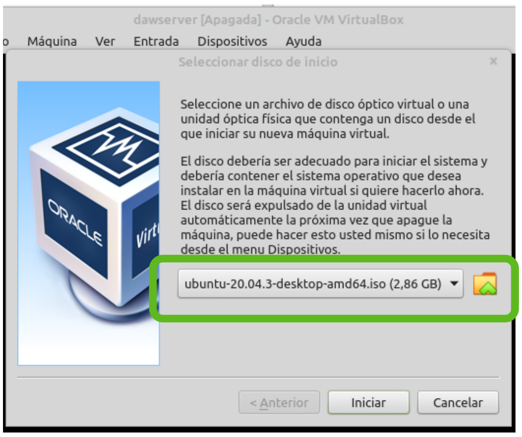
Nombre: dawserver
Sistema operativo: Oracle (64-bit)

Sistema

Memoria base: 5016 MB
Orden de arranque: Disquete, Óptica, Disco duro
Aceleración: VT-x/AMD-V, Paginación anida

Pantalla

Memoria de vídeo: 16 MB

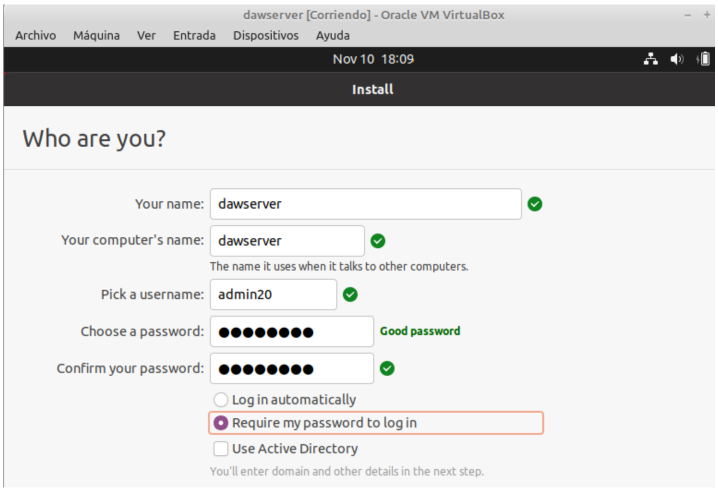

dawserver [Apagada] - Oracle VM VirtualBox
Máquina
Ver
Entrada
Dispositivos
Ayuda
Seleccionar disco de inicio
< Anterior
Iniciar
Cancelar

Seleccione un archivo de disco óptico virtual o una unidad óptica física que contenga un disco desde el que iniciar su nueva máquina virtual.

El disco debería ser adecuado para iniciar el sistema y debería contener el sistema operativo que desea instalar en la máquina virtual si quiere hacerlo ahora. El disco será expulsado de la unidad virtual automáticamente la próxima vez que apague la máquina, puede hacer esto usted mismo si lo necesita desde el menu Dispositivos.

ubuntu-20.04.3-desktop-amd64.iso (2,86 GB)

We install the OS with the required hostanme and username:
hostname: dawserver
user: admin20
password: #Daw2020



Who are you?

Your name: dawserver

Your computer's name: dawserver
The name it uses when it talks to other computers.

Pick a username: admin20

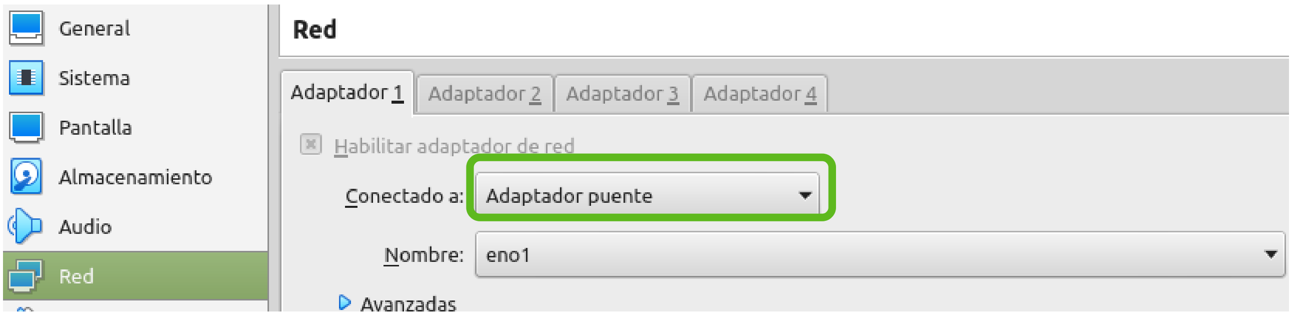
Choose a password: ●●●●●●●● Good password

Confirm your password: ●●●●●●●●

○ Log in automatically
● Require my password to log in
□ Use Active Directory
You'll enter domain and other details in the next step.

1.3 Network configuration

Once the OS is installed we have to configure the virtual machine network to **bridge adapter** in order that the virtual machine could access to our router.



Red

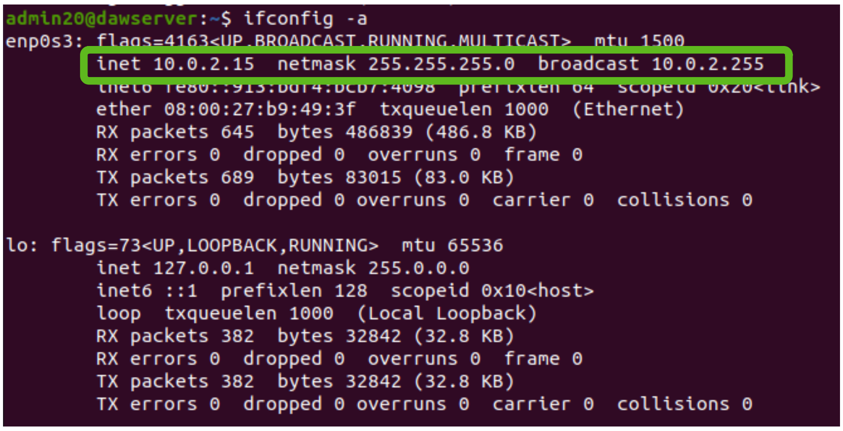
Adaptador 1 | Adaptador 2 | Adaptador 3 | Adaptador 4

☒ Habilitar adaptador de red

Conectado a: Adaptador puente

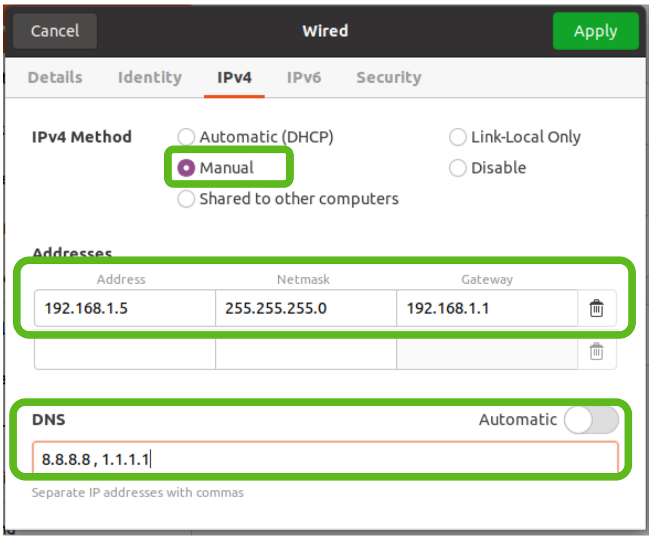
Nombre: eno1

Next we must include the virtual machine in our network **changing the IP** to one from our network. Here we can see the IP by default.



```
admin20@dawserver:~$ ifconfig -a
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::913:bdf4:bcb7:4098  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:b9:49:3f  txqueuelen 1000  (Ethernet)
        RX packets 645  bytes 486839 (486.8 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 689  bytes 83015 (83.0 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 382  bytes 32842 (32.8 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 382  bytes 32842 (32.8 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

We need to configure a **static IP** changing it from automatic to manual in our network settings. In this case I am going to use the IP 192.168.1.5 that belongs to my home network.



IPv4 Method

○ Automatic (DHCP) ○ Link-Local Only
● Manual ○ Disable
○ Shared to other computers

Addresses

Address	Netmask	Gateway
192.168.1.5	255.255.255.0	192.168.1.1

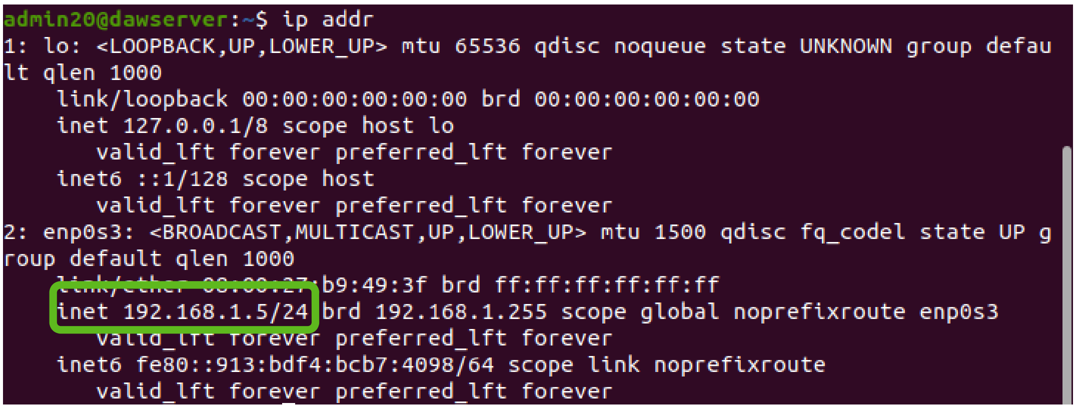
DNS Automatic ○

8.8.8.8 , 1.1.1.1

Separate IP addresses with commas

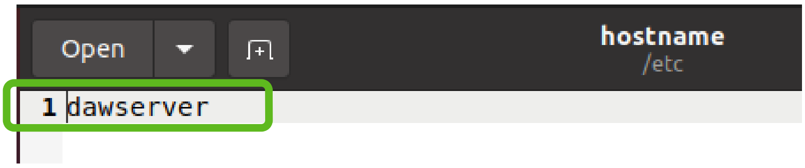
Once the network is restarted we must confirm that the configuration is correct.
We must check:

- The new static IP address using the command **ip addr**



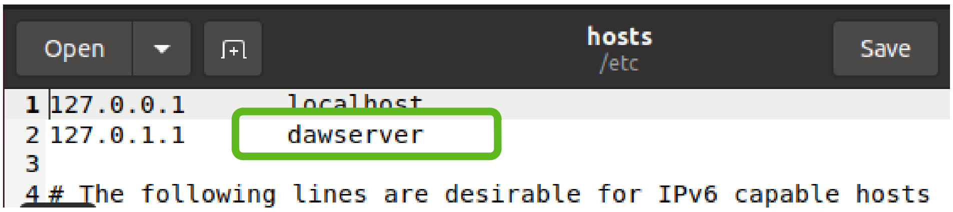
```
admin20@dawserver:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defau
lt qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP g
roup default qlen 1000
    link/ether 08:00:27:b9:49:3f brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.5/24 brd 192.168.1.255 scope global noprefixroute enp0s3
       valid_lft forever preferred_lft forever
    inet6 fe80::913:bdf4:bcb7:4098/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

- The hostname in the **hostname** configuration file content:



```
dawserver
```

- The hostname in the **hosts** configuration file content.

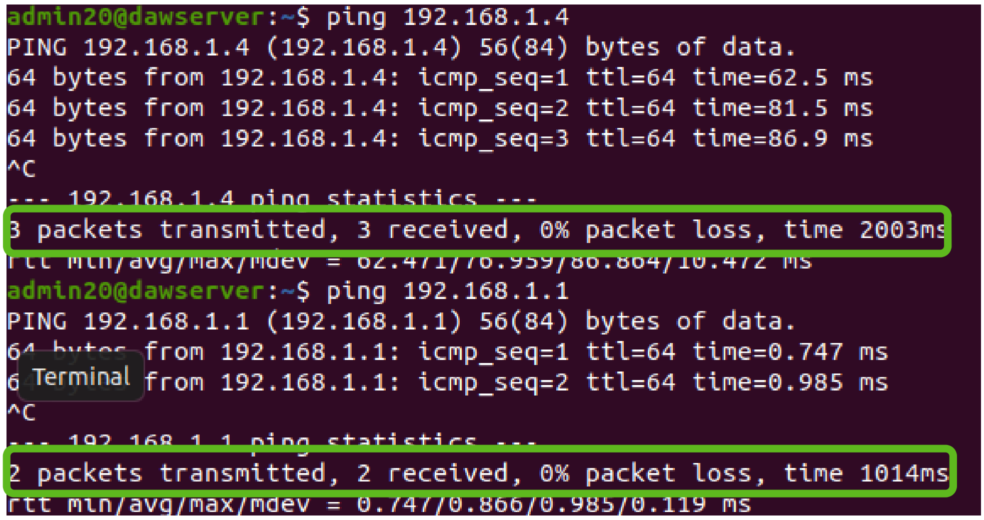


```
127.0.0.1       localhost
127.0.1.1       dawserver

# The following lines are desirable for IPv6 capable hosts
```

- **Reboot**

- The **network connection between both machines**, server and client.

We us the **ping command** to send packets of data to a specific IP address on a network, and to know how long it took to transmit that data and get a response. It is a tool to test our network.

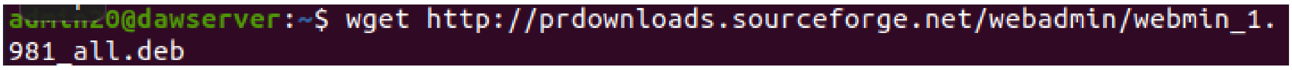


```
admin20@dawserver:~$ ping 192.168.1.4
PING 192.168.1.4 (192.168.1.4) 56(84) bytes of data.
64 bytes from 192.168.1.4: icmp_seq=1 ttl=64 time=62.5 ms
64 bytes from 192.168.1.4: icmp_seq=2 ttl=64 time=81.5 ms
64 bytes from 192.168.1.4: icmp_seq=3 ttl=64 time=86.9 ms
^C
--- 192.168.1.4 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 62.471/76.959/86.864/10.472 ms
admin20@dawserver:~$ ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=0.747 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=64 time=0.985 ms
^C
--- 192.168.1.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1014ms
rtt min/avg/max/mdev = 0.747/0.866/0.985/0.119 ms
```

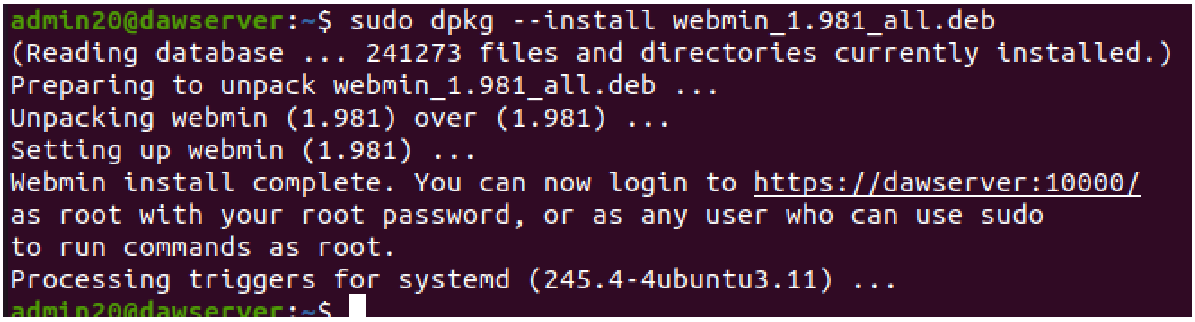
In this case, the server can reach the client.

1.4 Installing Webmin

Now we are going to download and **install Webmin**.

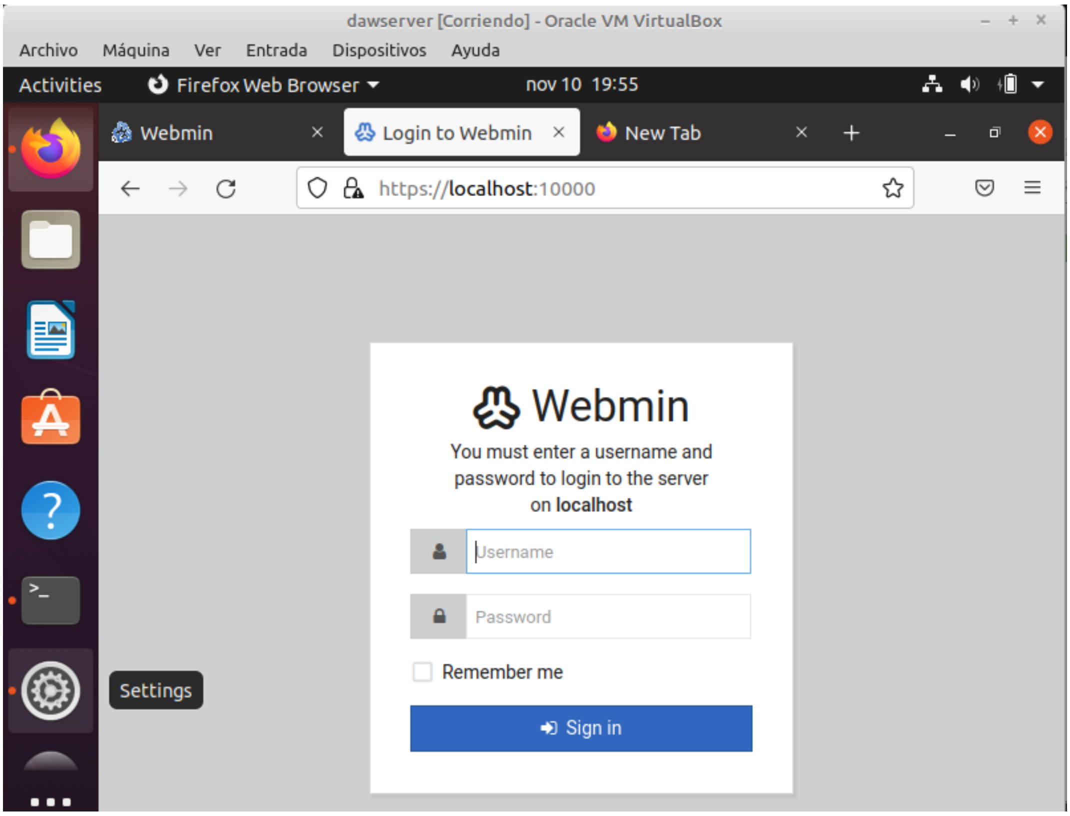


```
admin20@dawserver:~$ wget http://prdownloads.sourceforge.net/webadmin/webmin_1.
981_all.deb
```



```
admin20@dawserver:~$ sudo dpkg --install webmin_1.981_all.deb
(Reading database ... 241273 files and directories currently installed.)
Preparing to unpack webmin_1.981_all.deb ...
Unpacking webmin (1.981) over (1.981) ...
Setting up webmin (1.981) ...
Webmin install complete. You can now login to https://dawserver:10000/
as root with your root password, or as any user who can use sudo
to run commands as root.
Processing triggers for systemd (245.4-4ubuntu3.11) ...
admin20@dawserver:~$
```

Once installed we **set the username and password** (admin20/#Daw2020)

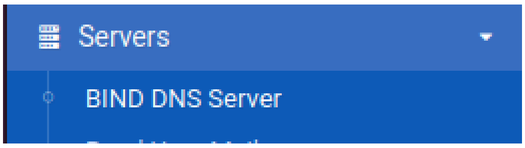


You must enter a username and password to login to the server on **localhost**

2 DNS SERVER

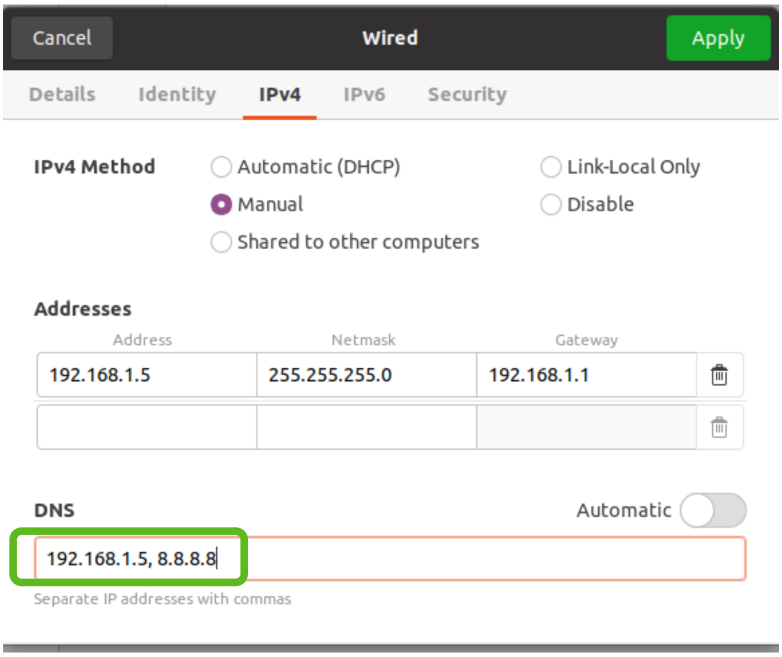
2.1 Installation

We need to **install BIND DNS server** (Un-used Modules) and refresh modules.
Once installed BIND DNS server is available on our webmin servers menu.



2.1.1 Configuration

We want to use our DNS server as default DNS, so we need to **change the DNS IP in our virtual machine network** configuration to our host IP. 192.168.1.5.



IPv4 Method
○ Automatic (DHCP)
● Manual
○ Shared to other computers
○ Link-Local Only
○ Disable

Addresses

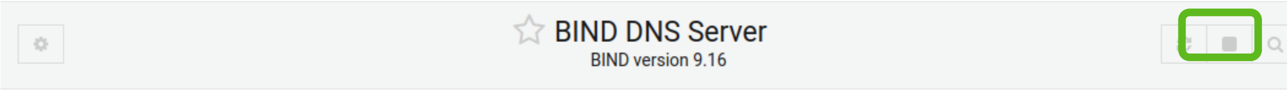
Address	Netmask	Gateway
192.168.1.5	255.255.255.0	192.168.1.1

DNS Automatic

192.168.1.5, 8.8.8.8

Separate IP addresses with commas

We **restart the network** and **confirm that BIND DNS server is on**.

