Estimació de la durada 6 hores + 1 hora d’avaluació.

Important: Fes servir una màquina sense servei DHCP.

Continguts

[Preparació de l’entorn](about:blank) 2

[Instal·lació del servei DNS](about:blank) 2

[Comprovació del servei DNS](about:blank) 3

[Instal·lació i comprovació de l’estat del servei FTP](about:blank) 3

[Modificació de paràmetres del servei FTP](about:blank) 4

[Preparació del servidor FTP privat](about:blank) 6

[Usuaris engabiats](about:blank) 7

[Links addicionals](about:blank) 8

**Preparació de l’entorn**

Server:

Adaptador1(eth0): Xarxa interna amb IP/M privada assignada manualment 172.30.0.1/16.

Adaptador2(eth1): Xarxa NAT a la Màquina Virtual amb IP assignada automàticament amb DHCP.

Nom de la Màquina Virtual: M7UF2*AcrònimNom*SRV (ex. M7UFAGUESRV)

Nom de la màquina al sistema operatiu: *AcrònimNom*SRV (ex. AGUESRV)

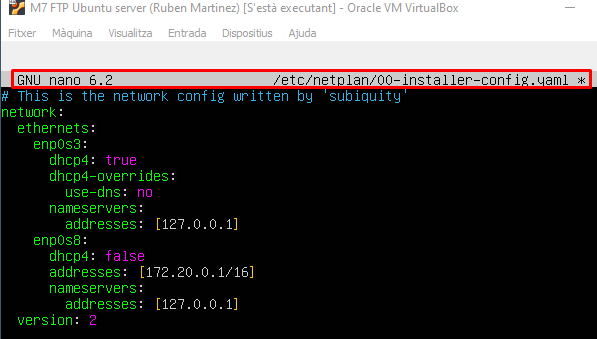
Clients:

Adaptador1(eth0): Xarxa interna amb una IP/M privada assignada manualment de la xarxa 172.30.0.0/16.

Tot fent servir un Ubuntu Server amb el Software VSFTPD instal·lat configurarem un lloc FTP que accepti peticions públiques i privades tot engabiant als usuaris als seus directoris personals.

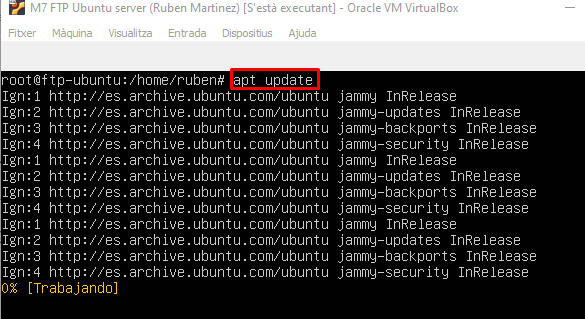
**Instal·lació del servei DNS**

1. Preparació del nostre servidor (2 hores aproximadament)
   1. Configuració de les interfícies. La de xarxa interna ha de tenir IP fixe.

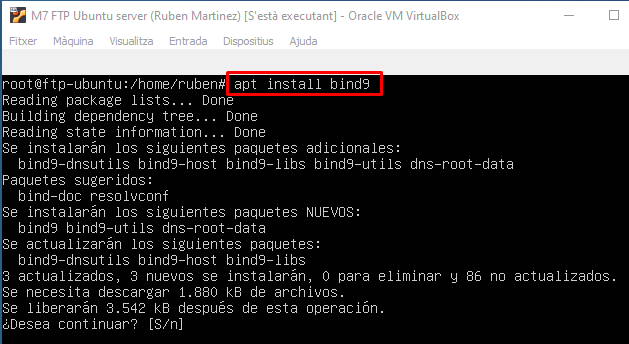




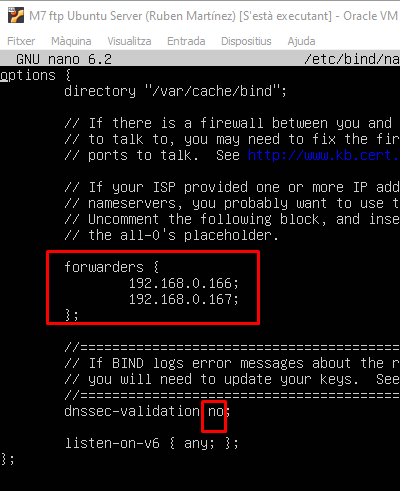
* 1. apt update, de manera que actualitzarem el repositori de sotware.



* 1. apt install bind9, si, caldrà instal·lar i configurar el DNS(Recorda fer còpia de seguretat de qualsevol fitxer que es modifiqui:



* + 1. Configuració prèvia del nostre servidors (BIND) -Recordatori-:
       1. Canvia el directori a “/etc/bind”
       2. Edita el fitxer named.conf.options per permetre al DNS de l’escola ser forwarder.



