# Comandos Servicios

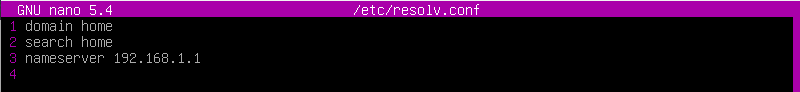
# Servicios que pueden salir:

SSH VSFTPD telnetd apache2

# Clientes que pueden salir:

SSH FILEZILLA PUTTY WINSCP Internet explorer LYNX

Archivo de configuración de resolv.conf, hace de DNS chustilla para facilitar tus comandos, funciona a nivel de solo el equipo



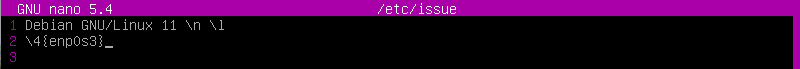
Archivo host.conf también resuelve direcciones Ip a nombres pero lo hace a nivel de red, ya es parte de un servicio DNS



Para cambiar el nombre del servidor simplemente hostnamectl



Para poner en la IP o un mensaje antes de inicar sesión editas /etc/issue

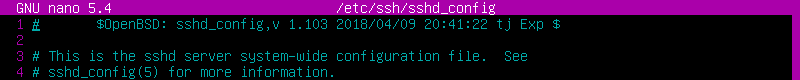




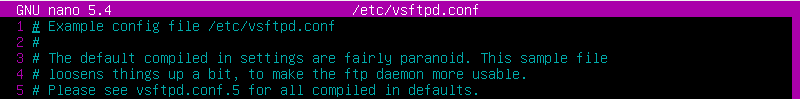
Para modificar el mensaje de bienvenida tras iniciar sesión modificamos el /etc/motd



Para configurar el servicio SSH nano /etc/ssh/sshd\_config

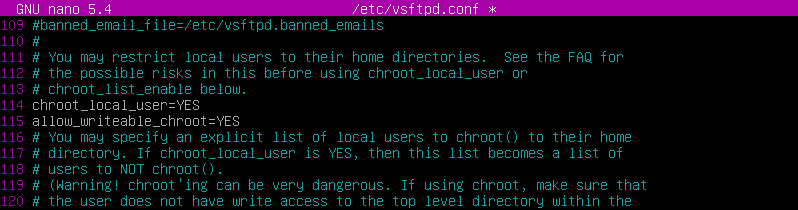


Para configurar el servicio vsftpd nano /etc/vsftpd.conf

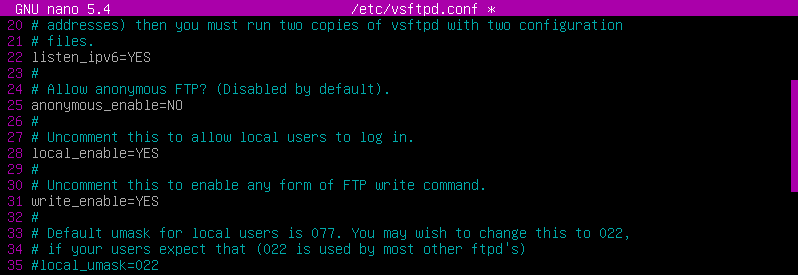


# Configuración VSFTPD

Para enjaular a los usuarios en vsftd.conf ponemos la línea 114 y 115

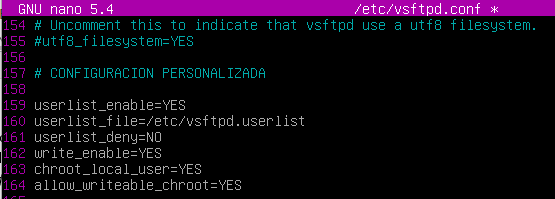


Para permitir que los usuarios puedan subir archivos hay que descomentar la línea 31



Si queremos que los usuarios locales no se puedan iniciar sesión y permitir entradas anonimas