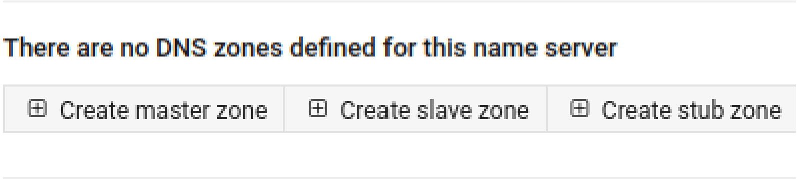


2.1.1.1 Configuring Lookup zone forward

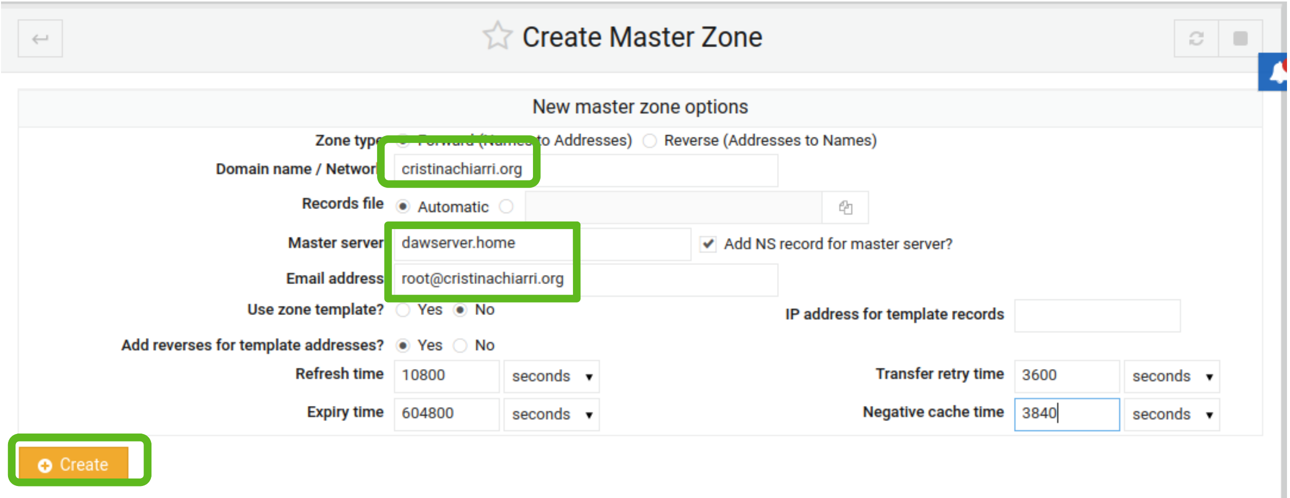
Forward lookup **resolve names to IP addresses.**

- **Create the master zone cristinachiarri.org**

We have to create a master zone with the domain name cristinachiarri.org



There are no DNS zones defined for this name server



Create Master Zone

New master zone options

Zone typ ○ Forward (Names to Addresses) ○ Reverse (Addresses to Names)

Domain name / Networ: cristinachiarri.org

Records file: ● Automatic ○

Master server: dawserver.home ☑ Add NS record for master server?

Email address: root@cristinachiarri.org

Use zone template? ○ Yes ● No

IP address for template records:

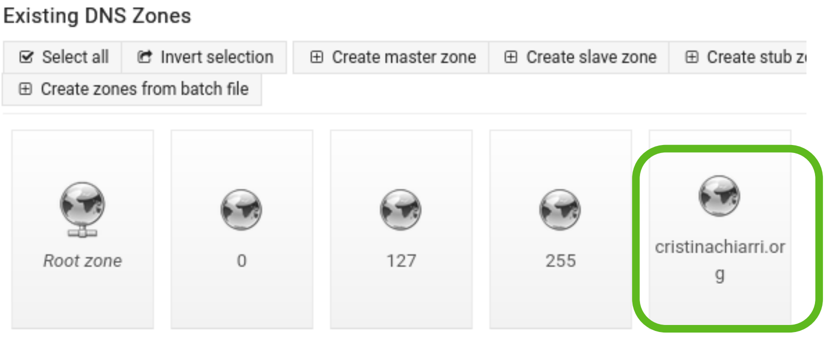
Add reverses for template addresses? ● Yes ○ No

Refresh time: 10800 seconds

Transfer retry time: 3600 seconds

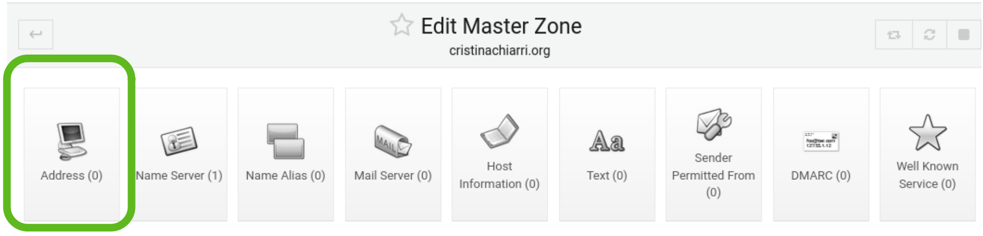
Expiry time: 604800 seconds

Negative cache time: 3840 seconds



Existing DNS Zones

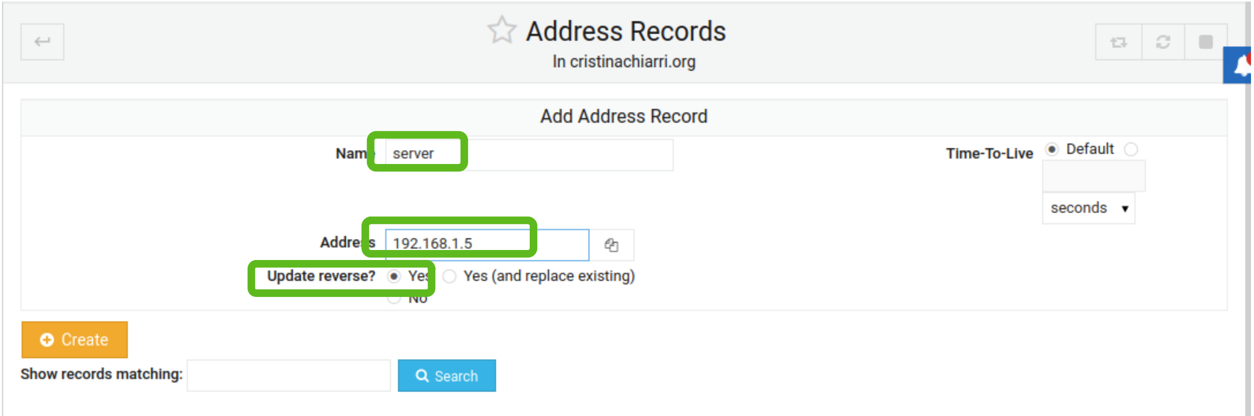
- **Edit Address and Name server records:**



Edit Master Zone
cristinachiarri.org

We need to create the **Address Records** of every subdomain or virtual machine.
The address record is the **basic type of DNS record: it indicates the IP address of a given domain.**

- **server.cristinachiarri.org** (dawserver machine)



Address Records
In cristinachiarri.org

Add Address Record

Name: server

Time-To-Live: ● Default ○ seconds

Address: 192.168.1.5

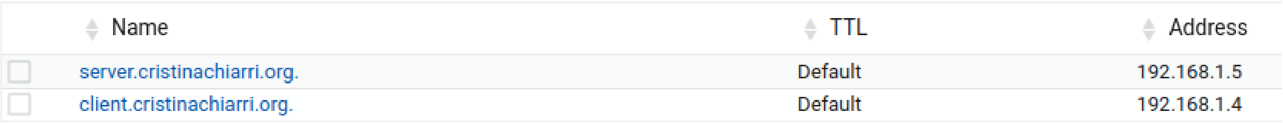
Update reverse? ● Yes ○ Yes (and replace existing) ○ No

We have to check the Update reverse button to create the reverse address in the reverse zone.

- **client.cristinachiarri.org** (client machine).

We have to repeat the same process for the client virtual machine.

Here we can see that both have been configured.



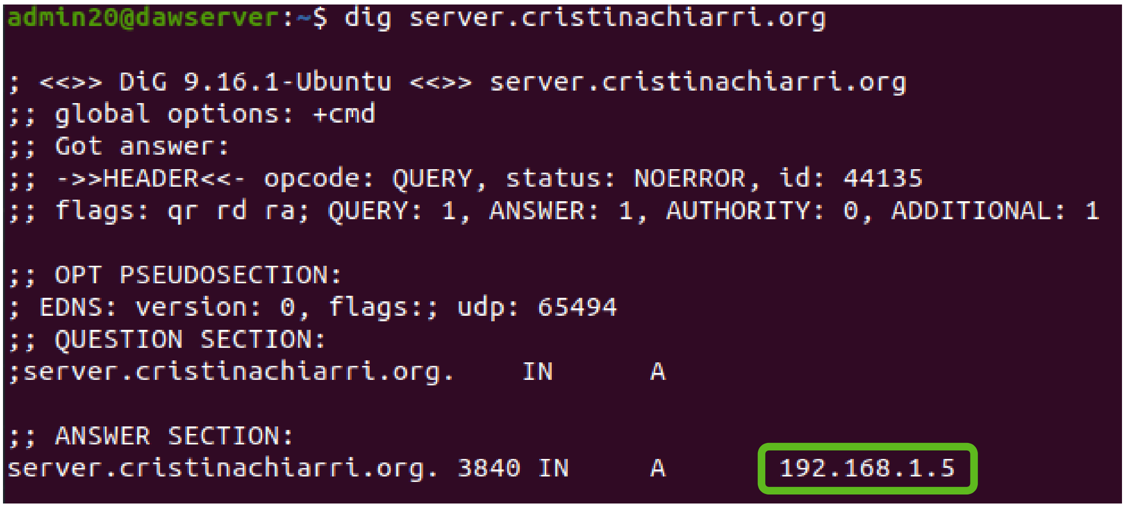
	Name	TTL	Address
□	server.cristinachiarri.org.	Default	192.168.1.5
□	client.cristinachiarri.org.	Default	192.168.1.4

We must apply the new configuration.

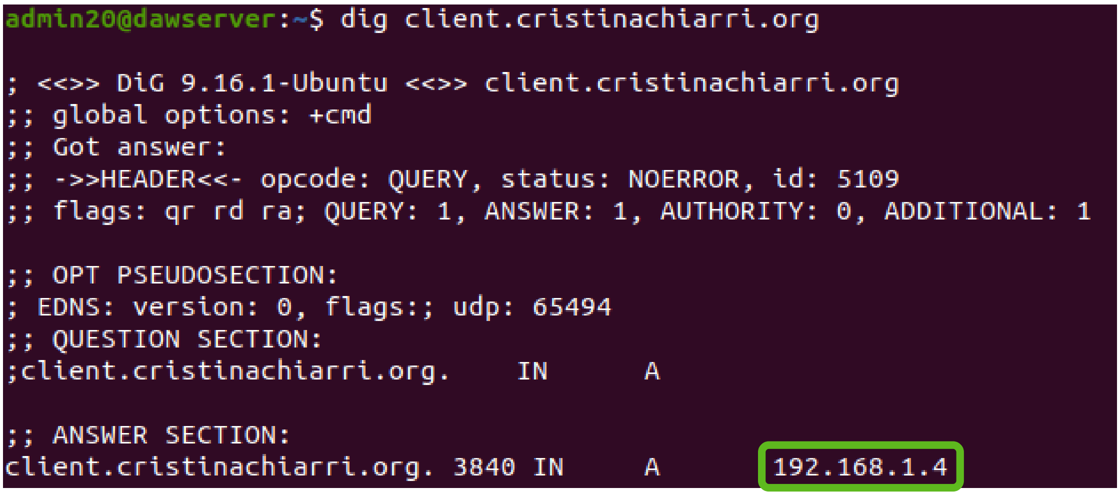
Check the configuration with: dig

We use the **dig command** to check the configuration.

The dig command (domain information groper) is used to **ask the DNS name servers for an IP address corresponding to the given domain**.



```
admin20@dawserver:~$ dig server.cristinachiarri.org

; <<>> DiG 9.16.1-Ubuntu <<>> server.cristinachiarri.org
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 44135
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;server.cristinachiarri.org.    IN      A

;; ANSWER SECTION:
server.cristinachiarri.org. 3840 IN     A       192.168.1.5
```

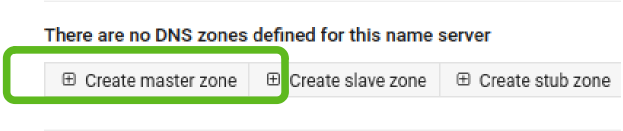


```
admin20@dawserver:~$ dig client.cristinachiarri.org

; <<>> DiG 9.16.1-Ubuntu <<>> client.cristinachiarri.org
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 5109
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;client.cristinachiarri.org.    IN      A

;; ANSWER SECTION:
client.cristinachiarri.org. 3840 IN     A       192.168.1.4
```

2.1.1.2 Configuring Lookup zone reverse

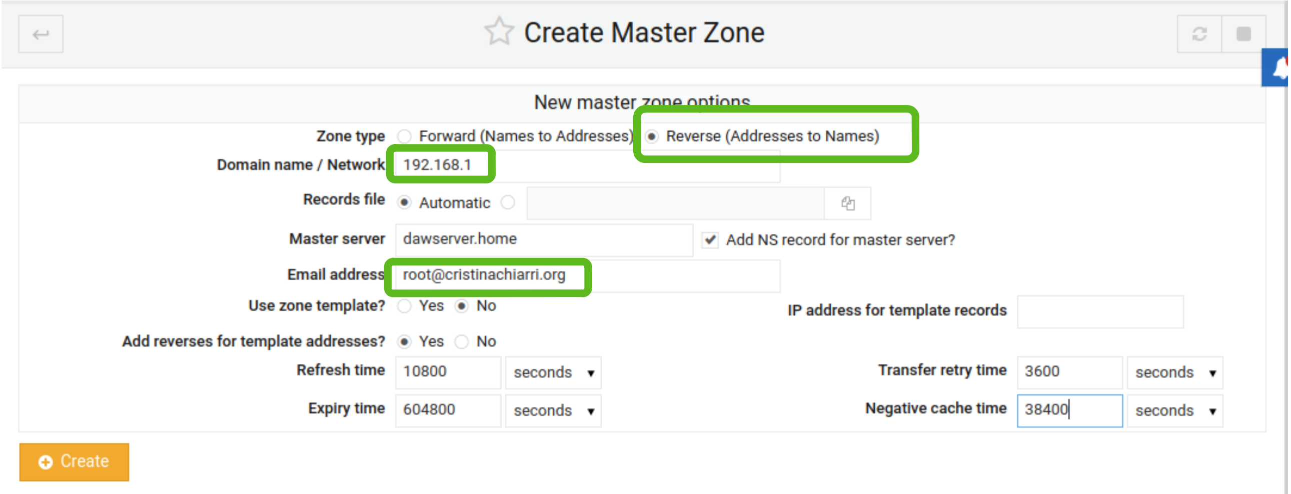
Reverse lookup zones **resolve IP addresses to names**.

- **Create a the masterzone**



There are no DNS zones defined for this name server

In this case, the zone type must be reverse.



New master zone options

Zone type ○ Forward (Names to Addresses) ● Reverse (Addresses to Names)

Domain name / Network: 192.168.1

Records file: ● Automatic ○

Master server: dawserver.home ☑ Add NS record for master server?

Email address: root@cristinachiarri.org

Use zone template? ○ Yes ● No

IP address for template records:

Add reverses for template addresses? ● Yes ○ No

Refresh time: 10800 seconds

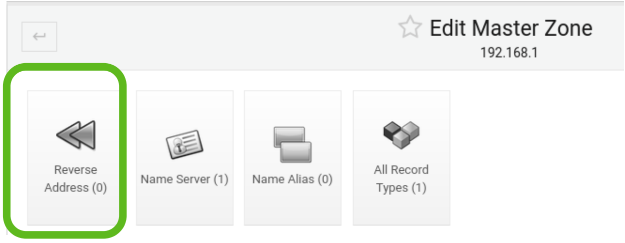
Transfer retry time: 3600 seconds

Expiry time: 604800 seconds

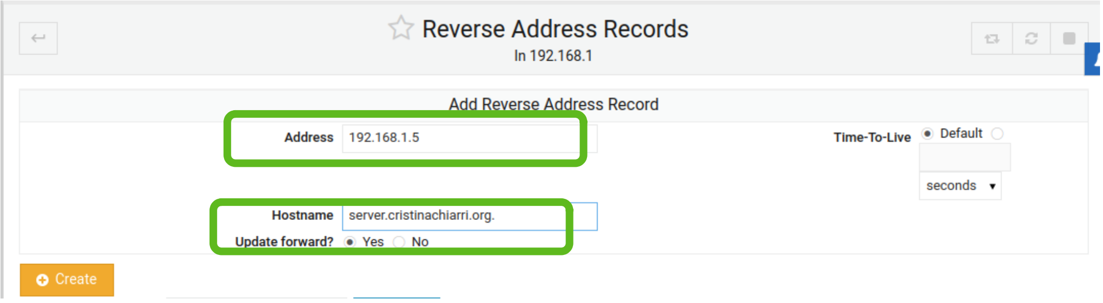
Negative cache time: 38400 seconds

- **Create new PTR records**

A reverse record or pointer record is a type of **DNS record that resolves an IP address to a domain or host name**, unlike an A record which points a domain name to an IP address.



We must create a reverse address record for each subdomain:



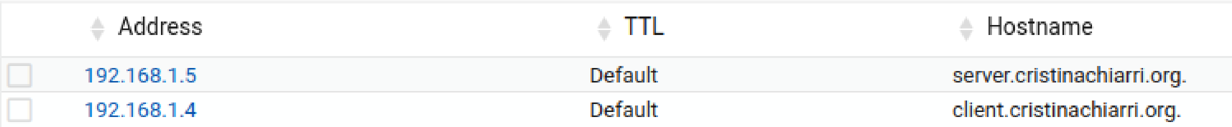
Add Reverse Address Record

Address: 192.168.1.5

Time-To-Live: ● Default ○ seconds

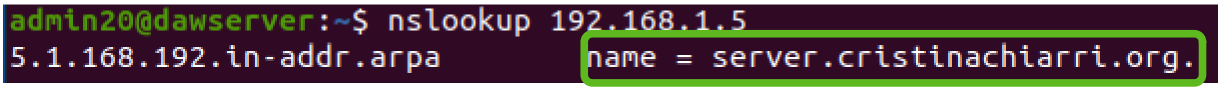
Hostname: server.cristinachiarri.org.

Update forward? ● Yes ○ No

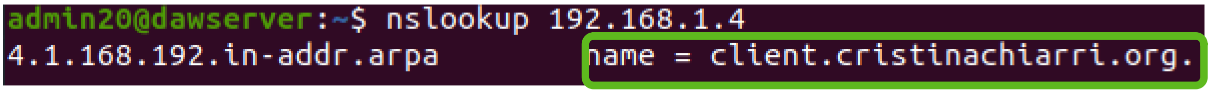


	Address	TTL	Hostname
□	192.168.1.5	Default	server.cristinachiarri.org.
□	192.168.1.4	Default	client.cristinachiarri.org.

Once applied the new configuration, we can check it using the command **nslookup <IP-address>**
“Name Server Lookup” is a network administration tool for querying the DNS to obtain domain name or IP address.



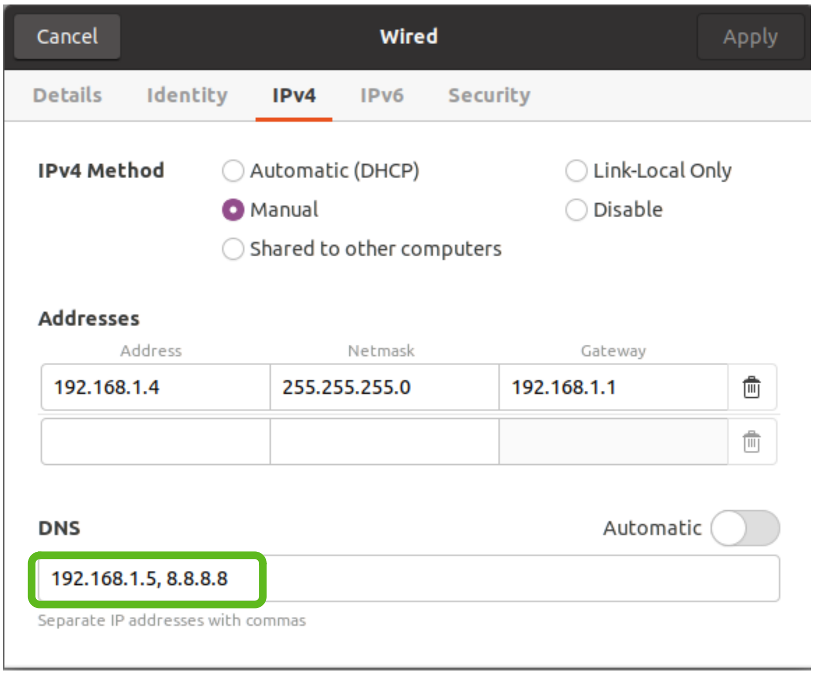
```
admin20@dawserver:~$ nslookup 192.168.1.5
5.1.168.192.in-addr.arpa        name = server.cristinachiarri.org.
```



```
admin20@dawserver:~$ nslookup 192.168.1.4
4.1.168.192.in-addr.arpa        name = client.cristinachiarri.org.
```

- ### Configuring the Client

Now we have to change the network configuration in the client virtual machine to set the DNS server the same way and we restart the network.



IPv4 Method
○ Automatic (DHCP) ○ Link-Local Only
● Manual ○ Disable
○ Shared to other computers

Addresses

Address	Netmask	Gateway
192.168.1.4	255.255.255.0	192.168.1.1

DNS Automatic ○

192.168.1.5, 8.8.8.8

Separate IP addresses with commas

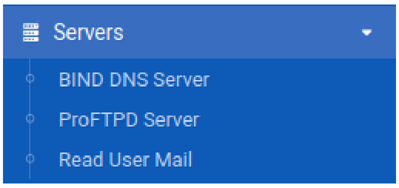
3 FTP

ProFTPD (Pro FTP daemon) is an FTP server.
FTP servers are used for file transfers across the internet. If you send files using FTP, files are either uploaded or downloaded to the FTP server.
The FTP connection allows you to transfer files from one machine to the other (drag and drop), as well as creating, renaming and deleting files and folders.

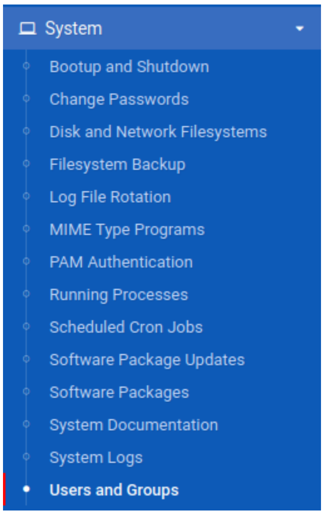
3.1 Installation

We need to **install the Webmin ProFTPD module**. We must go to Un-used modules as already described for BIND DNS Server.(2.1.1).