* + - 1. Edita el fitxer named.conf.local

zone “nomdomini.lan”{

type master;

file “/etc/bind/db.nomdomini”;

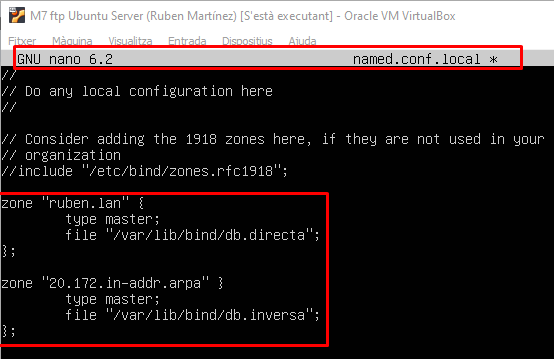
};

zone “30.172.in-addr.arpa”{

type master;

file “/etc/bind/db.172.30”;

};



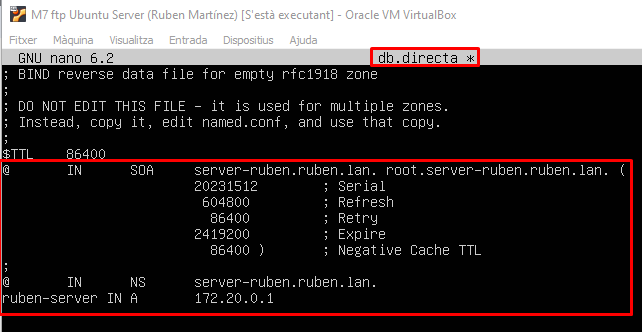
* + - 1. Genera ambdues zones (db.nomdomini,db.IPgirada):
         1. db.nomdomini:

$TTL 86400;

@ IN SOA hostname.nomdomini.lan. root.nomdomini.lan.(aaaammdd#prova 1w 1d 1w 1h);

@ IN NS hostname.nomdomini.lan.

hostname IN A IP



* + - * 1. db.172.30:

$TTL 86400;

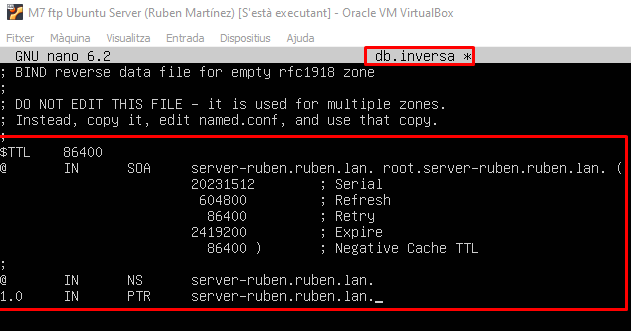
@ IN SOA hostname.nomdomini.lan. root.nomdomini.lan.(

aaaammdd#prova 1w 1d 1w 1h

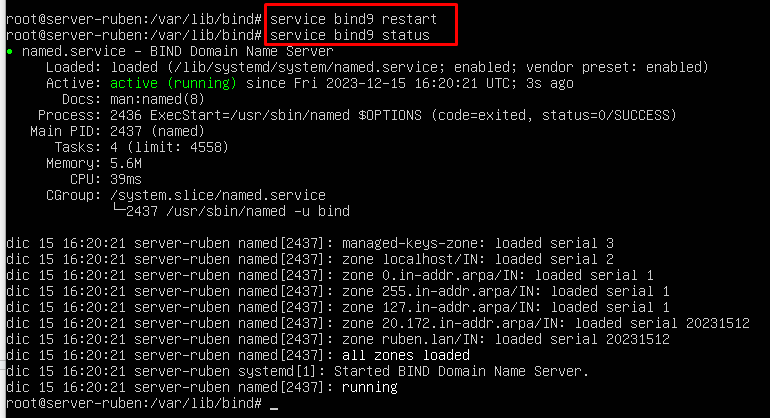
);

@ IN NS hostname.nomdomini.lan.