local\_enable=NO

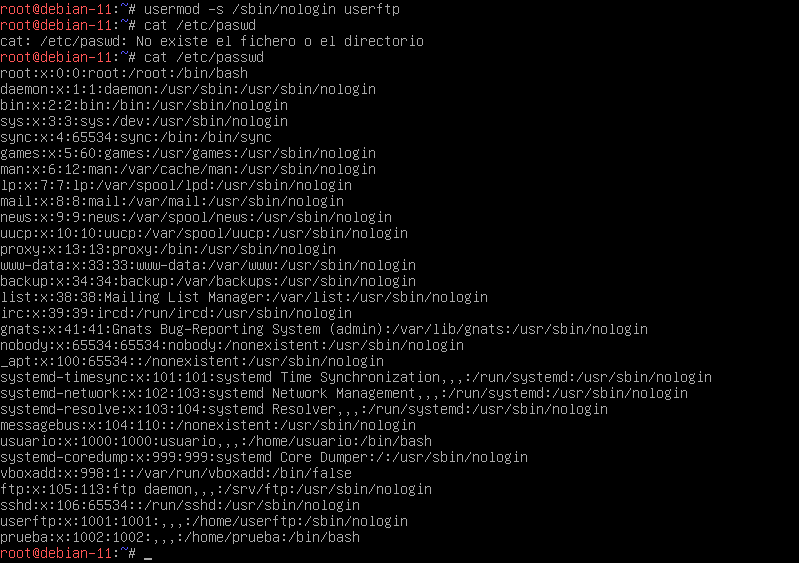
Anonymous\_enable=YES

Dirección y puerto de escucha

listen\_address=mi\_direccion\_ip

listen\_port=21

Si queremos hacer que una cuenta no pueda acceder al Shell pero siga siendo un usuario



# Configuración SSH

Permitir a un usuario usar SSH en el archivo de configuración

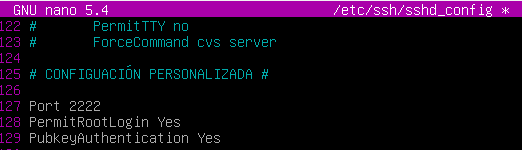
Allowusers “usuario”

port 4321 = cambia el puerto por defecto que usa ssh al puesto

LoginGraceTime 30 = tiempo que tienes para iniciar sesión (en minutos es 1m)

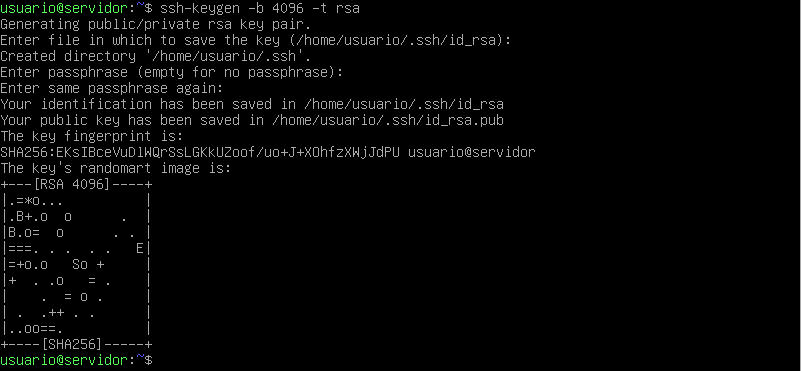
PermitRootLogin no = no permite iniciar sesión con root

MaxAuthTries 2 = máximo numero de intentos para logearte

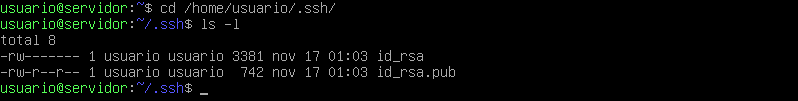


# Claves Asimétricas

Generar unas claves con 4096 bits y en formato rsa (HACER EN EL USUARIO, NO EN ROOT)



Cuando pide los nombres no escribimos nada, le damos a enter directamente y nos creará el directorio .ssh y se pondrá el nombre por defecto id\_rsa



Ahora creamos un archivo llamado authorized\_keys dentro del .ssh



Ahora copiaremos la clave publica que generamos en el cliente al servidor

scp id\_rsa.pub usuario@”IPservidor”:~/



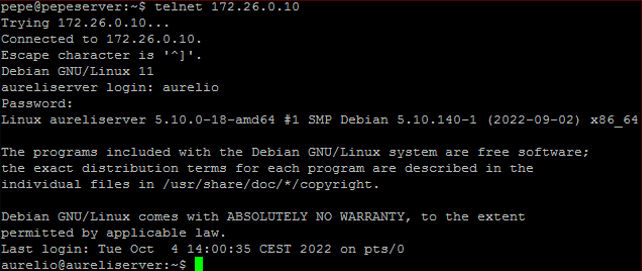
Por ultimo copiamos la clave publica al authorized\_keys que creamos antes