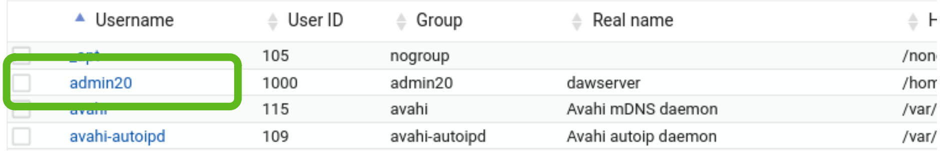
Once istalled, we have to **refresh the module**s and it is available in the Servers menu.



The **FTP servers use the OS users to allow connections**.
So we have to **configure our user to be able to connect to the FTP server**.
We must go to the Webmin System menu and then to Users and Groups.



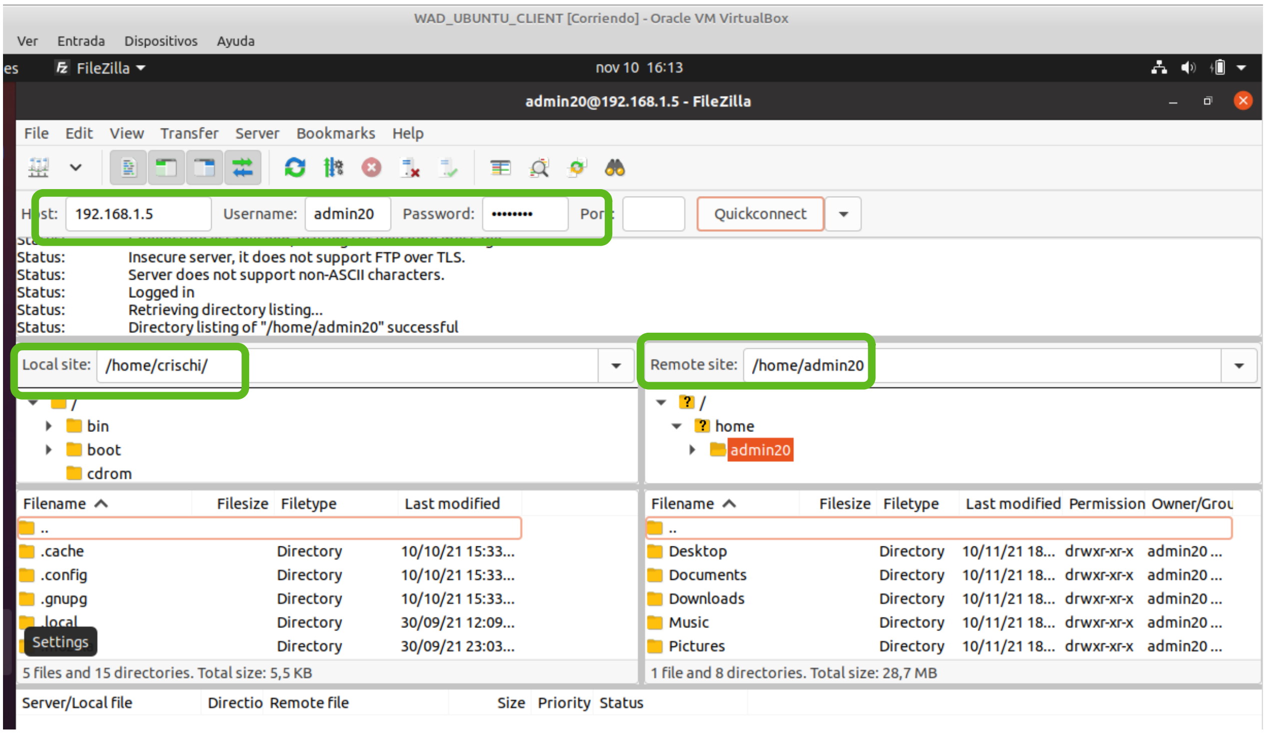
We can see the list with the users and groups and our user **admin20**



	Username	User ID	Group	Real name	H
□	_apt	105	nogroup		/non
□	admin20	1000	admin20	dawserver	/hom
□	avahi	115	avahi	Avahi mDNS daemon	/var/
□	avahi-autoipd	109	avahi-autoipd	Avahi autoip daemon	/var/

Check the connection from the client

Now we are going to test if we can connect from our Client to the FTP Server in the server machine using the user admin20, using an FTP Client software, in this case FileZilla.



Host: 192.168.1.5 Username: admin20 Password: •••••••• Port:

```
Status:     Insecure server, it does not support FTP over TLS.
Status:     Server does not support non-ASCII characters.
Status:     Logged in
Status:     Retrieving directory listing...
Status:     Directory listing of "/home/admin20" successful
```

Local site: /home/crischi/

```
/
  bin
  boot
  cdrom
```

Filename	Filesize	Filetype	Last modified
..			
.cache		Directory	10/10/21 15:33...
.config		Directory	10/10/21 15:33...
.gnupg		Directory	10/10/21 15:33...
.local		Directory	30/09/21 12:09...
		Directory	30/09/21 23:03...

5 files and 15 directories. Total size: 5,5 KB

Remote site: /home/admin20

```
/
  home
    admin20
```

Filename	Filesize	Filetype	Last modified	Permission	Owner/Grou
..					
Desktop		Directory	10/11/21 18...	drwxr-xr-x	admin20 ...
Documents		Directory	10/11/21 18...	drwxr-xr-x	admin20 ...
Downloads		Directory	10/11/21 18...	drwxr-xr-x	admin20 ...
Music		Directory	10/11/21 18...	drwxr-xr-x	admin20 ...
Pictures		Directory	10/11/21 18...	drwxr-xr-x	admin20 ...

1 file and 8 directories. Total size: 28,7 MB

Server/Local file	Directio	Remote file	Size	Priority	Status

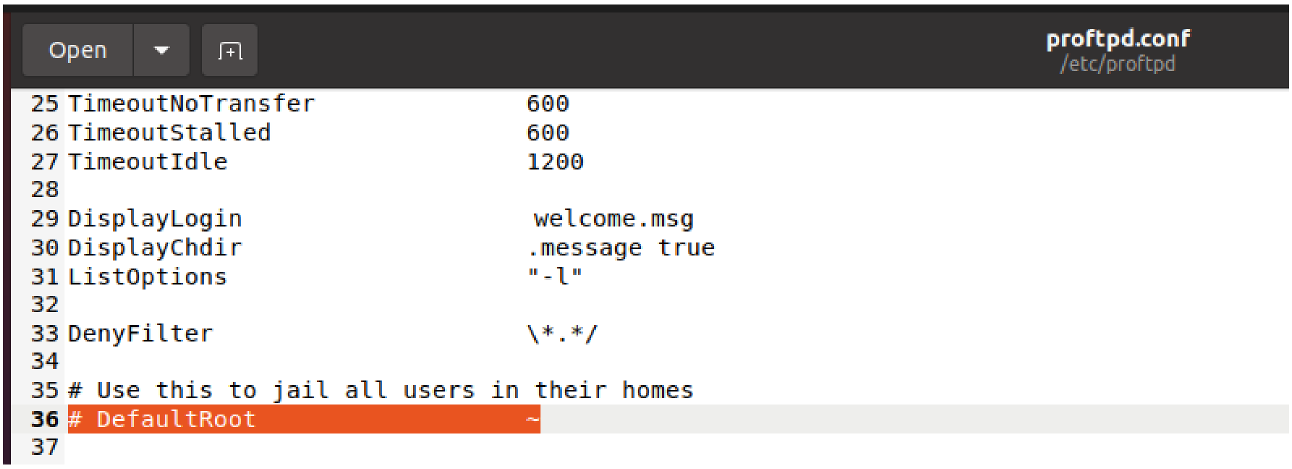
3.2 Configure permissions

We have to configure the server's user admin20 as follows:

- User must be jailed in his own user directory, can't access further information.
- User won't have write permissions.

Jail the ftp user

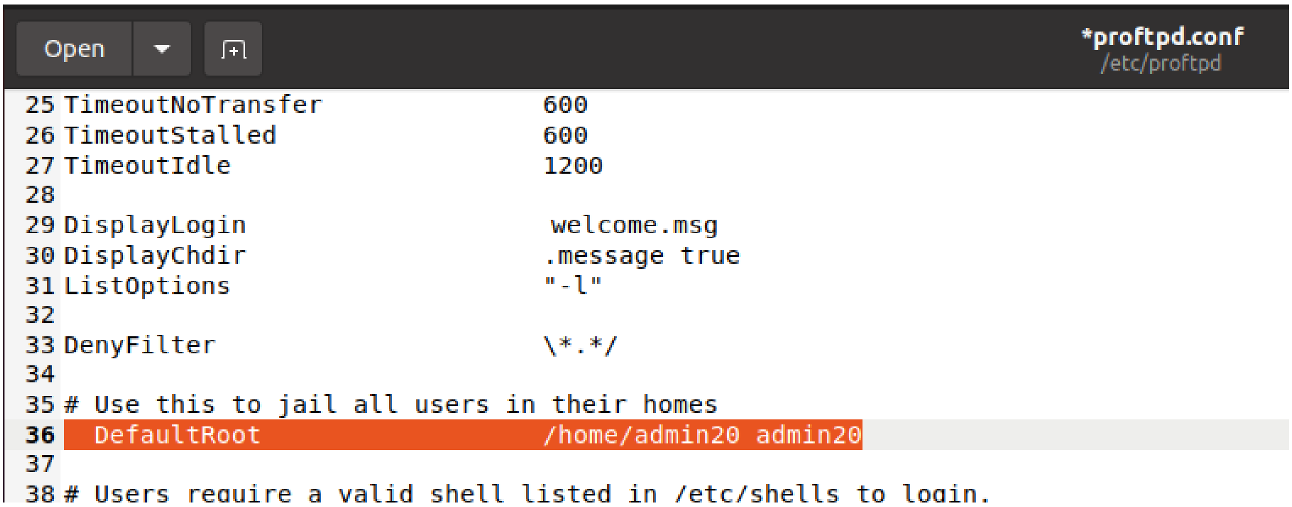
We can **edit the ProFTPd configuration file**:



```
TimeoutNoTransfer                600
TimeoutStalled                   600
TimeoutIdle                      1200

DisplayLogin                      welcome.msg
DisplayChdir                     .message true
ListOptions                      "-l"

DenyFilter                       \*.*/

# Use this to jail all users in their homes
# DefaultRoot                    ~

```

DefaultRoot is the parameter used by proftpd to enable the jail functionality.
admin 20 is the primary group of all users being chrooted and /home/admin20 is the directory where the user will be jailed.

So, we enable the DefaultRoot line removing the comment and we add the path.

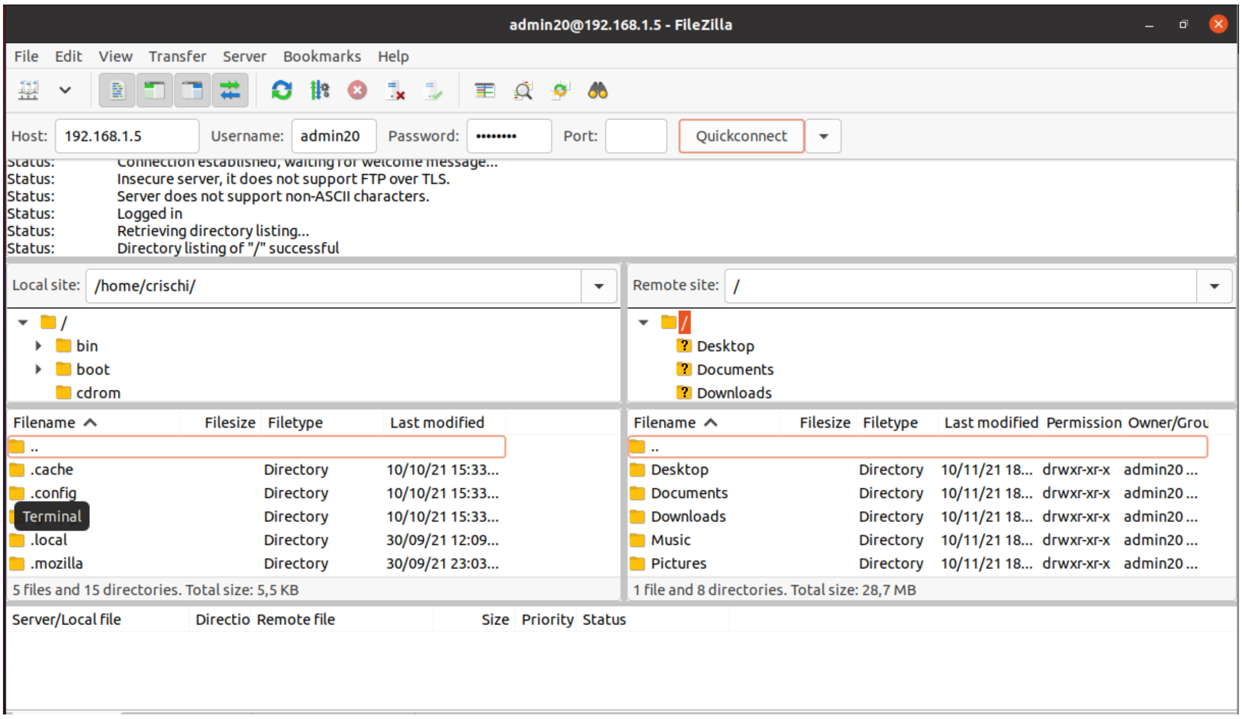


```
TimeoutNoTransfer                600
TimeoutStalled                   600
TimeoutIdle                      1200

DisplayLogin                      welcome.msg
DisplayChdir                     .message true
ListOptions                      "-l"

DenyFilter                       \*.*/

# Use this to jail all users in their homes
  DefaultRoot                    /home/admin20 admin20

# Users require a valid shell listed in /etc/shells to login.
```

Then we have to **restart the FTP server**: /etc/init.d/proftpd restart"

https://serverfault.com/questions/153701/how-to-jail-a-ftp-user-inside-its-home-directory-proftpd

Now we are going to connect with FileZilla from our Client to the FTP Server using admin20 to see if the user has been jailed correctly.



admin20@192.168.1.5 - FileZilla
File Edit View Transfer Server Bookmarks Help

Host: 192.168.1.5 Username: admin20 Password: •••••••• Port: Quickconnect

```
Status:    Connection established, waiting for welcome message...
Status:    Insecure server, it does not support FTP over TLS.
Status:    Server does not support non-ASCII characters.
Status:    Logged in
Status:    Retrieving directory listing...
Status:    Directory listing of "/" successful
```

Local site: /home/crischi/

- /
  - bin
  - boot
  - cdrom

Filename	Filesize	Filetype	Last modified
..			
.cache		Directory	10/10/21 15:33...
.config		Directory	10/10/21 15:33...
Terminal		Directory	10/10/21 15:33...
.local		Directory	30/09/21 12:09...
.mozilla		Directory	30/09/21 23:03...

5 files and 15 directories. Total size: 5,5 KB

Remote site: /

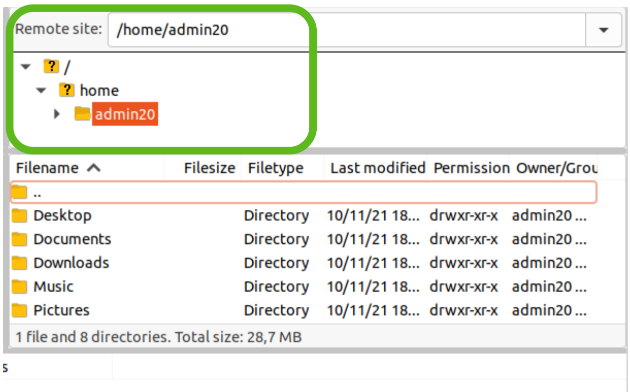
- /
  - Desktop
  - Documents
  - Downloads

Filename	Filesize	Filetype	Last modified	Permission	Owner/Grou
..					
Desktop		Directory	10/11/21 18...	drwxr-xr-x	admin20 ...
Documents		Directory	10/11/21 18...	drwxr-xr-x	admin20 ...
Downloads		Directory	10/11/21 18...	drwxr-xr-x	admin20 ...
Music		Directory	10/11/21 18...	drwxr-xr-x	admin20 ...
Pictures		Directory	10/11/21 18...	drwxr-xr-x	admin20 ...

1 file and 8 directories. Total size: 28,7 MB

Server/Local file	Directio	Remote file	Size	Priority	Status

If we compare both connections, before and after jailing process, we can see that now, the home directory is not accessible anymore. The user can now only access to his own directory.

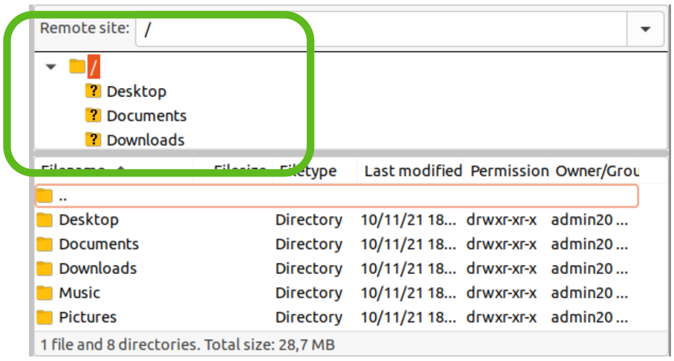


Remote site: /home/admin20

- /
  - home
    - admin20

Filename	Filesize	Filetype	Last modified	Permission	Owner/Grou
..					
Desktop		Directory	10/11/21 18...	drwxr-xr-x	admin20 ...
Documents		Directory	10/11/21 18...	drwxr-xr-x	admin20 ...
Downloads		Directory	10/11/21 18...	drwxr-xr-x	admin20 ...
Music		Directory	10/11/21 18...	drwxr-xr-x	admin20 ...
Pictures		Directory	10/11/21 18...	drwxr-xr-x	admin20 ...

1 file and 8 directories. Total size: 28,7 MB



Remote site: /

- /
  - Desktop
  - Documents
  - Downloads

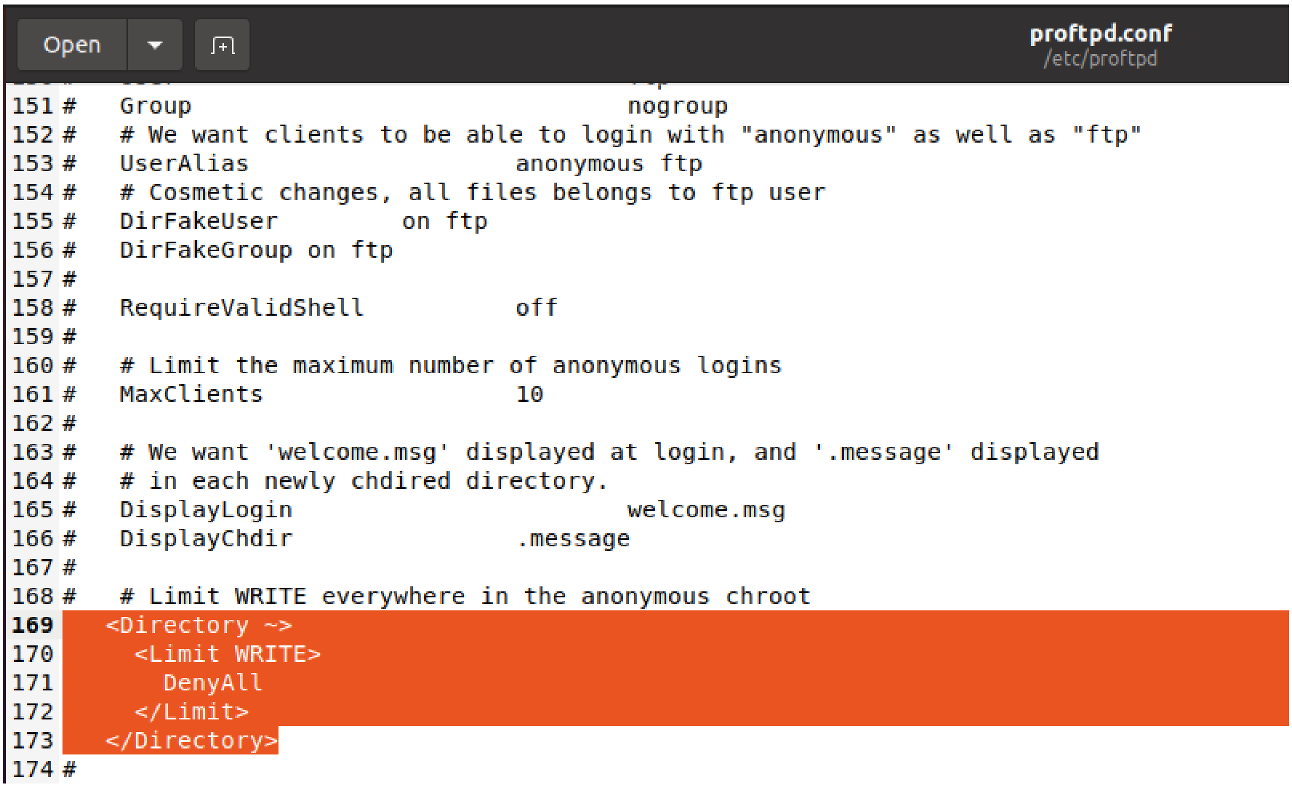
Filename	Filesize	Filetype	Last modified	Permission	Owner/Grou
..					
Desktop		Directory	10/11/21 18...	drwxr-xr-x	admin20 ...
Documents		Directory	10/11/21 18...	drwxr-xr-x	admin20 ...
Downloads		Directory	10/11/21 18...	drwxr-xr-x	admin20 ...
Music		Directory	10/11/21 18...	drwxr-xr-x	admin20 ...
Pictures		Directory	10/11/21 18...	drwxr-xr-x	admin20 ...