cat id\_rsa.pub >> ~/.ssh/authorized\_key

Y ya podríamos acceder sin contraseña al servidor

# Telnet

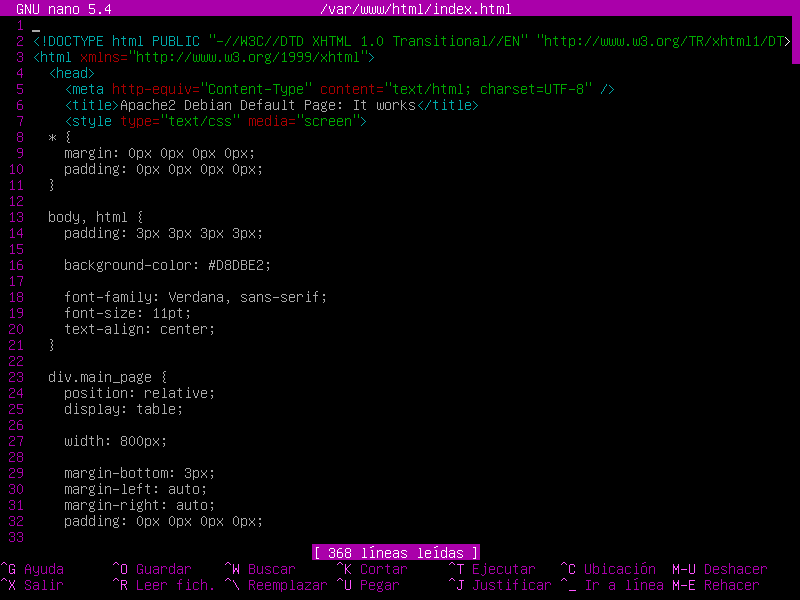
Para usar telnet simplemente hacemos telnet y la ip del equipo, luego se dice el usuario y la contraseña, no hay que configurar nada



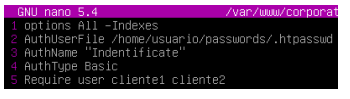
# Apache2

Cuando instalamos apache2 por defecto el archivo index estará en /var/www/html/index.html

Si queremos poner otra página simplemente sustituimos el index o lo modificamos



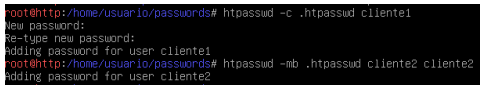
Pagina web por defecto



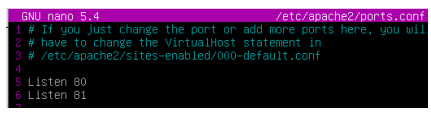
Htaccess

Htpasswd para preguntarte los usuarios a conectarse

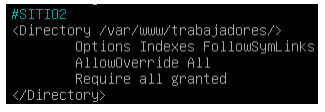
-c (crear) si vamos a crear mas de 1 quitar el -c



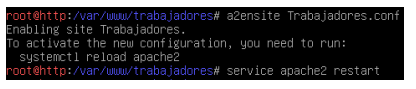
Ingresar contraseña cliente



Puertos de escucha



Archivo /etc/apache/apache2.conf



Levantamos la página web y reiniciamos el servicio

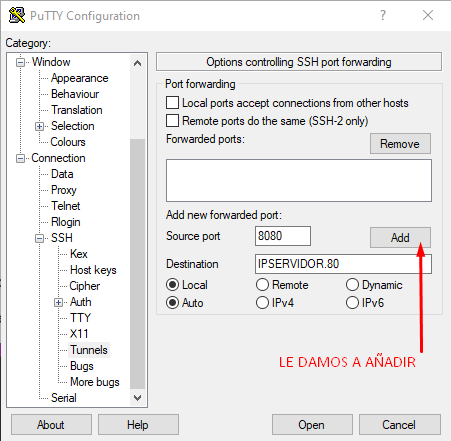
# TUNELES

Ssh –L 8080:IPSERVIDOR/APACHE2:80 usuario@Ipbastion

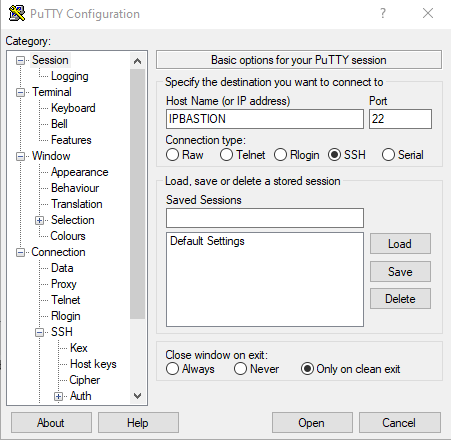
En una nueva ventana o navegador ponemos:

Localhost:8080

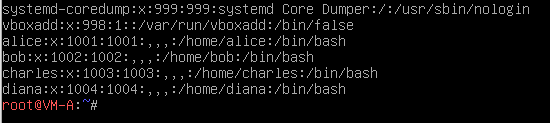
AHORA HAREMOS UN TUNEL POR PUTTY



En IP servidor, ponemos la IP del servidor que tiene el servicio que queremos consumir, después nos vamos a sesión y ponemos la IP del bastión



Para ver los usuarios y contraseñas escribir cat /etc/passwd



Para poner la bidilla que es lo que esta en la ñ

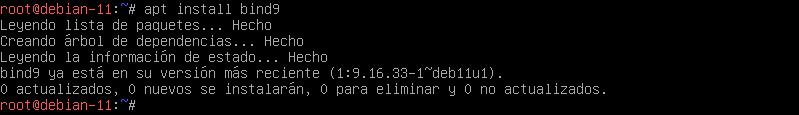
Se hace con alt+4 =~

Para pasar un archivo por scp atraves de un bastion

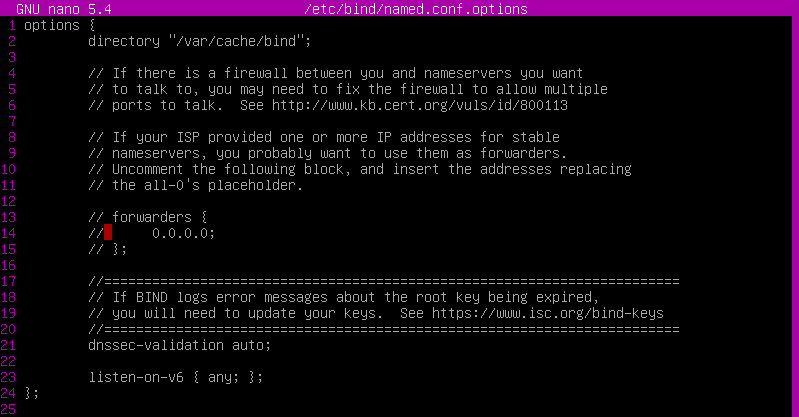
Scp –J usuariobastion@bastion archivo usuarioservidor@servidor: ~/

# DNS Y DHCP

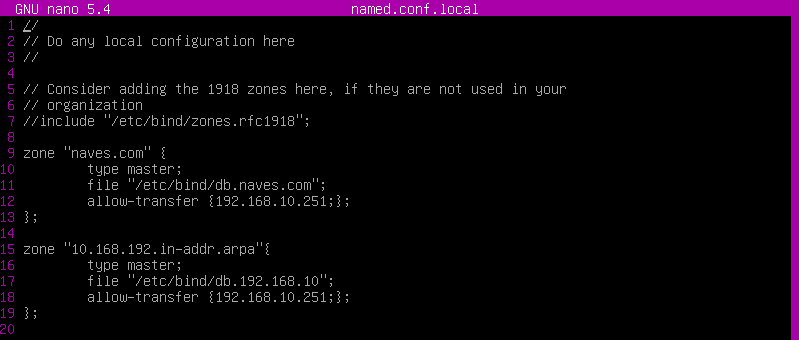
Apt install Bind9



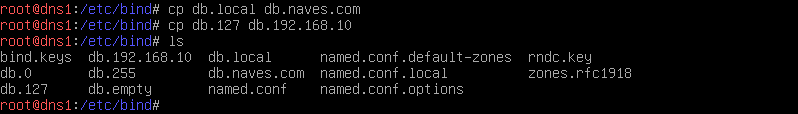
Poner reenviadores



Configuración de zonas, aquí ponemos todas las zonas como master en el primario y slave en los secundarios



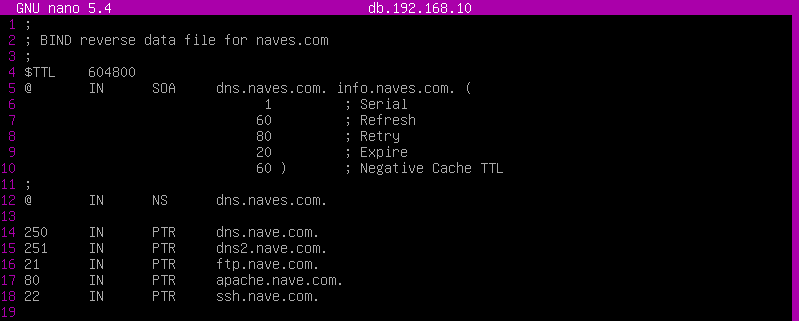
Ahora copiamos el archivo directo (db.local) y el inverso (db.127) y les cambiamos el nombre