1 file and 8 directories. Total size: 28,7 MB

Deny write permission

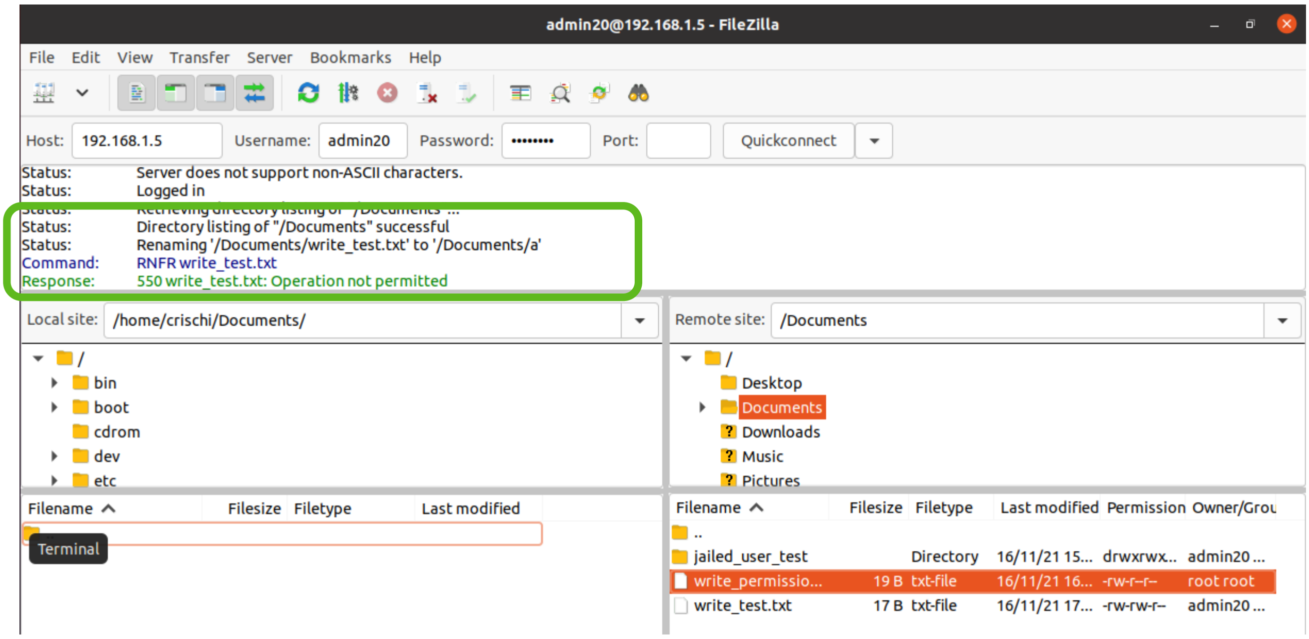
We must edit the **ProFTPd configuration file** once again.

We have to remove the comments from lines 169 to 173, to **enable Limit write directive.**



```
151 #   Group                                nogroup
152 #   # We want clients to be able to login with "anonymous" as well as "ftp"
153 #   UserAlias                   anonymous ftp
154 #   # Cosmetic changes, all files belongs to ftp user
155 #   DirFakeUser        on ftp
156 #   DirFakeGroup on ftp
157 #
158 #   RequireValidShell           off
159 #
160 #   # Limit the maximum number of anonymous logins
161 #   MaxClients                  10
162 #
163 #   # We want 'welcome.msg' displayed at login, and '.message' displayed
164 #   # in each newly chdired directory.
165 #   DisplayLogin                         welcome.msg
166 #   DisplayChdir                .message
167 #
168 #   # Limit WRITE everywhere in the anonymous chroot
169   <Directory ~>
170     <Limit WRITE>
171       DenyAll
172     </Limit>
173   </Directory>
174 #
```

If we connect with FileZilla from our Client using admin20, and we try to modify a file created previously in the server's user directory, we can see a message "Operation not permited".



admin20@192.168.1.5 - FileZilla
File Edit View Transfer Server Bookmarks Help
Quickconnect
Terminal

Host: 192.168.1.5 Username: admin20 Password: •••••••• Port:

```
Status:     Server does not support non-ASCII characters.
Status:     Logged in
Status:     Retrieving directory listing of "/Documents"...
Status:     Directory listing of "/Documents" successful
Status:     Renaming '/Documents/write_test.txt' to '/Documents/a'
Command:    RNFR write_test.txt
Response:   550 write_test.txt: Operation not permitted
```

Local site: /home/crischi/Documents/

```
/
  bin
  boot
  cdrom
  dev
  etc
```

Filename	Filesize	Filetype	Last modified

Remote site: /Documents

```
/
  Desktop
  Documents
  Downloads
  Music
  Pictures
```

Filename	Filesize	Filetype	Last modified	Permission	Owner/Grou
..					
jailed_user_test		Directory	16/11/21 15...	drwxrwx...	admin20 ...
write_permissio...	19 B	txt-file	16/11/21 16...	-rw-r--r--	root root
write_test.txt	17 B	txt-file	16/11/21 17...	-rw-rw-r--	admin20 ...

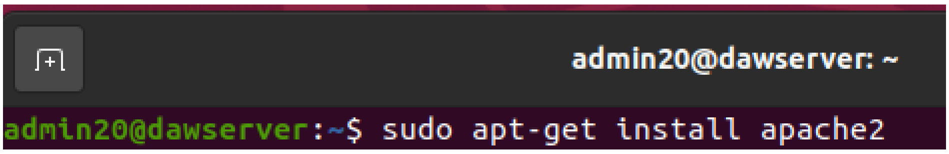
https://serverfault.com/questions/236874/proftpd-disable-writing-and-deleting-to-a-particular-directory

4 WEB SERVER

I am going to install Apache web server for my activity.

A web server is a program or a set of programs allowing two or more programs to communicate over a network.

4.1 Apache web server installation

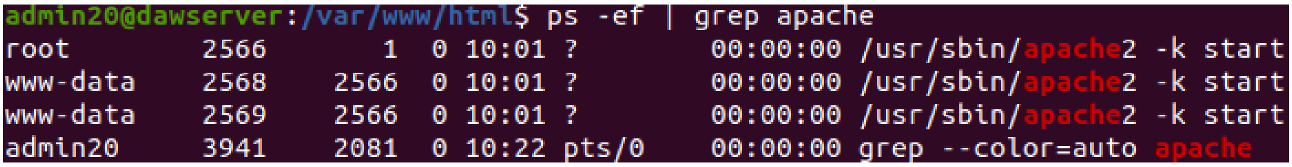


```
admin20@dawserver: ~
admin20@dawserver:~$ sudo apt-get install apache2
```

The following elements have been created:

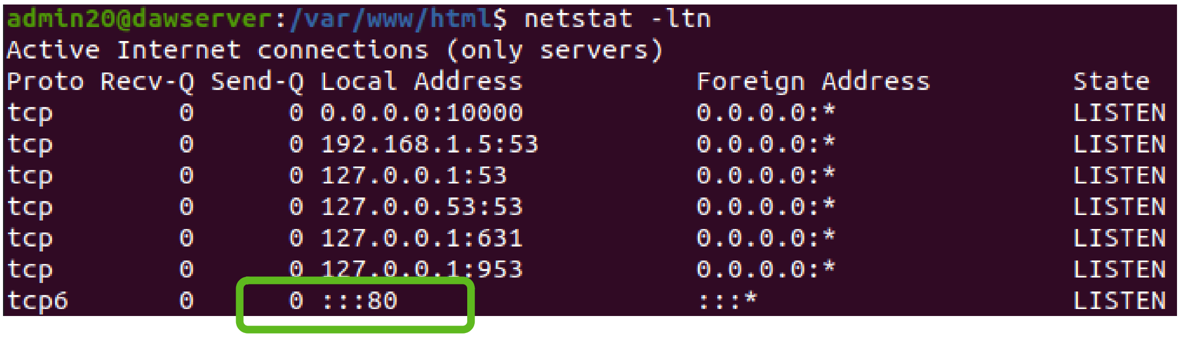
- configuration files
- user and group www-data (Apache uses them to request the queries.)
- root directory of the default virtual server /var/www/html
- root directory default page /var/www/html/index.html

We can see that **Apache is running** using the command ps that enables you to check the status of active processes on a system and display technical information about the processes.



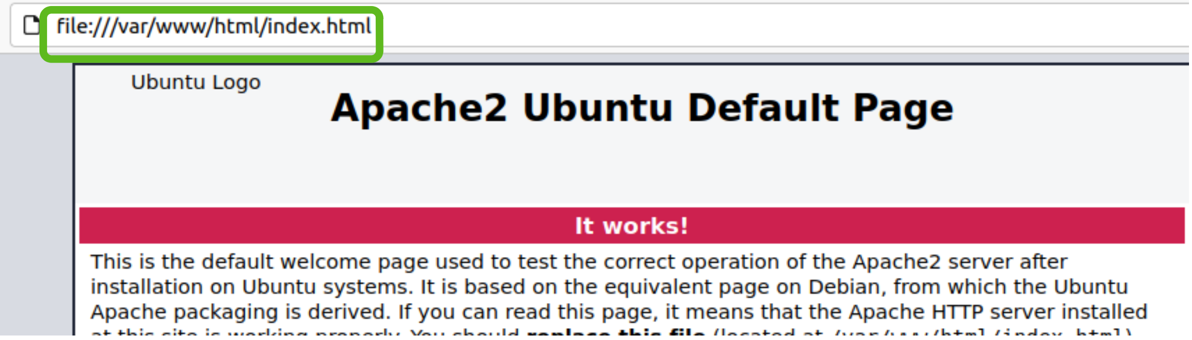
```
admin20@dawserver:/var/www/html$ ps -ef | grep apache
root        2566       1  0 10:01 ?        00:00:00 /usr/sbin/apache2 -k start
www-data    2568    2566  0 10:01 ?        00:00:00 /usr/sbin/apache2 -k start
www-data    2569    2566  0 10:01 ?        00:00:00 /usr/sbin/apache2 -k start
admin20     3941    2081  0 10:22 pts/0    00:00:00 grep --color=auto apache
```

We can aslo **check that Apache is listening in port 80**/TCP using the netstat command, used to show network status.



```
admin20@dawserver:/var/www/html$ netstat -ltn
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:10000           0.0.0.0:*               LISTEN
tcp        0      0 192.168.1.5:53          0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:53            0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:953           0.0.0.0:*               LISTEN
tcp6       0      0 :::80                   :::*                    LISTEN
```

We can see the Apache default page in the browser of our server machine.



file:///var/www/html/index.html

Ubuntu Logo

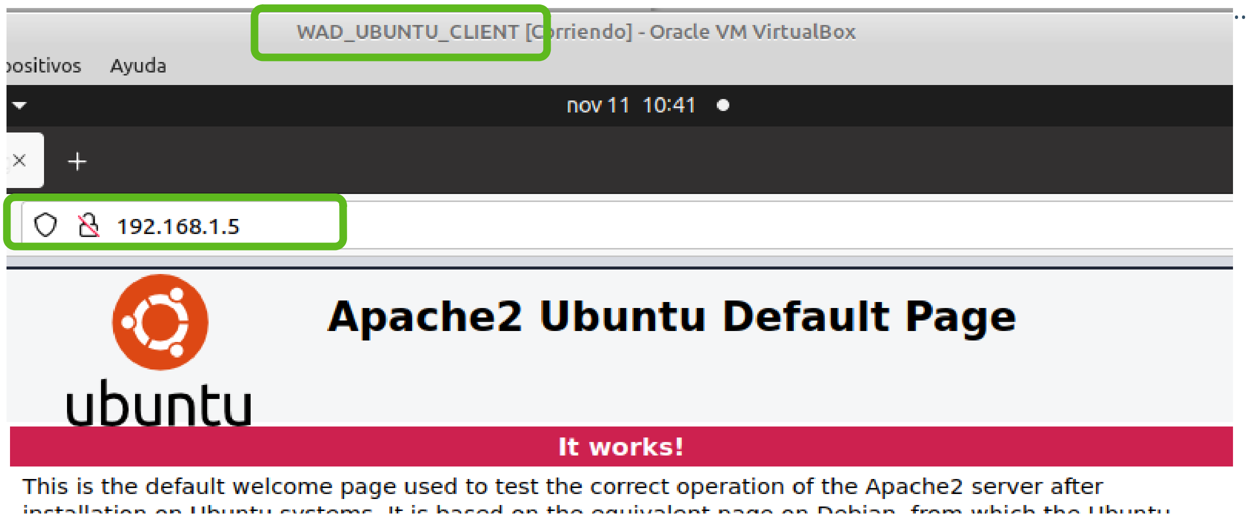
Apache2 Ubuntu Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at /var/www/html/index.html)

4.1.1 Check the connection from the client

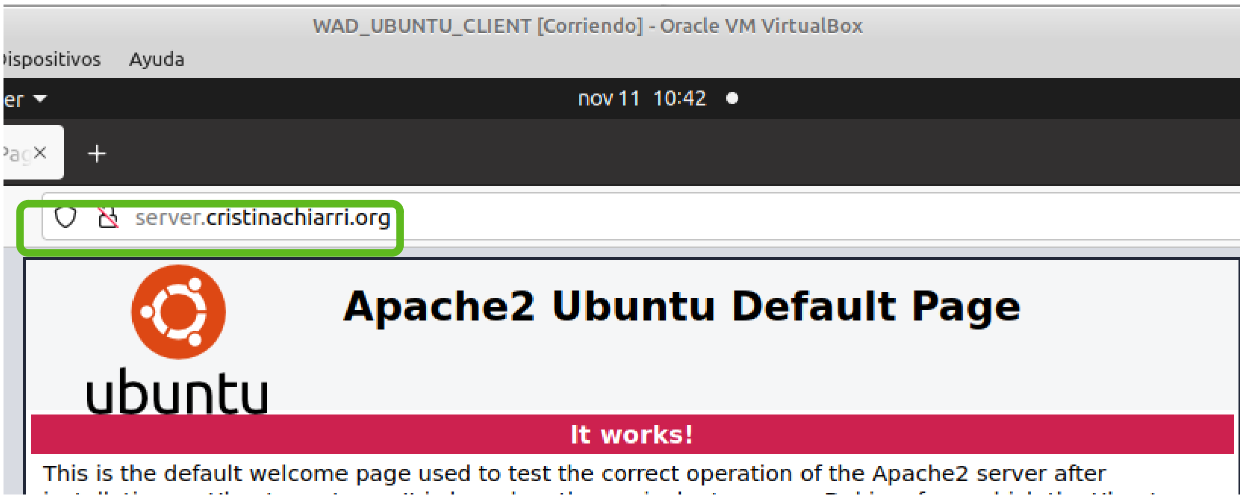
We have to check that the web server is reacheable from our client machine using the IP address or the domain name configured in our DNS server. (2.1.1.1)



Apache2 Ubuntu Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu


WAD_UBUNTU_CLIENT [Corriendo] - Oracle VM VirtualBox
ispositivos
Ayuda
er
nov 11 10:42
Pag
server.cristinachiarri.org
ubuntu

Apache2 Ubuntu Default Page

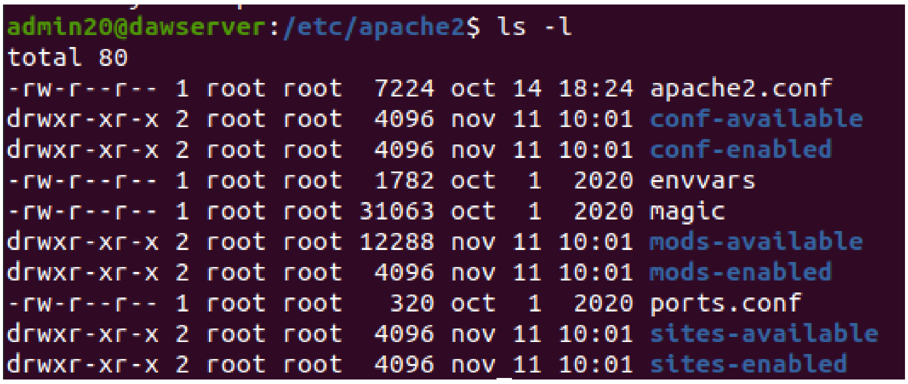
It works!

This is the default welcome page used to test the correct operation of the Apache2 server after

4.1.2 Check the configuration files

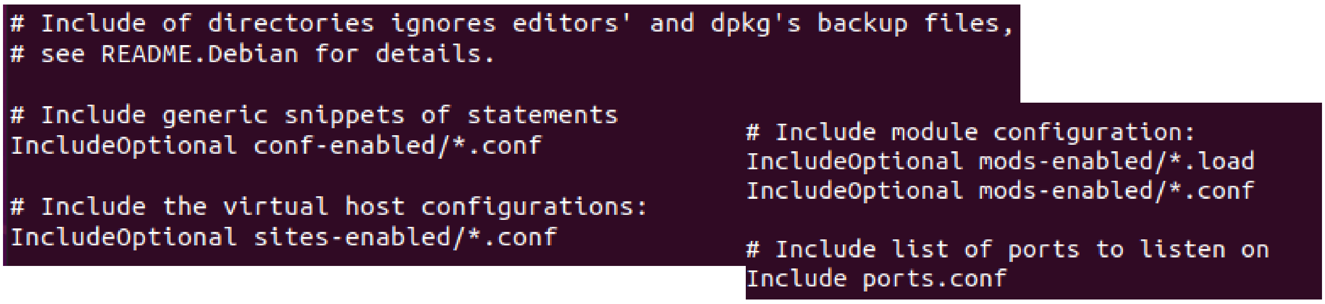
We must confirm that the configuration files are set correctly.

Here we can see the content of our apache2 directory



```
admin20@dawserver:/etc/apache2$ ls -l
total 80
-rw-r--r-- 1 root root  7224 oct 14 18:24 apache2.conf
drwxr-xr-x 2 root root  4096 nov 11 10:01 conf-available
drwxr-xr-x 2 root root  4096 nov 11 10:01 conf-enabled
-rw-r--r-- 1 root root  1782 oct  1  2020 envvars
-rw-r--r-- 1 root root 31063 oct  1  2020 magic
drwxr-xr-x 2 root root 12288 nov 11 10:01 mods-available
drwxr-xr-x 2 root root  4096 nov 11 10:01 mods-enabled
-rw-r--r-- 1 root root   320 oct  1  2020 ports.conf
drwxr-xr-x 2 root root  4096 nov 11 10:01 sites-available
drwxr-xr-x 2 root root  4096 nov 11 10:01 sites-enabled
```

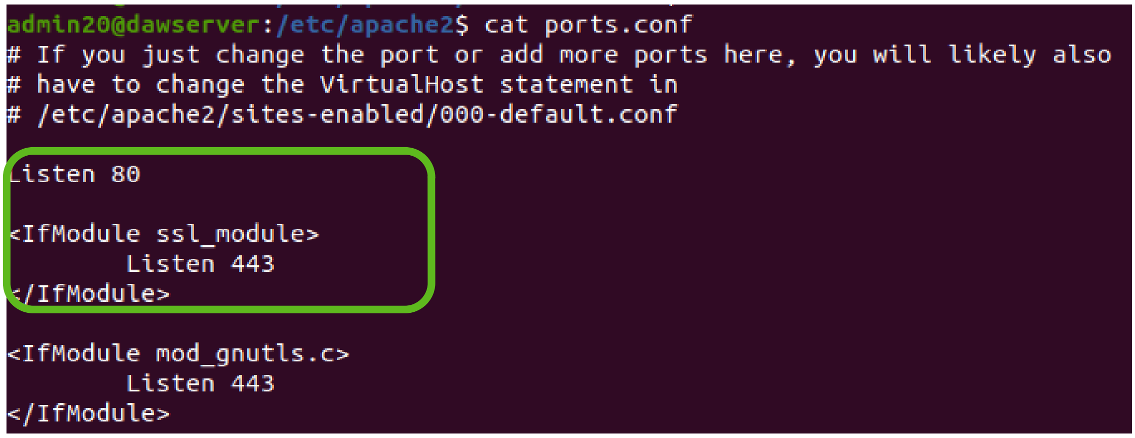
- We check that apache2.conf content include directives to other files



```
# Include of directories ignores editors' and dpkg's backup files,
# see README.Debian for details.

# Include generic snippets of statements
IncludeOptional conf-enabled/*.conf

# Include the virtual host configurations:
IncludeOptional sites-enabled/*.conf
```

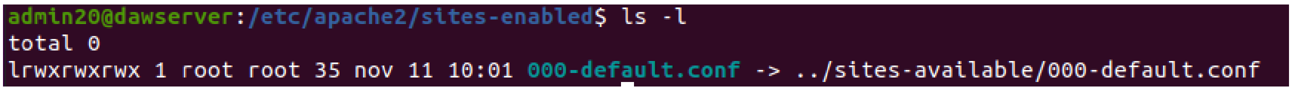
```
# Include module configuration:
IncludeOptional mods-enabled/*.load
IncludeOptional mods-enabled/*.conf

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

- We check that the **ports are configured properly** (80 to HTTP and 443 to HTTPS requests) checking the content of the file ports.confls



```
admin20@dawserver:/etc/apache2$ cat 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

<IfModule ssl_module>
        Listen 443
</IfModule>

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

- We list the contents of /etc/apache2/sites-enabled to confirm that the file **000-default.conf** exists. It also exists in the directory /etc/apache2/sites-available



```
admin20@dawserver:/etc/apache2/sites-enabled$ ls -l
total 0
lrwxrwxrwx 1 root root 35 nov 11 10:01 000-default.conf -> ../sites-available/000-default.conf
```

This file includes the performance of the virtual server by default.

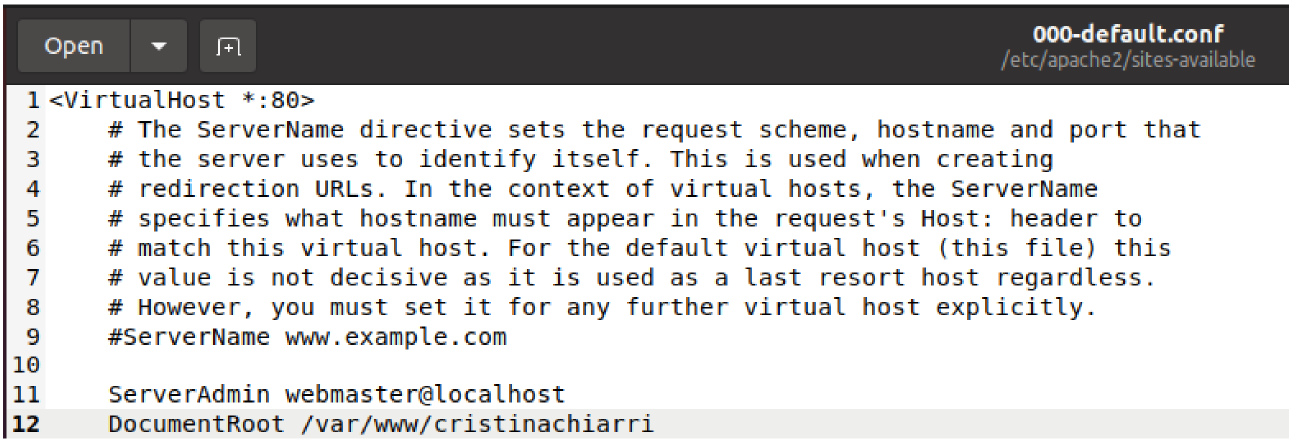
4.2 Applying the activity required configuration

The root directory must be **/var/www/cristinachiarri**

4.2.1 Create the virtual host

Create the directories and files

I change the configuration file **000-default.conf** and modify the DocumentRoot value from **/var/www/html** to **var/www/cristinachiarri**



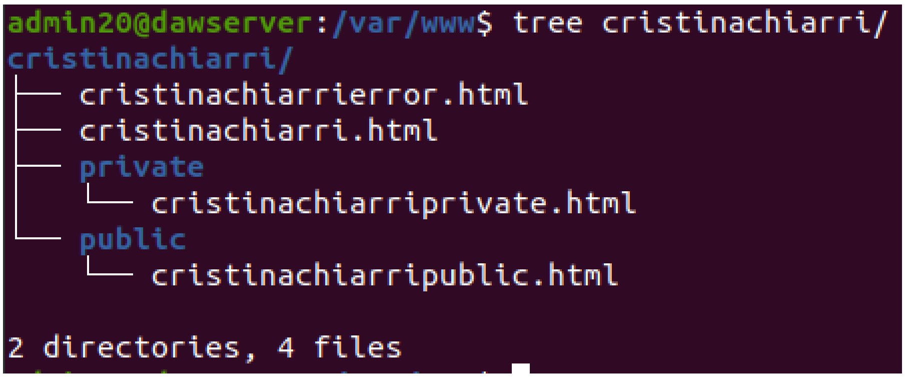
```
<VirtualHost *:80>
	# The ServerName directive sets the request scheme, hostname and port that
	# the server uses to identify itself. This is used when creating
	# redirection URLs. In the context of virtual hosts, the ServerName
	# specifies what hostname must appear in the request's Host: header 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/cristinachiarri
```

Now I am going to create the folder structure.

First, we have to create the folders cristinachiarri , cristinachiarri/public and cristinachiarri/private with the command **mkdir**.

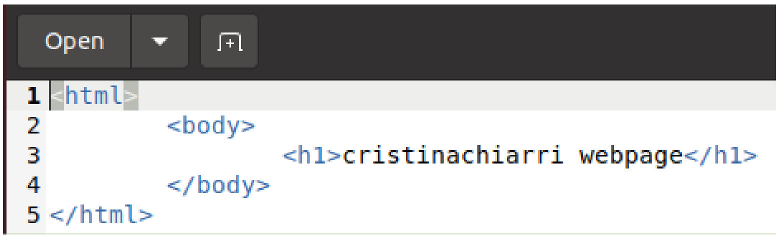
Next, we have to create the html files with sudo **gedit,** in each case, in the correcto folder.

This is the final crsitinachiarri folder's structure:



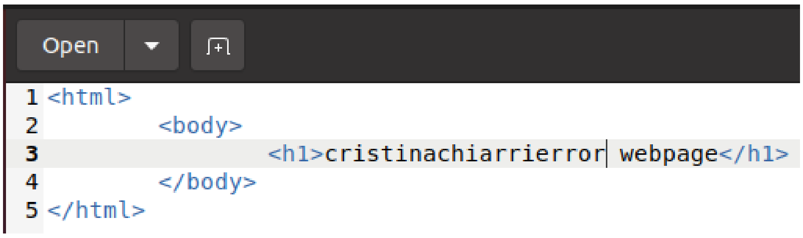
```
admin20@dawserver:/var/www$ tree cristinachiarri/
cristinachiarri/
├── cristinachiarrierror.html
├── cristinachiarri.html
├── private
│   └── cristinachiarriprivate.html
└── public
    └── cristinachiarripublic.html

2 directories, 4 files
```

Now I am going to include the content of each html file:
cristinachiarri.html



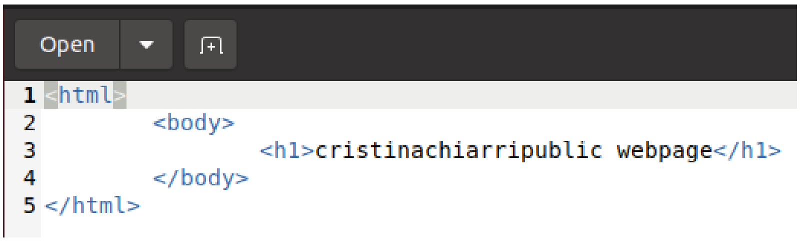
```
<html>
        <body>
                <h1>cristinachiarri webpage</h1>
        </body>
</html>
```

cristinachiarrierror.html



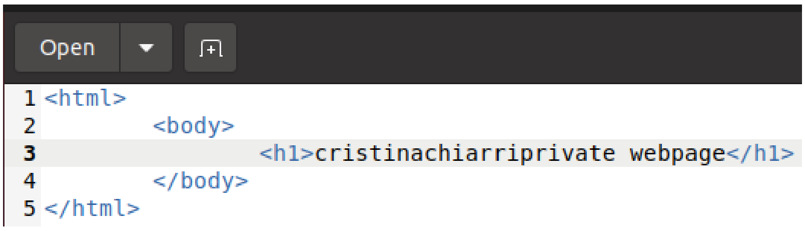
```
<html>
        <body>
                <h1>cristinachiarrierror webpage</h1>
        </body>
</html>
```

cristinachiarripublic.html



```
<html>
        <body>
                <h1>cristinachiarripublic webpage</h1>
        </body>
</html>
```

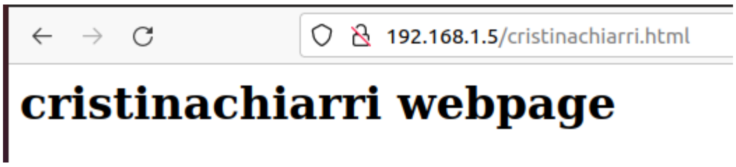
cristinachiarriprivate.html



```
<html>
        <body>
                <h1>cristinachiarriprivate webpage</h1>
        </body>
</html>
```

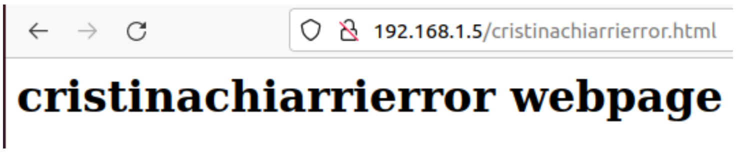
Check the connection

If we connect from the client, we can see our directories and html archives.



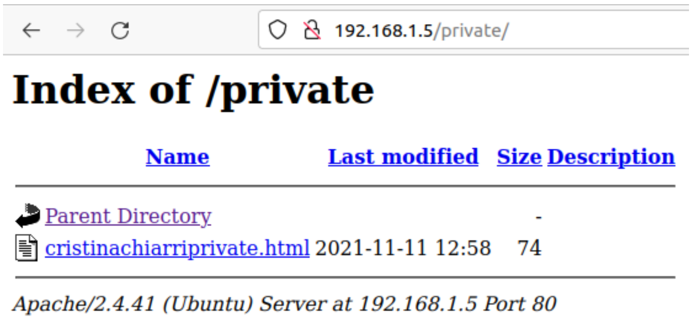
192.168.1.5/cristinachiarri.html

cristinachiarri webpage



192.168.1.5/cristinachiarrierror.html

cristinachiarrierror webpage

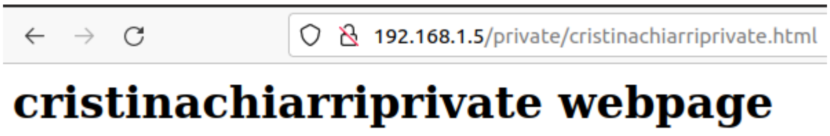


192.168.1.5/private/

Index of /private

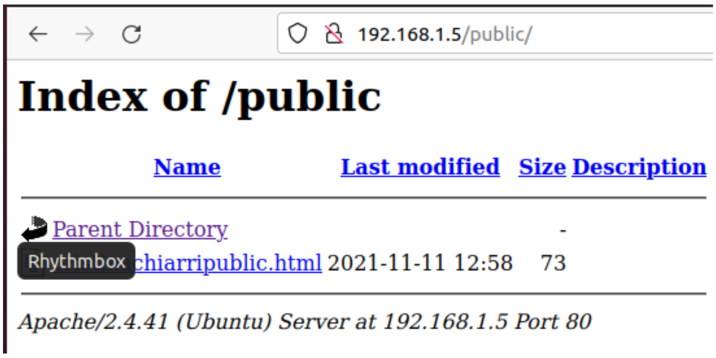
Name	Last modified	Size	Description
Parent Directory		-	
cristinachiarriprivate.html	2021-11-11 12:58	74	

Apache/2.4.41 (Ubuntu) Server at 192.168.1.5 Port 80



192.168.1.5/private/cristinachiarriprivate.html

cristinachiarriprivate webpage

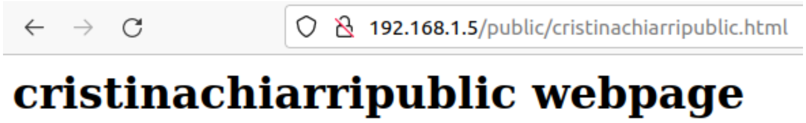


192.168.1.5/public/

Index of /public

Name	Last modified	Size	Description
Parent Directory		-	
Rhythmbox chiarripublic.html	2021-11-11 12:58	73	

Apache/2.4.41 (Ubuntu) Server at 192.168.1.5 Port 80



192.168.1.5/public/cristinachiarripublic.html

cristinachiarripublic webpage

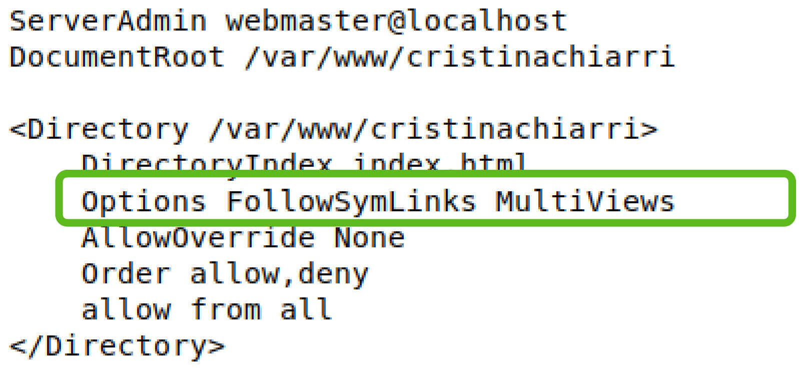
4.2.2 Change the default page by default and directory options

The content must not be indexed in this exercise.

But if the server does not find the file index.html in the root directory (/var/www/cristinachiarri) it indexes the content of the directory.

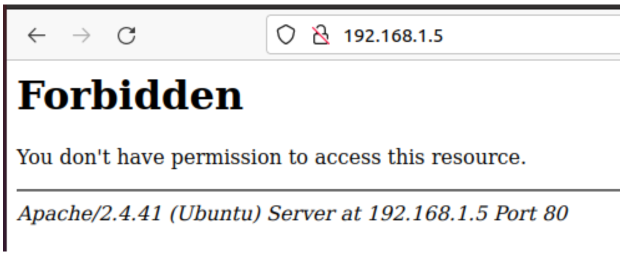
We need to change the configuration file **000-default.conf.**

We have to **add a <Directory> directive** that specifies that we don't want the content to be indexed.
We use:
Options **Indexes** FollowSymLinks MultiViews, if we want to index the content.
Options FollowSymLinks MultiViews , if we does not want to index the content.



```
ServerAdmin webmaster@localhost
DocumentRoot /var/www/cristinachiarri

<Directory /var/www/cristinachiarri>
    DirectoryIndex index.html
    Options FollowSymLinks MultiViews
    AllowOverride None
    Order allow,deny
    allow from all
</Directory>
```

But if we does not have an index.html and we doesn't index the content, when we connect from the client this is what we have:

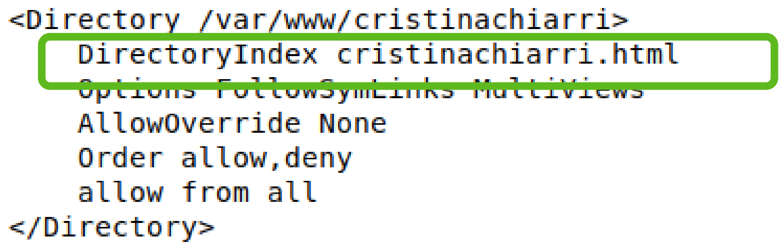


Forbidden

You don't have permission to access this resource.

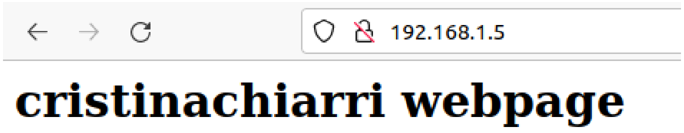
Apache/2.4.41 (Ubuntu) Server at 192.168.1.5 Port 80

We are goint to use cristinachiarri.html as default page to be loaded.
We just have to set the correct html file in the configuration file **000-default.conf** directive.



```
<Directory /var/www/cristinachiarri>
    DirectoryIndex cristinachiarri.html
    Options FollowSymLinks MultiViews
    AllowOverride None
    Order allow,deny
    allow from all
</Directory>
```

If we restart the Apache server, we can connect and the server shows the page as configured.

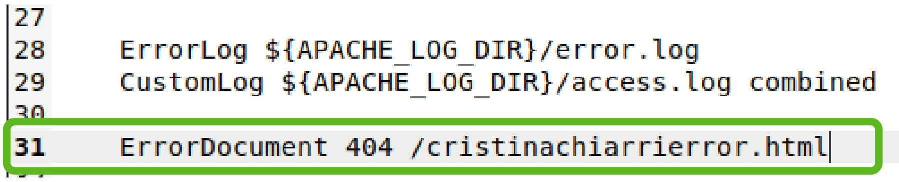


cristinachiarri webpage

4.2.3 Configure error codes

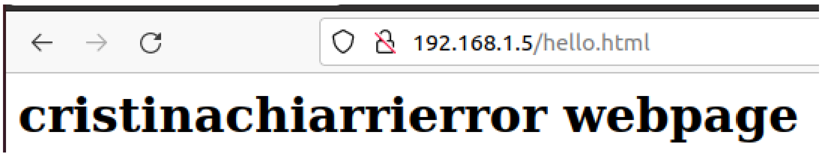
Now, we are going to configure the server for the case when the file is not found.
In this case, we want to show a specific webpage: cristinachiarrierror.html.

Once again, we are going to configure the configuration file **000-default.conf** to return a personalized message if the requested URL was not found on the server.
We have to **insert the line with the directive ErrorDocument** as we can see below.



```

    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined

    ErrorDocument 404 /cristinachiarrierror.html
```

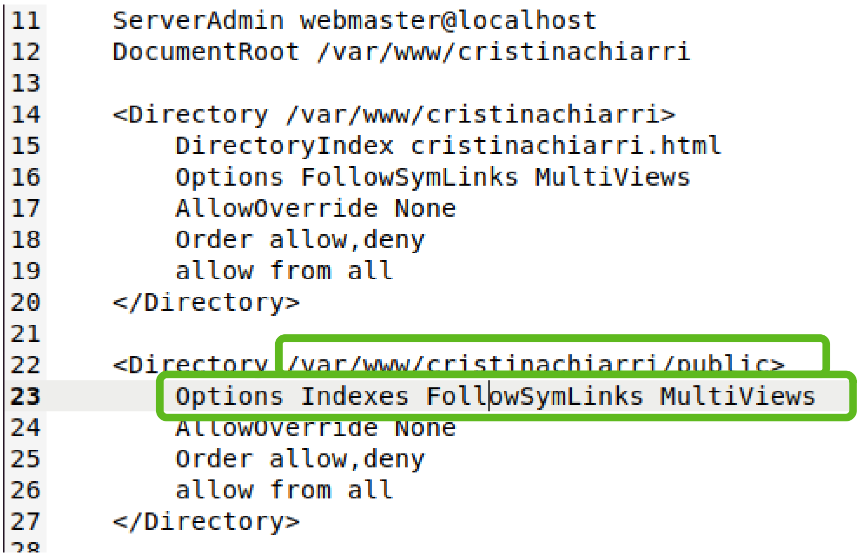
If we **restart apache** and connect from the client, we can see crsitinachiarrierror.html



cristinachiarrierror webpage

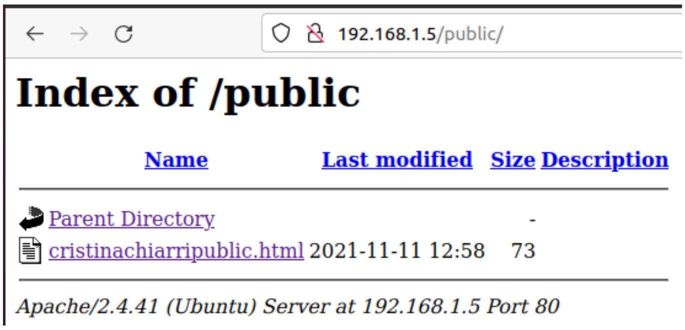
4.2.4 Show the index content cristinachiarri/public

In order to show the content of the public folder, we have to add a new directive to the configuration file **000-default.conf adding the option “**Options **Indexes** FollowSymLinks MultiViews,” as seen previously.



```
    ServerAdmin webmaster@localhost
    DocumentRoot /var/www/cristinachiarri

    <Directory /var/www/cristinachiarri>
        DirectoryIndex cristinachiarri.html
        Options FollowSymLinks MultiViews
        AllowOverride None
        Order allow,deny
        allow from all
    </Directory>

    <Directory /var/www/cristinachiarri/public>
        Options Indexes FollowSymLinks MultiViews
        AllowOverride None
        Order allow,deny
        allow from all
    </Directory>
```

If we **restart apache** and connect from the client, we can see the content indexed.



Index of /public

Name	Last modified	Size	Description
Parent Directory		-	
cristinachiarripublic.html	2021-11-11 12:58	73	

Apache/2.4.41 (Ubuntu) Server at 192.168.1.5 Port 80

4.2.5 Configure the access control for cristinachiarri/private

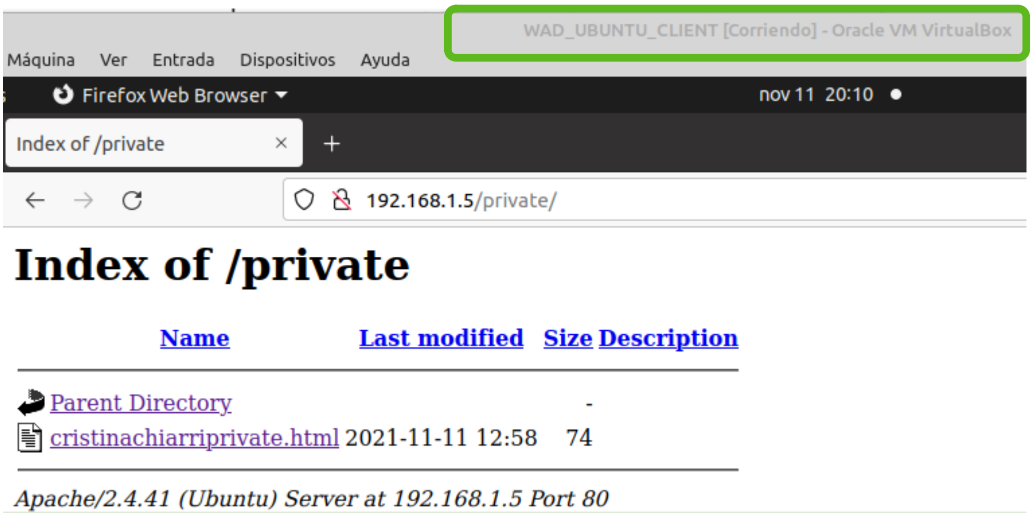
4.2.5.1 Allow only 192.68.1.4 IP

Cristinachiarri.org/private will only be accessed by the client IP, in this case: 192.168.1.4 and user chiarri using HTTP Basic authentication

We have to **add a new directive to the configuration file 000-default.conf** to allow the connection only from the client IP.

```
<Directory /var/www/cristinachiarri/private>
    Options Indexes FollowSymLinks MultiViews
    AllowOverride None
    Order allow,deny
    allow from 192.168.1.4
</Directory>
```

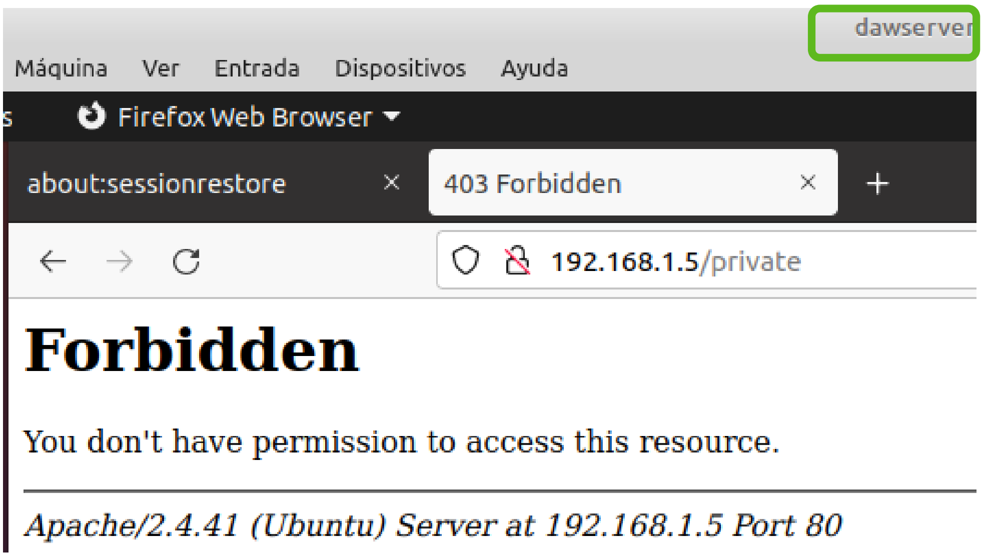
If we r**estart apache** we can see that we are allowed to connect only from the client



Index of /private

Name	Last modified	Size	Description
Parent Directory		-	
cristinachiarriprivate.html	2021-11-11 12:58	74	

Apache/2.4.41 (Ubuntu) Server at 192.168.1.5 Port 80



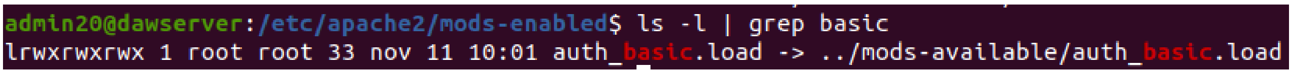
Forbidden

You don't have permission to access this resource.