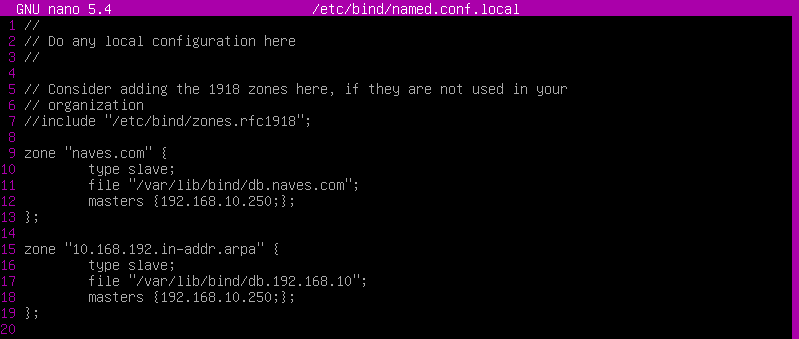
Y lo editamos añadiendo las máquinas de la red (cname sirve para traducir nombres a nombres, mx para correo)



Y también con la inversa



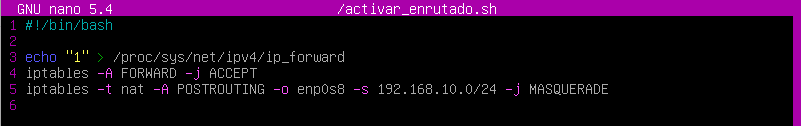
Las configuración de zona inversa (*CUIDADO CON EL FILE /VAR/LIB/BIND,* ***CREAR LA CARPETA BIND ANTES***)



No hace falta configurar nada más en el esclavo ya que cogerá los archivos directos e inversos del DNS principal, se almacenarán los archivos donde le dijimos en el /var/lib/bind

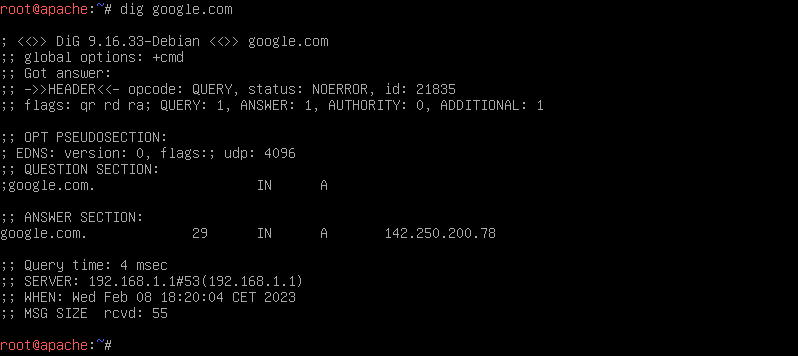


Ponemos el enrutador en el servidor SSH



Le damos permisos de ejecución y lo ejecutamos (tenemos que tener iptables instalado previamente)

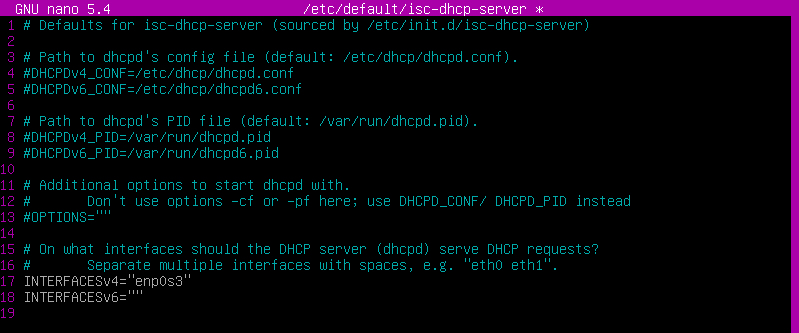


Y comprobamos usando DIG

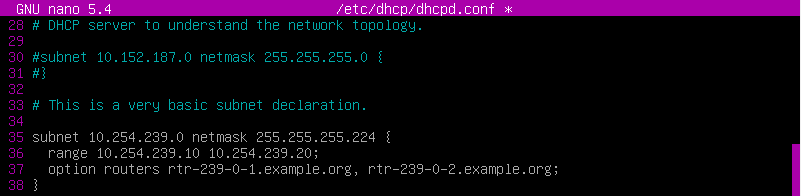
DHCP



Primer archivo de configuración dhcp



Y este es el segundo



Para hacer una reserva