Apache/2.4.41 (Ubuntu) Server at 192.168.1.5 Port 80

4.2.5.2 Allow only user chiarri using HTTP Basic authentication

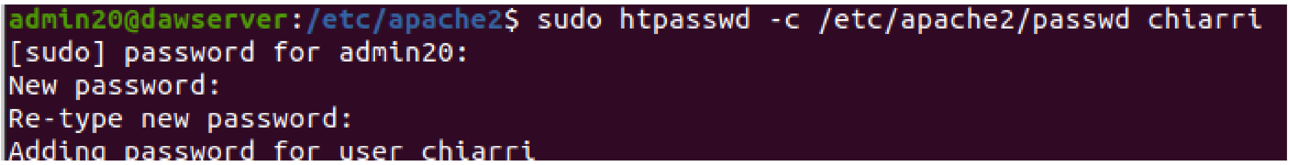
We have to **check in the directory /etc/apache2/mods-enabled if the auth_basic module is enabled**



```
admin20@dawserver:/etc/apache2/mods-enabled$ ls -l | grep basic
lrwxrwxrwx 1 root root 33 nov 11 10:01 auth_basic.load -> ../mods-available/auth_basic.load
```

- **Create a basic authentication file for user chiarri**

To use the HTTP Basic authentication we have to **create a file to store users and passwords**.
sudo htpasswd -c /etc/apache2/passwd chiarri
htpasswd is used to create the file passwd whith the user chiarri name and password. It encrypts the password using bcrypt



```
admin20@dawserver:/etc/apache2$ sudo htpasswd -c /etc/apache2/passwd chiarri
[sudo] password for admin20:
New password:
Re-type new password:
Adding password for user chiarri
```

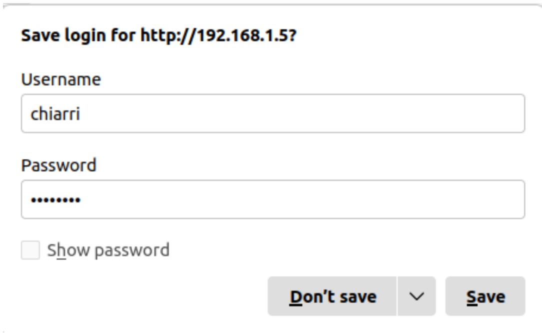
- **Add a directive**

We have to add a new directive to the configuration file 000-default.conf to **allow the connection for user chiarri**.

```
<Directory /var/www/cristinachiarri/private>
    Options Indexes FollowSymLinks MultiViews
    AllowOverride None
    Order allow,deny
    allow from 192.168.1.4
    AuthType Basic
    AuthName "Restricted access"
    AuthUserFile /etc/apache2/passwd
    Require user chiarri
</Directory>
```

If we **restart apache** and try to connect from the client, a sign in window is displayed.

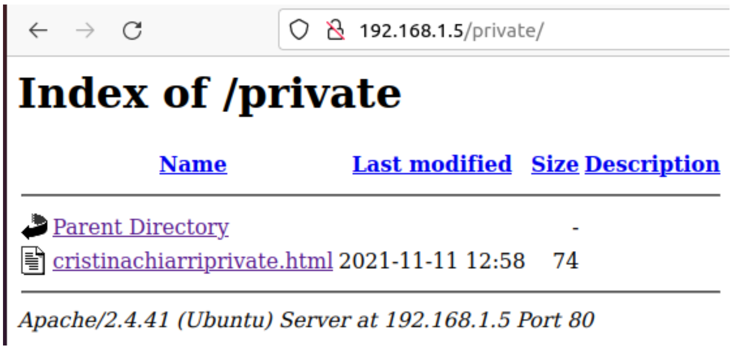
We can acceess using user chiarri



Save login for http://192.168.1.5?

Username
chiarri

Password
••••••••



Index of /private

```
Name                         Last modified     Size Description
Parent Directory                                 -
cristinachiarriprivate.html  2021-11-11 12:58   74
```

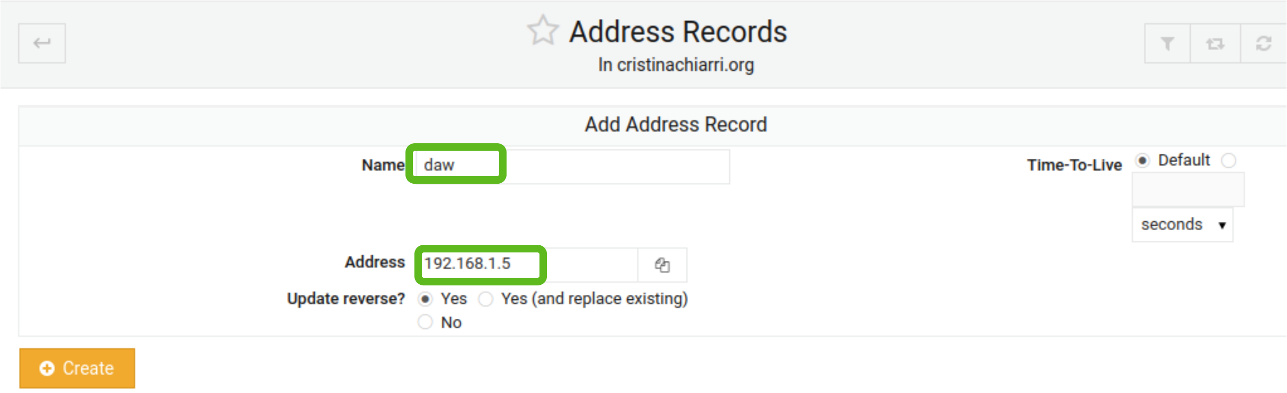
Apache/2.4.41 (Ubuntu) Server at 192.168.1.5 Port 80

5 VIRTUAL HOST daw.cristinachiarri.org

We have to add a second virtual host called daw.cristinachiarri.org as.

5.1 Add the address record of the new virtual host in our DNS server

We are going to use the same IP address.



Address Records

In cristinachiarri.org

Add Address Record

Name: daw

Time-To-Live: ● Default ○

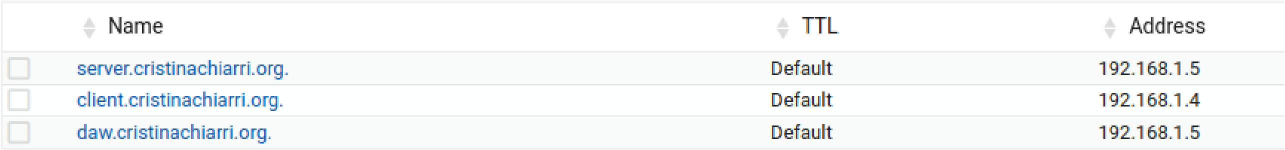
seconds ▾

Address: 192.168.1.5

Update reverse? ● Yes ○ Yes (and replace existing) ○ No

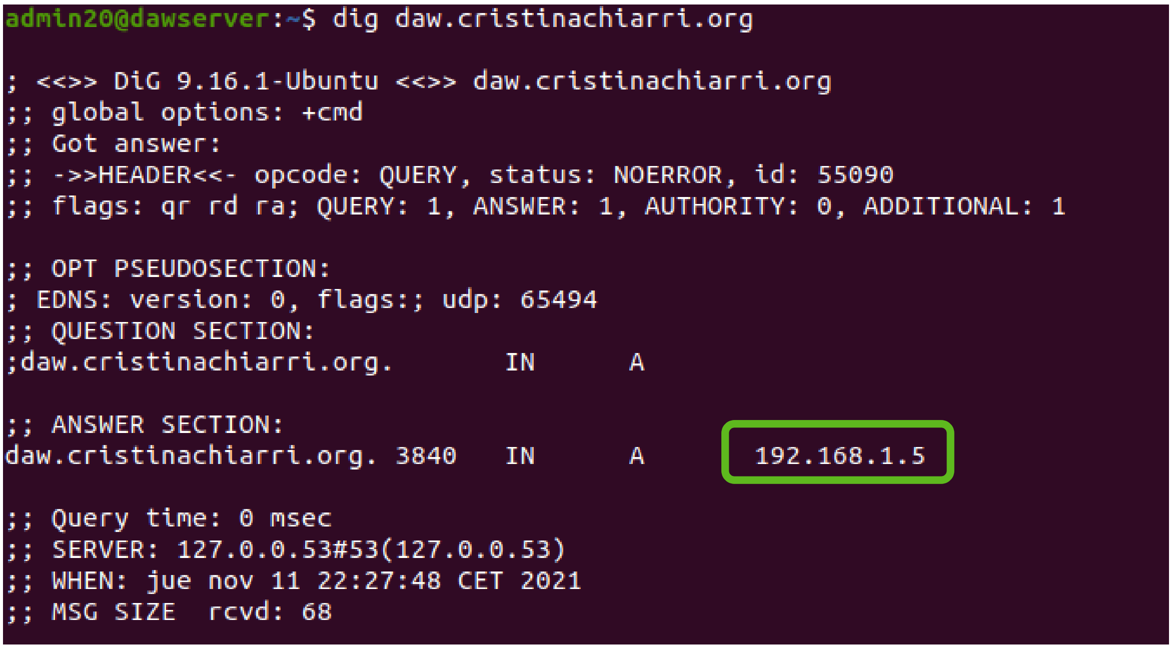
Create

Here we can see all our virtual host



	Name	TTL	Address
□	server.cristinachiarri.org.	Default	192.168.1.5
□	client.cristinachiarri.org.	Default	192.168.1.4
□	daw.cristinachiarri.org.	Default	192.168.1.5

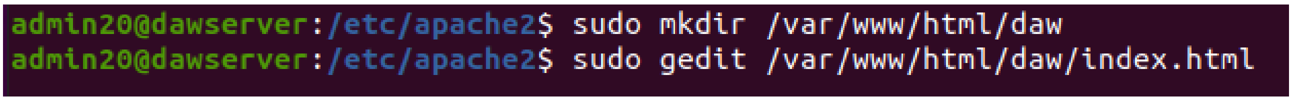
We must apply the new configuration and confirm that it is correct.



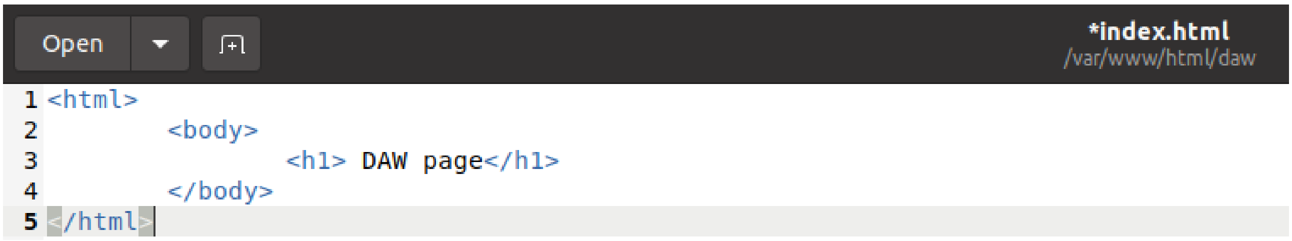
```
admin20@dawserver:~$ dig daw.cristinachiarri.org

; <<>> DiG 9.16.1-Ubuntu <<>> daw.cristinachiarri.org
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 55090
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;daw.cristinachiarri.org.       IN      A

;; ANSWER SECTION:
daw.cristinachiarri.org. 3840   IN      A       192.168.1.5

;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: jue nov 11 22:27:48 CET 2021
;; MSG SIZE  rcvd: 68
```

5.2 Configure the new virtual host in Apache

5.2.1 Create the directories and files



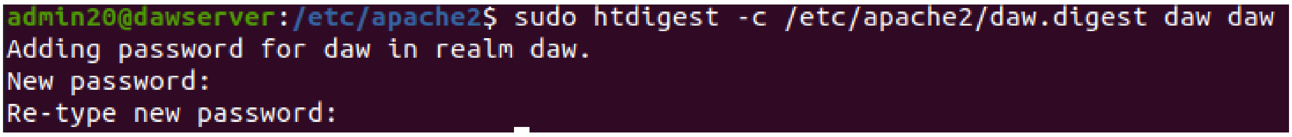
```
admin20@dawserver:/etc/apache2$ sudo mkdir /var/www/html/daw
admin20@dawserver:/etc/apache2$ sudo gedit /var/www/html/daw/index.html
```



```
<html>
        <body>
                <h1> DAW page</h1>
        </body>
</html>
```

This file only can be access by the user daw using HTTP Digest authentication.

5.2.2 Create a digest authentication file for user daw

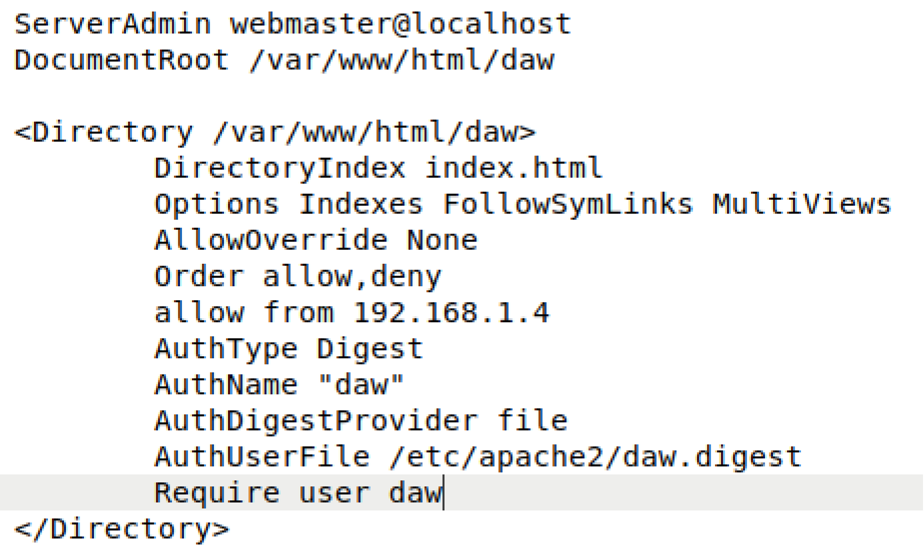


```
admin20@dawserver:/etc/apache2$ sudo htdigest -c /etc/apache2/daw.digest daw daw
Adding password for daw in realm daw.
New password:
Re-type new password:
```

5.2.3 Create a file configuration daw.conf

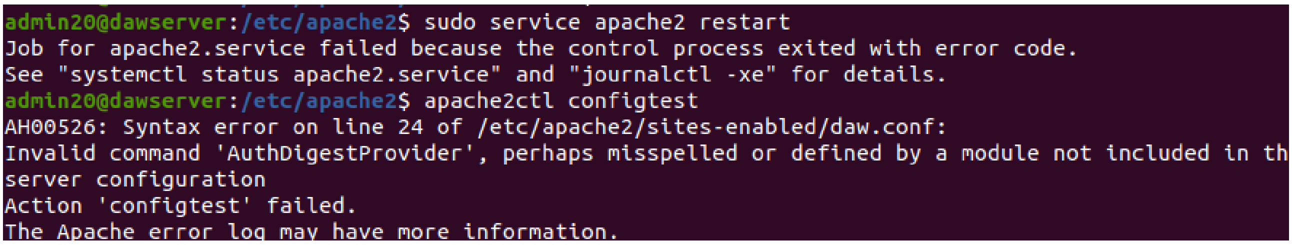
Now we are going to **create the file /etc/apache2/sites-available/daw.conf.**
(We can use a copy of 000-default.conf and modify it)

In this case, we will allow the access to the private zone only for linuxclient (192.168.1.4) and the user **daw**

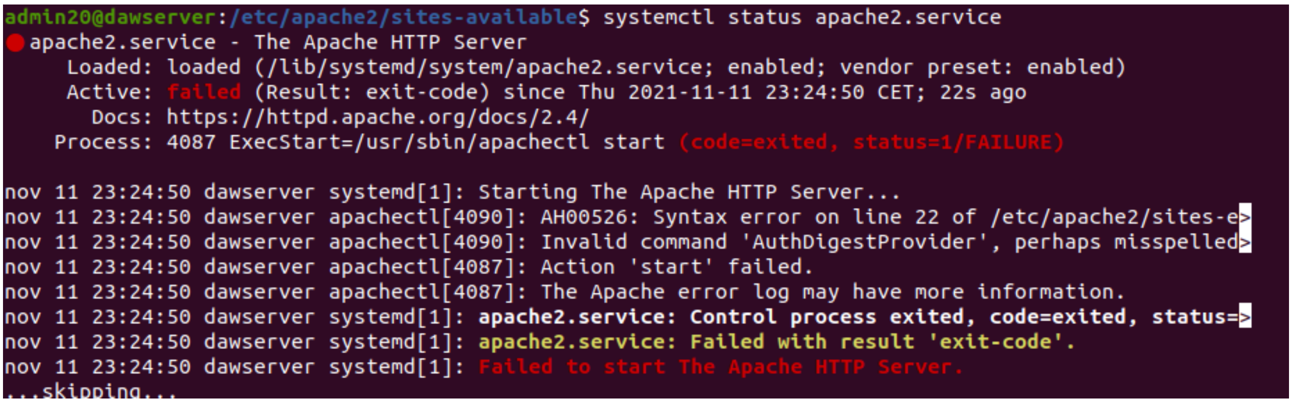


```
ServerAdmin webmaster@localhost
DocumentRoot /var/www/html/daw

<Directory /var/www/html/daw>
        DirectoryIndex index.html
        Options Indexes FollowSymLinks MultiViews
        AllowOverride None
        Order allow,deny
        allow from 192.168.1.4
        AuthType Digest
        AuthName "daw"
        AuthDigestProvider file
        AuthUserFile /etc/apache2/daw.digest
        Require user daw
</Directory>
```

5.2.4 Enable the virtual host and restart the Apache server.



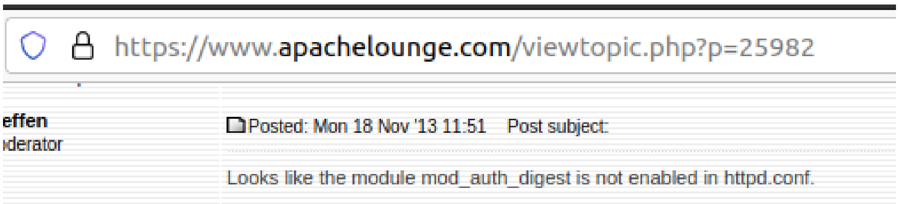
```
admin20@dawserver:/etc/apache2$ sudo service apache2 restart
Job for apache2.service failed because the control process exited with error code.
See "systemctl status apache2.service" and "journalctl -xe" for details.
admin20@dawserver:/etc/apache2$ apache2ctl configtest
AH00526: Syntax error on line 24 of /etc/apache2/sites-enabled/daw.conf:
Invalid command 'AuthDigestProvider', perhaps misspelled or defined by a module not included in th
server configuration
Action 'configtest' failed.
The Apache error log may have more information.
```



```
admin20@dawserver:/etc/apache2/sites-available$ systemctl status apache2.service
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset: enabled)
     Active: failed (Result: exit-code) since Thu 2021-11-11 23:24:50 CET; 22s ago
       Docs: https://httpd.apache.org/docs/2.4/
    Process: 4087 ExecStart=/usr/sbin/apachectl start (code=exited, status=1/FAILURE)

nov 11 23:24:50 dawserver systemd[1]: Starting The Apache HTTP Server...
nov 11 23:24:50 dawserver apachectl[4090]: AH00526: Syntax error on line 22 of /etc/apache2/sites-e>
nov 11 23:24:50 dawserver apachectl[4090]: Invalid command 'AuthDigestProvider', perhaps misspelled>
nov 11 23:24:50 dawserver apachectl[4087]: Action 'start' failed.
nov 11 23:24:50 dawserver apachectl[4087]: The Apache error log may have more information.
nov 11 23:24:50 dawserver systemd[1]: apache2.service: Control process exited, code=exited, status=>
nov 11 23:24:50 dawserver systemd[1]: apache2.service: Failed with result 'exit-code'.
nov 11 23:24:50 dawserver systemd[1]: Failed to start The Apache HTTP Server.
...skipping...
```

The system does not accept the AuthDigestProviider command in the configuration file daw.conf.

Looking for information in internet, I have found this forum.



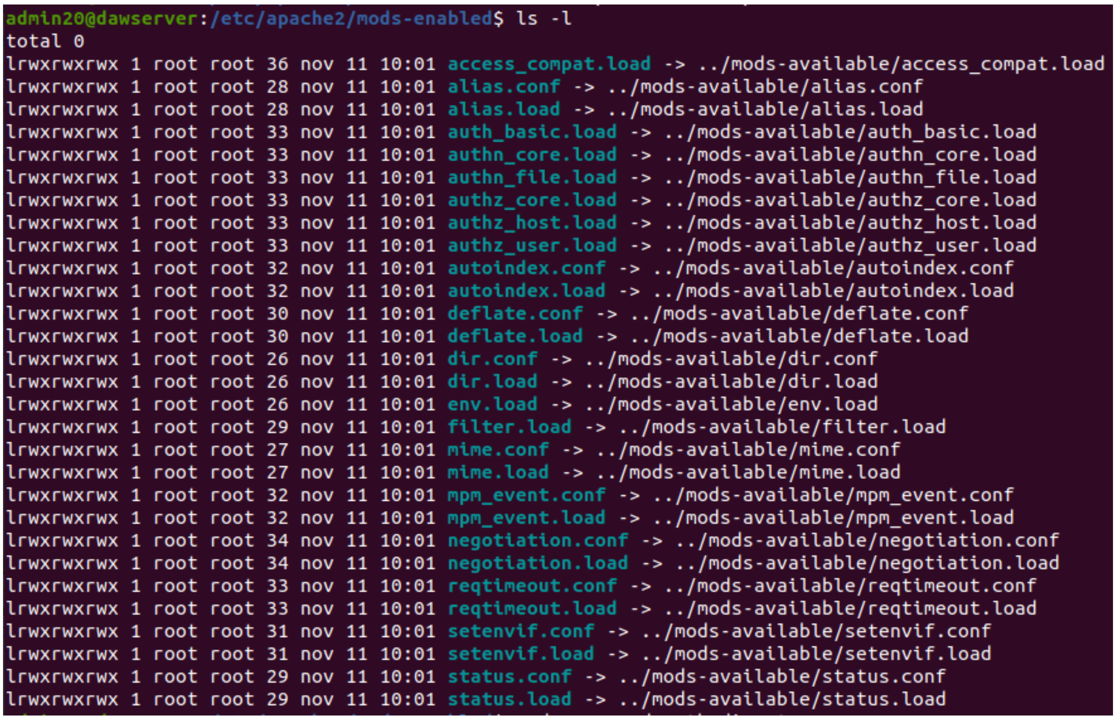
https://www.apachelounge.com/viewtopic.php?p=25982

effen
iderator

Posted: Mon 18 Nov '13 11:51 Post subject:

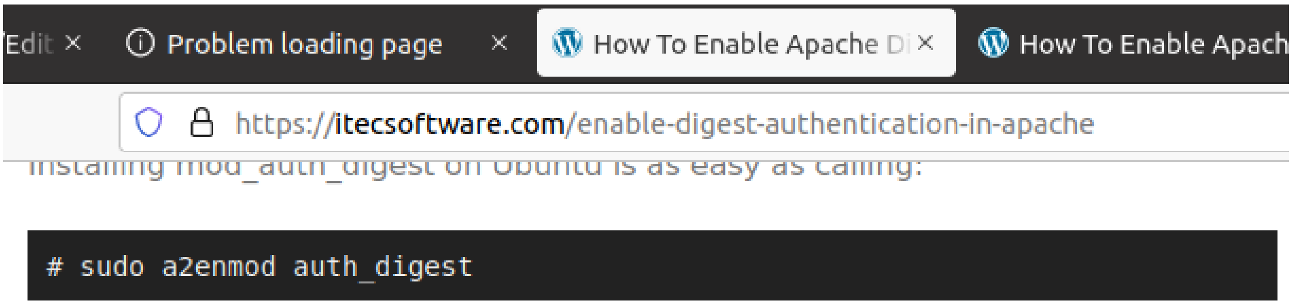
Looks like the module mod_auth_digest is not enabled in httpd.conf.

It seems that the module mod_auth_digest may not be enabled.



```
admin20@dawserver:/etc/apache2/mods-enabled$ ls -l
total 0
lrwxrwxrwx 1 root root 36 nov 11 10:01 access_compat.load -> ../mods-available/access_compat.load
lrwxrwxrwx 1 root root 28 nov 11 10:01 alias.conf -> ../mods-available/alias.conf
lrwxrwxrwx 1 root root 28 nov 11 10:01 alias.load -> ../mods-available/alias.load
lrwxrwxrwx 1 root root 33 nov 11 10:01 auth_basic.load -> ../mods-available/auth_basic.load
lrwxrwxrwx 1 root root 33 nov 11 10:01 authn_core.load -> ../mods-available/authn_core.load
lrwxrwxrwx 1 root root 33 nov 11 10:01 authn_file.load -> ../mods-available/authn_file.load
lrwxrwxrwx 1 root root 33 nov 11 10:01 authz_core.load -> ../mods-available/authz_core.load
lrwxrwxrwx 1 root root 33 nov 11 10:01 authz_host.load -> ../mods-available/authz_host.load
lrwxrwxrwx 1 root root 33 nov 11 10:01 authz_user.load -> ../mods-available/authz_user.load
lrwxrwxrwx 1 root root 32 nov 11 10:01 autoindex.conf -> ../mods-available/autoindex.conf
lrwxrwxrwx 1 root root 32 nov 11 10:01 autoindex.load -> ../mods-available/autoindex.load
lrwxrwxrwx 1 root root 30 nov 11 10:01 deflate.conf -> ../mods-available/deflate.conf
lrwxrwxrwx 1 root root 30 nov 11 10:01 deflate.load -> ../mods-available/deflate.load
lrwxrwxrwx 1 root root 26 nov 11 10:01 dir.conf -> ../mods-available/dir.conf
lrwxrwxrwx 1 root root 26 nov 11 10:01 dir.load -> ../mods-available/dir.load
lrwxrwxrwx 1 root root 26 nov 11 10:01 env.load -> ../mods-available/env.load
lrwxrwxrwx 1 root root 29 nov 11 10:01 filter.load -> ../mods-available/filter.load
lrwxrwxrwx 1 root root 27 nov 11 10:01 mime.conf -> ../mods-available/mime.conf
lrwxrwxrwx 1 root root 27 nov 11 10:01 mime.load -> ../mods-available/mime.load
lrwxrwxrwx 1 root root 32 nov 11 10:01 mpm_event.conf -> ../mods-available/mpm_event.conf
lrwxrwxrwx 1 root root 32 nov 11 10:01 mpm_event.load -> ../mods-available/mpm_event.load
lrwxrwxrwx 1 root root 34 nov 11 10:01 negotiation.conf -> ../mods-available/negotiation.conf
lrwxrwxrwx 1 root root 34 nov 11 10:01 negotiation.load -> ../mods-available/negotiation.load
lrwxrwxrwx 1 root root 33 nov 11 10:01 reqtimeout.conf -> ../mods-available/reqtimeout.conf
lrwxrwxrwx 1 root root 33 nov 11 10:01 reqtimeout.load -> ../mods-available/reqtimeout.load
lrwxrwxrwx 1 root root 31 nov 11 10:01 setenvif.conf -> ../mods-available/setenvif.conf
lrwxrwxrwx 1 root root 31 nov 11 10:01 setenvif.load -> ../mods-available/setenvif.load
lrwxrwxrwx 1 root root 29 nov 11 10:01 status.conf -> ../mods-available/status.conf
lrwxrwxrwx 1 root root 29 nov 11 10:01 status.load -> ../mods-available/status.load
```

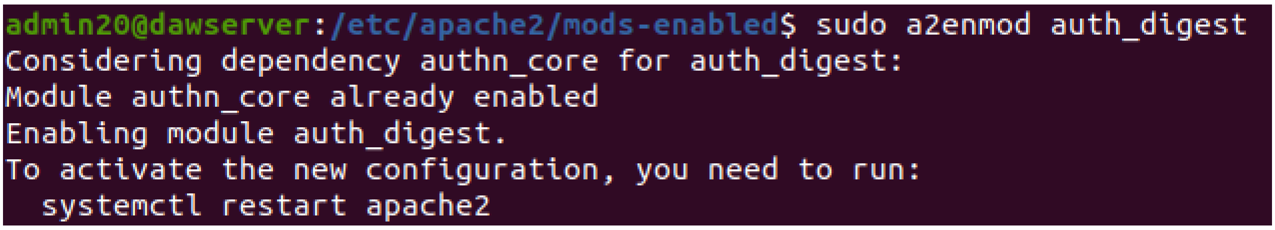
Once confirmed, I enable the module auth _digest.



https://itecsoftware.com/enable-digest-authentication-in-apache

Installing mod_auth_digest on Ubuntu is as easy as calling:

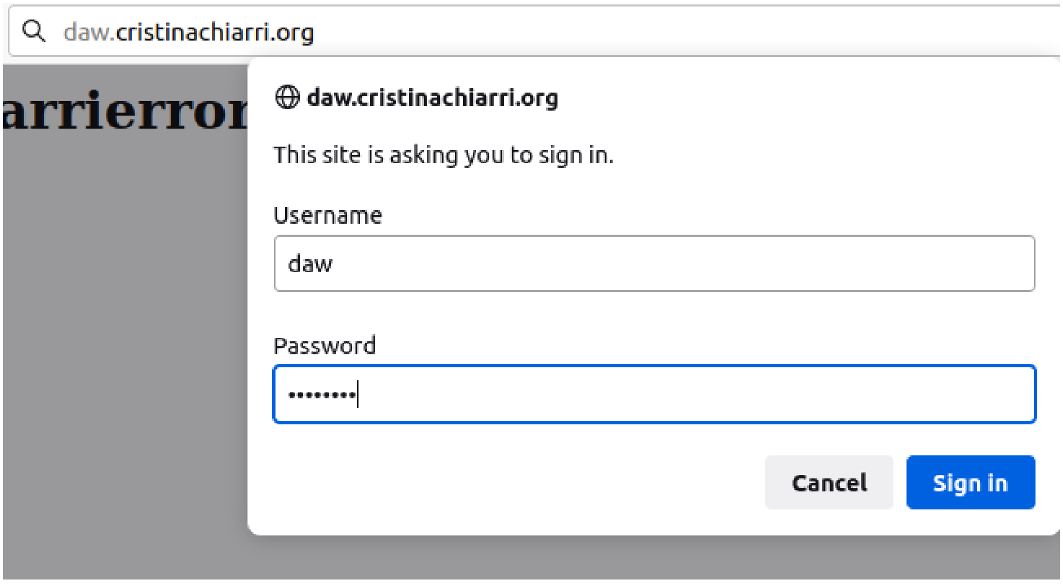
```
# sudo a2enmod auth_digest
```



```
admin20@dawserver:/etc/apache2/mods-enabled$ 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
```

Apache can now be restarted.

If we try to access from the client to the new virtual host daw.cristinachiarri.org, we will need to use the user and password.



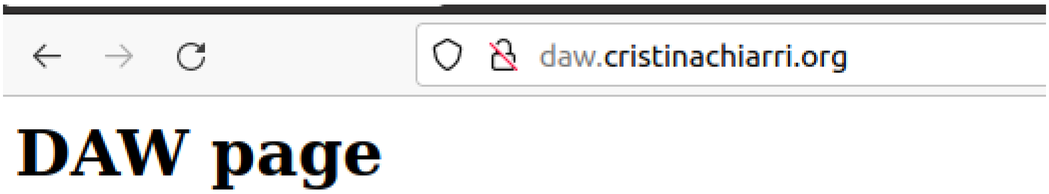
daw.cristinachiarri.org

daw.cristinachiarri.org

This site is asking you to sign in.

Username: daw

Password: ••••••••



daw.cristinachiarri.org

DAW page

6 VIRTUAL HOST ssl.cristinachiarri.org

We are going to configure a new virtual host: ssl.mailname.org.

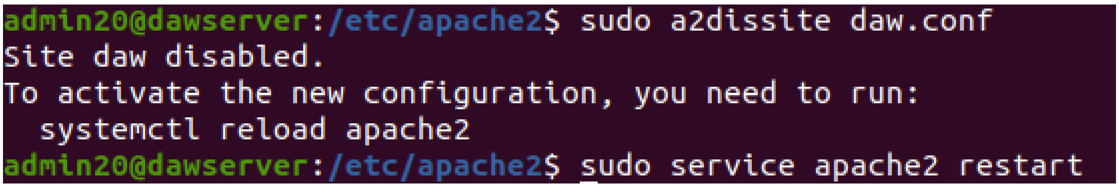
It must be configured to work with HTTPS connections only, with a self-signed certification.
It will only contain a web page called index.html

6.1 Configure the HTTPS protocol in Apache

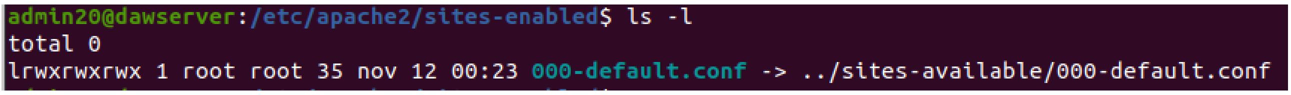
6.1.1 HTTPS default virtual host configuration

- **Disable the virtual host daw.cristinachiarri.org**

We have to **disable the virtual host daw** and the **default virtual host must be enabled**.

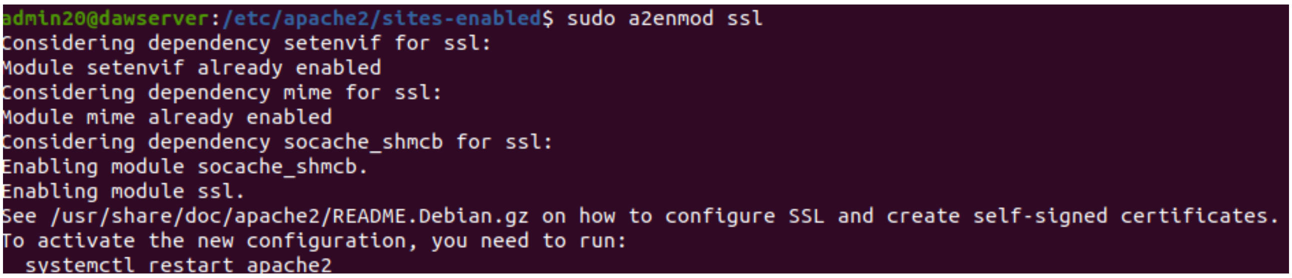


```
admin20@dawserver:/etc/apache2$ sudo a2dissite daw.conf
Site daw disabled.
To activate the new configuration, you need to run:
  systemctl reload apache2
admin20@dawserver:/etc/apache2$ sudo service apache2 restart
```



```
admin20@dawserver:/etc/apache2/sites-enabled$ ls -l
total 0
lrwxrwxrwx 1 root root 35 nov 12 00:23 000-default.conf -> ../sites-available/000-default.conf
```

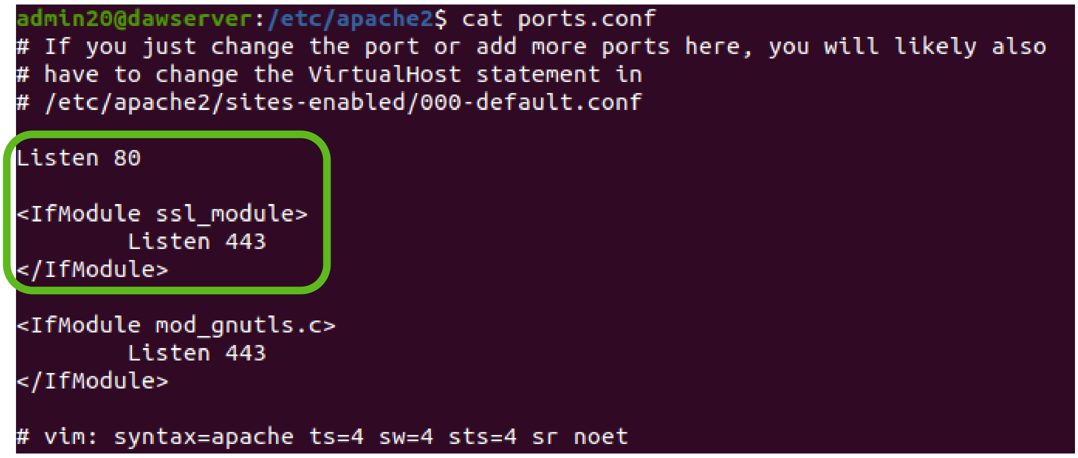
- **Enable the module mod_ssl and restart the server**



```
admin20@dawserver:/etc/apache2/sites-enabled$ sudo 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
```

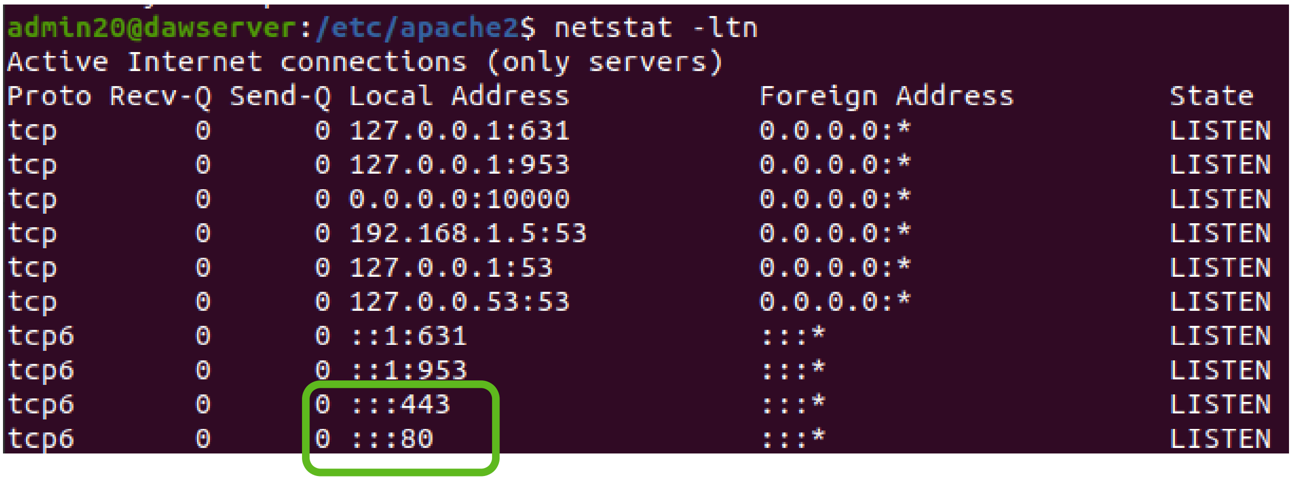
- **Chek configuration file ports.conf**

The server uses the 443 port to listen SSL queries so we are going to check the configurartion file ports.conf to confirm it.



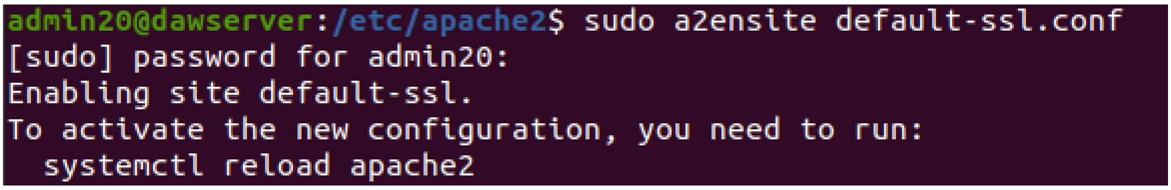
```
admin20@dawserver:/etc/apache2$ cat ports.conf
# If you just change the port or add more ports here, you will likely also
# have to change the VirtualHost statement in
# /etc/apache2/sites-enabled/000-default.conf

Listen 80

<IfModule ssl_module>
        Listen 443
</IfModule>

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

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

We also confirm that the server is listen in ports 80 and 443



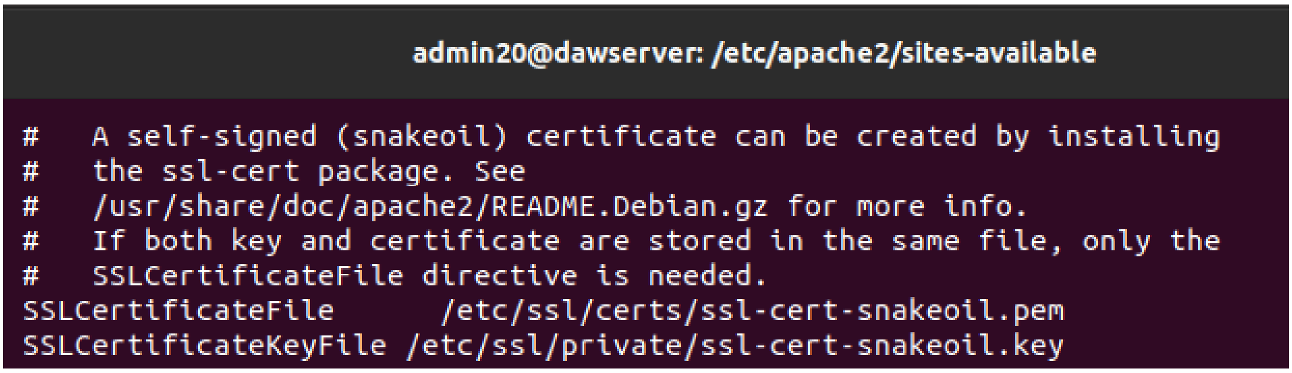
```
admin20@dawserver:/etc/apache2$ netstat -ltn
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:953           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:10000           0.0.0.0:*               LISTEN
tcp        0      0 192.168.1.5:53          0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:53            0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN
tcp6       0      0 ::1:631                 :::*                    LISTEN
tcp6       0      0 ::1:953                 :::*                    LISTEN
tcp6       0      0 :::443                  :::*                    LISTEN
tcp6       0      0 :::80                   :::*                    LISTEN
```

- **Enable the SSL virtual host by default an restart the server**



```
admin20@dawserver:/etc/apache2$ sudo a2ensite default-ssl.conf
[sudo] password for admin20:
Enabling site default-ssl.
To activate the new configuration, you need to run:
  systemctl reload apache2
```

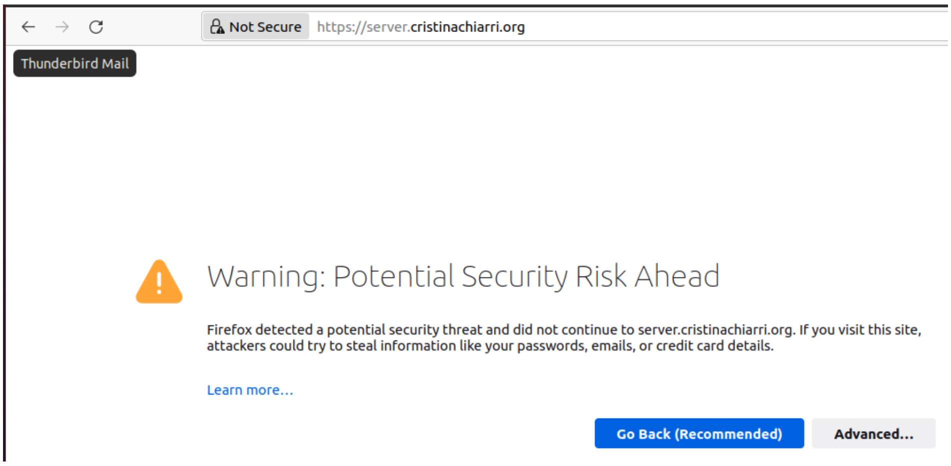
If we check the content of default-ssl.conf we can see that the server uses a default self-signed digital certificate, not signed by a certification authority **so it is not a valid certificate for the browsers**



admin20@dawserver: /etc/apache2/sites-available

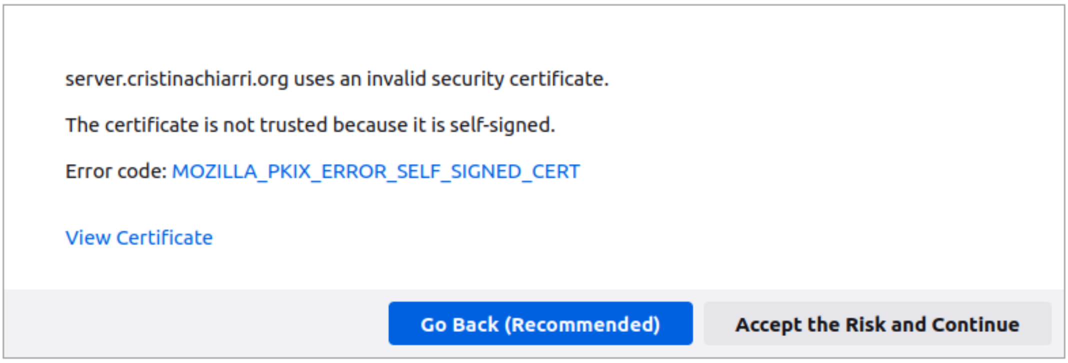
```
#   A self-signed (snakeoil) certificate can be created by installing
#   the ssl-cert package. See
#   /usr/share/doc/apache2/README.Debian.gz for more info.
#   If both key and certificate are stored in the same file, only the
#   SSLCertificateFile directive is needed.
SSLCertificateFile      /etc/ssl/certs/ssl-cert-snakeoil.pem
SSLCertificateKeyFile /etc/ssl/private/ssl-cert-snakeoil.key
```

If we try to connect to **https:**//server.cristinachiarri.org from the client, the browser tells us that the certificate is not valid.



Warning: Potential Security Risk Ahead

Firefox detected a potential security threat and did not continue to server.cristinachiarri.org. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.

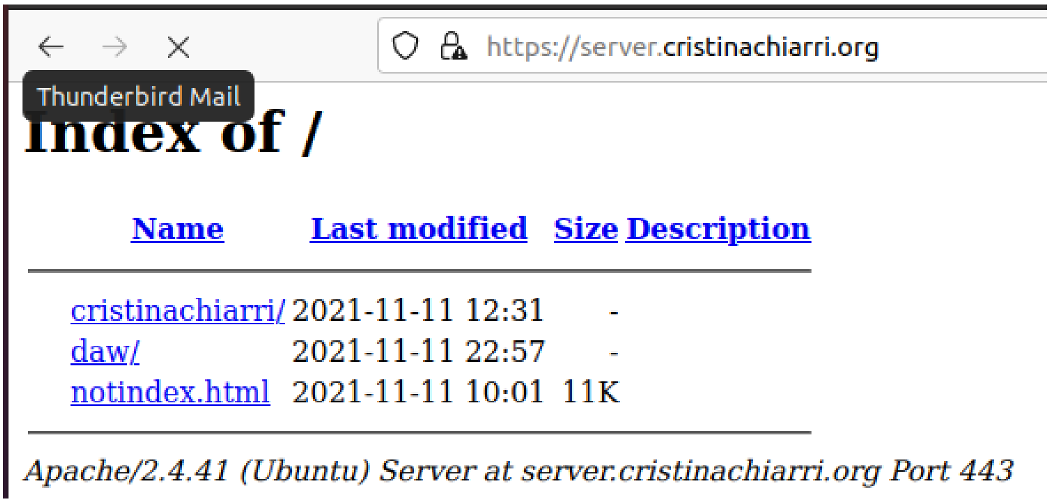


server.cristinachiarri.org uses an invalid security certificate.

The certificate is not trusted because it is self-signed.

Error code: MOZILLA_PKIX_ERROR_SELF_SIGNED_CERT

If we accept, we will see the default SSL page content (there is no index.html)



Index of /

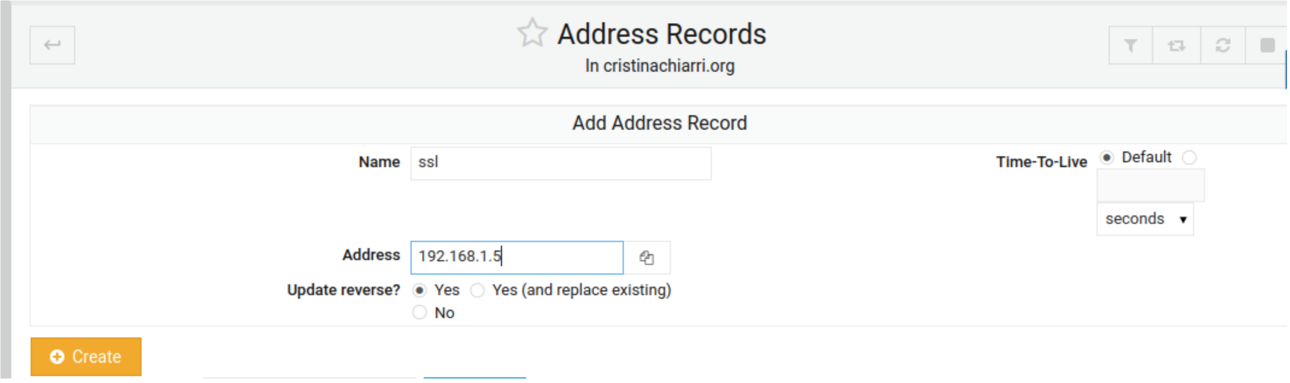
Name	Last modified	Size	Description
cristinachiarri/	2021-11-11 12:31	-	
daw/	2021-11-11 22:57	-	
notindex.html	2021-11-11 10:01	11K	

Apache/2.4.41 (Ubuntu) Server at server.cristinachiarri.org Port 443

6.2 Create a new HTTPS virtual host

We are going to create a third virtual host called ssl.cristinachiarri.org

Add the address record in our DNS server



Address Records

In cristinachiarri.org

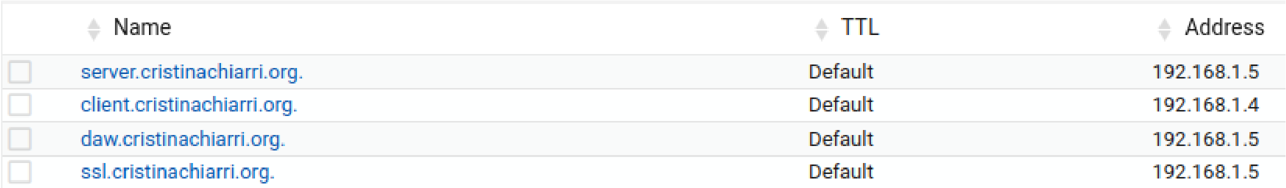
Add Address Record

Name: ssl

Time-To-Live: ● Default ○ seconds ▾

Address: 192.168.1.5

Update reverse? ● Yes ○ Yes (and replace existing) ○ No

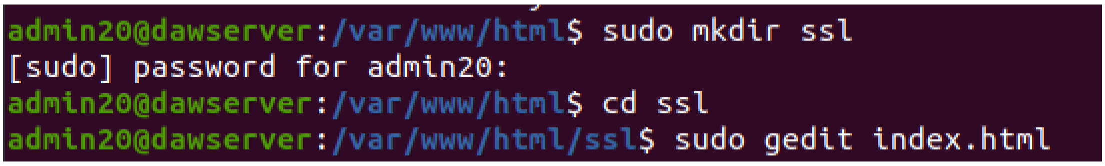


	Name	TTL	Address
□	server.cristinachiarri.org.	Default	192.168.1.5
□	client.cristinachiarri.org.	Default	192.168.1.4
□	daw.cristinachiarri.org.	Default	192.168.1.5
□	ssl.cristinachiarri.org.	Default	192.168.1.5

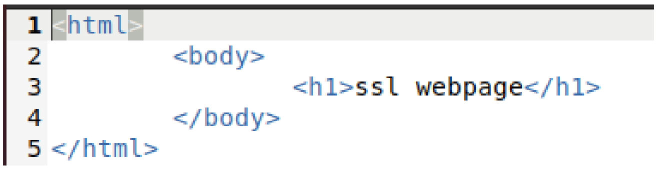
Apply configuration

6.3 Configure the new virtual host in Apache

6.3.1 Create the directories and files



```
admin20@dawserver:/var/www/html$ sudo mkdir ssl
[sudo] password for admin20:
admin20@dawserver:/var/www/html$ cd ssl
admin20@dawserver:/var/www/html/ssl$ sudo gedit index.html
```

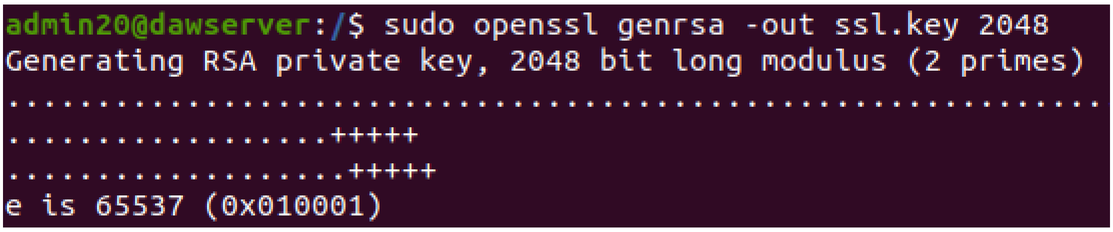


```
<html>
		<body>
			<h1>ssl webpage</h1>
		</body>
</html>
```

6.3.2 Create the self-signed certificate

We have to create a self-signed certificate using OpenSSL wich is a command line tool used to generate private keys, create CSRs, install your SSL/TLS certificate, and identify certificate information.

6.3.2.1 Create a RSA private key in home directory

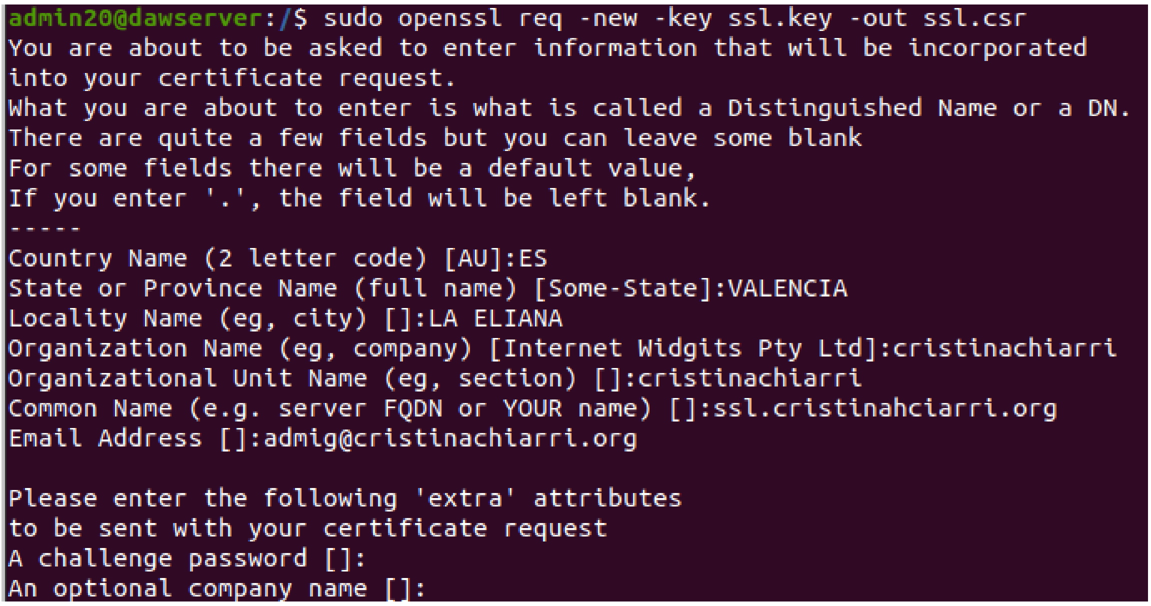


```
admin20@dawserver:/$ sudo openssl genrsa -out ssl.key 2048
Generating RSA private key, 2048 bit long modulus (2 primes)
.............................................................
..................+++++
...................+++++
e is 65537 (0x010001)
```

A 2048 bits key has been generated.

6.3.2.2 Generate the Certificate Signing Request (CSR)

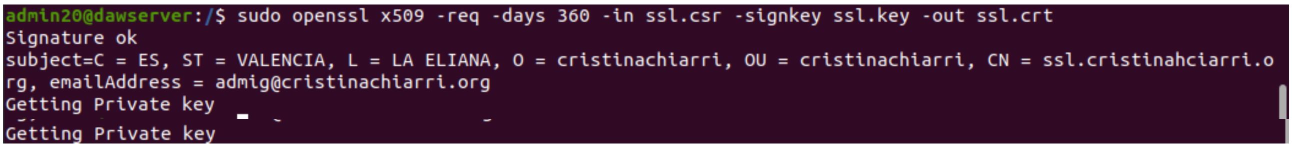
It is one of the first steps towards getting your own SSL/TLS certificate.
Generated on the same server you plan to install the certificate on, the CSR contains information the Certificate Authority will use to create your certificate.



```
admin20@dawserver:/$ sudo openssl req -new -key ssl.key -out ssl.csr
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]:VALENCIA
Locality Name (eg, city) []:LA ELIANA
Organization Name (eg, company) [Internet Widgits Pty Ltd]:cristinachiarri
Organizational Unit Name (eg, section) []:cristinachiarri
Common Name (e.g. server FQDN or YOUR name) []:ssl.cristinahciarri.org
Email Address []:admig@cristinachiarri.org

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

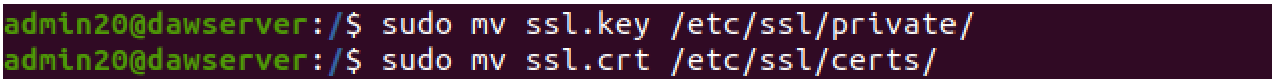
6.3.2.3 create the self-signed certificate

We are going to create the self-signed certificate using our private key and our CSR
sudo openssl x509 -req -days 360 -in **ssl**.csr -signkey **ssl**.key -out **ssl**.crt



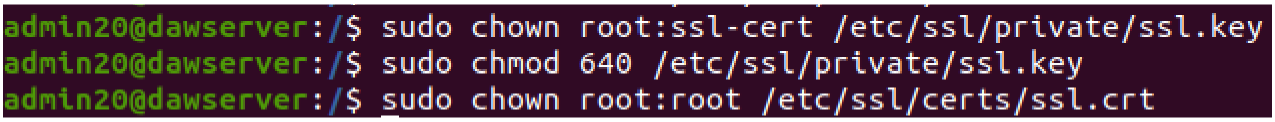
```
admin20@dawserver:/$ sudo openssl x509 -req -days 360 -in ssl.csr -signkey ssl.key -out ssl.crt
Signature ok
subject=C = ES, ST = VALENCIA, L = LA ELIANA, O = cristinachiarri, OU = cristinachiarri, CN = ssl.cristinahciarri.o
rg, emailAddress = admig@cristinachiarri.org
Getting Private key
Getting Private key
```

6.3.2.4 Copy the key and the certificate into the Apache directories



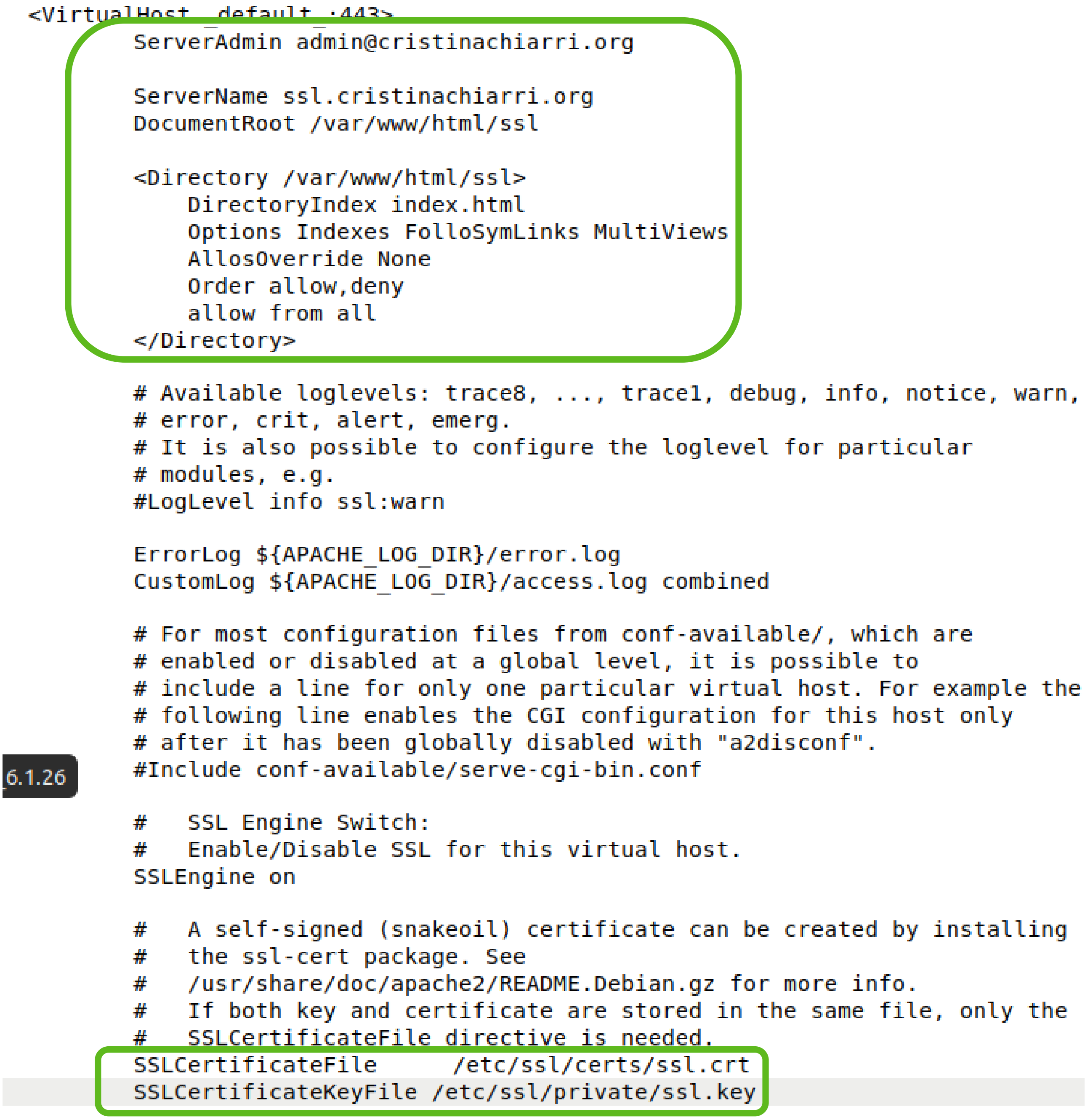
```
admin20@dawserver:/$ sudo mv ssl.key /etc/ssl/private/
admin20@dawserver:/$ sudo mv ssl.crt /etc/ssl/certs/
```

6.3.2.5 Configure the permissions



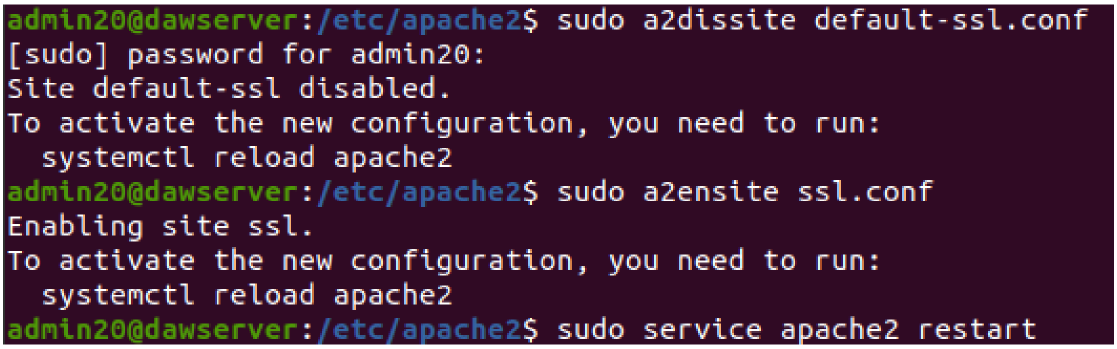
```
admin20@dawserver:/$ sudo chown root:ssl-cert /etc/ssl/private/ssl.key
admin20@dawserver:/$ sudo chmod 640 /etc/ssl/private/ssl.key
admin20@dawserver:/$ sudo chown root:root /etc/ssl/certs/ssl.crt
```

6.4 Create a file configuration ssl.conf



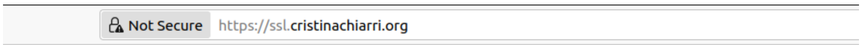
```
<VirtualHost _default_:443>
        ServerAdmin admin@cristinachiarri.org

        ServerName ssl.cristinachiarri.org
        DocumentRoot /var/www/html/ssl

        <Directory /var/www/html/ssl>
            DirectoryIndex index.html
            Options Indexes FolloSymLinks MultiViews
            AllosOverride None
            Order allow,deny
            allow from all
        </Directory>

        # 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

        #   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/ssl/certs/ssl.crt
        SSLCertificateKeyFile /etc/ssl/private/ssl.key
```

6.5 disable the default SSL server, enable ssl virtual host and restart the server

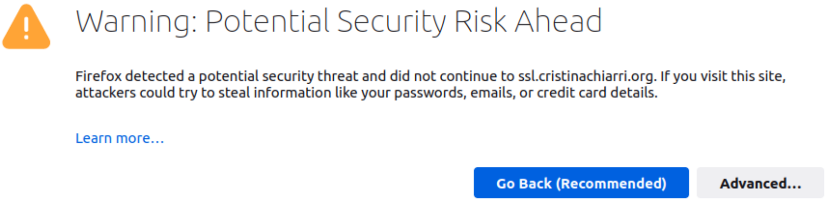


```
admin20@dawserver:/etc/apache2$ sudo a2dissite default-ssl.conf
[sudo] password for admin20:
Site default-ssl disabled.
To activate the new configuration, you need to run:
  systemctl reload apache2
admin20@dawserver:/etc/apache2$ sudo a2ensite ssl.conf
Enabling site ssl.
To activate the new configuration, you need to run:
  systemctl reload apache2
admin20@dawserver:/etc/apache2$ sudo service apache2 restart
```

If we try to connect to https://ssl.cristinachiarri.org from the client, the browser alerts that the certificate is invalid because is not signed by a certification authority. (It is a self-signed certificate)



Not Secure https://ssl.cristinachiarri.org

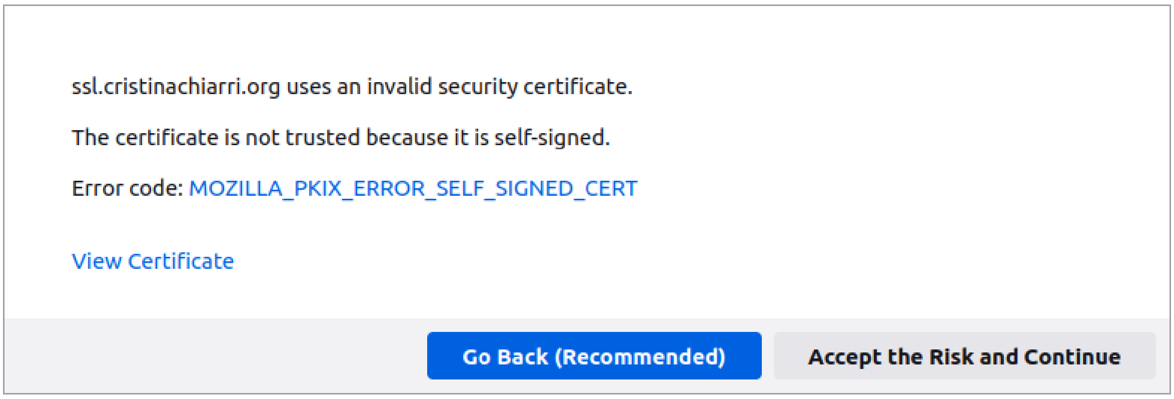


Warning: Potential Security Risk Ahead

Firefox detected a potential security threat and did not continue to ssl.cristinachiarri.org. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.

Learn more…

Go Back (Recommended) Advanced…



ssl.cristinachiarri.org uses an invalid security certificate.

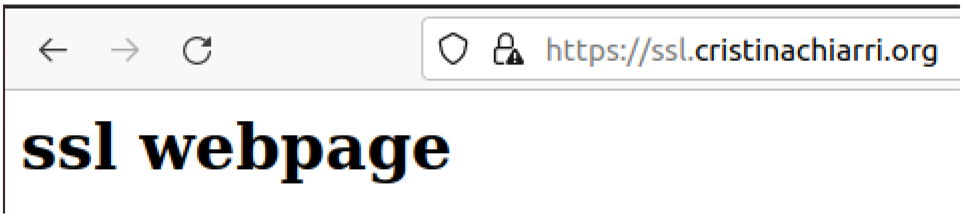
The certificate is not trusted because it is self-signed.

Error code: MOZILLA_PKIX_ERROR_SELF_SIGNED_CERT

View Certificate

Go Back (Recommended) Accept the Risk and Continue

If we accept, we can see the ssl web page.



https://ssl.cristinachiarri.org

ssl webpage