1.0 IN PTR hostname.nomdomini.lan.



* + 1. Reinicia el servei: “service bind9 restart”



* + 1. Comprova la seva funcionalitat: namedcheckconf, namedcheckzone, nslookup (set q= any -enter- nomdomini.lan -enter-). (recorda que si fas les proves al mateix servidor has de modificar el netplan de manera que el servidor es resolgui a si mateix)
       1. ex.

ensp0s3:

dhcp4: true

dhcp4-overrides:

use-dns: no

nameservers:

addresses: [127.0.0.1]

ensp0s8:

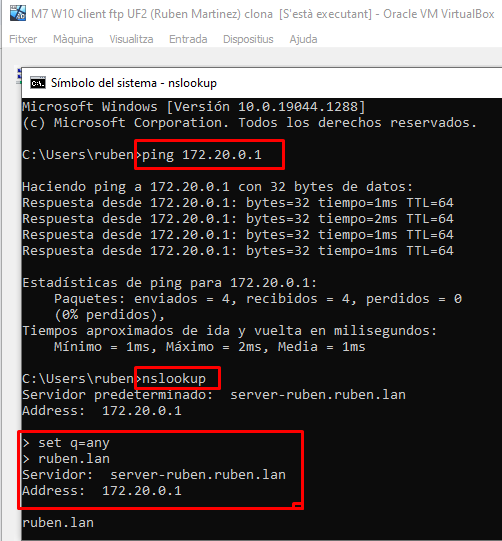
dhcp4: false

nameservers:

addresses: [127.0.0.1]

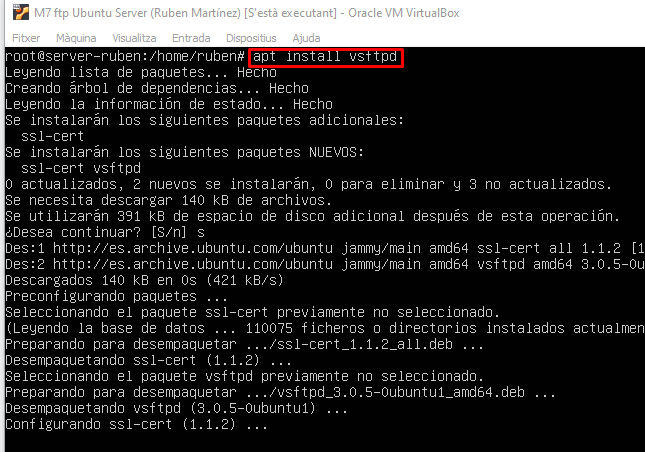
**Comprovació del servei DNS**

1. Un cop comprovat des del client i des del servidor que el nostre DNS és operatiu.

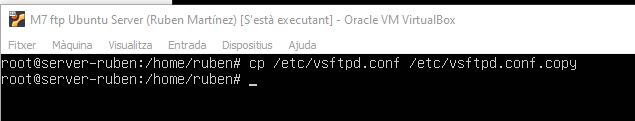


**Instal·lació i comprovació de l’estat del servei FTP**

1. Instal·larem VSFTPD.
   1. Comprovació dels paràmetres per defecte del nostre servidor FTP :



* + 1. Fes una còpia de seguretat del fitxer vsftpd.conf

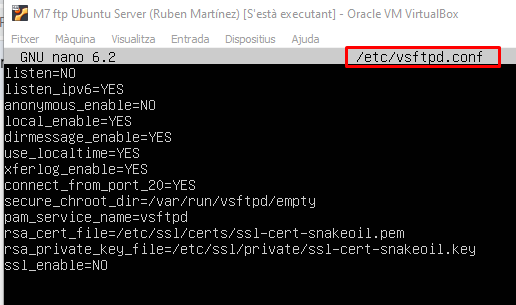


* + 1. Per defecte vsftpd ve amb els següents paràmetres:
       1. Aquest servei no dóna massa pistes i és bo que vagis fent noves còpies a mesura que avancis en l’exercici.
    2. Executa la següent comanda:

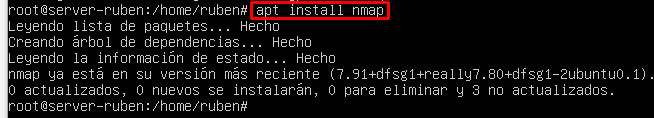
grep -v "#" /etc/vsftpd.conf | sed -e '/^$/d'

Aquesta comanda fa que surti per pantalla exclusivament les línies que es troben actives. El pots fer servir per analitzar el servei si aquest no fa el que tu desitjaves.



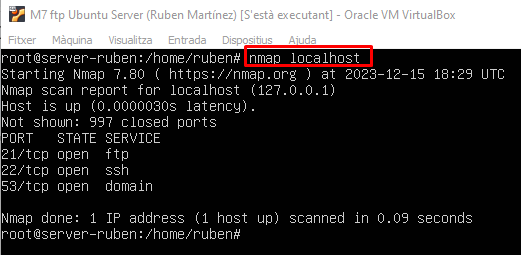


* + - 1. Accés pel port 21?
         1. Instal·la l’aplicació nmap amb apt install nmap



* + - * 1. Escriu la següent comanda al servidor i avalua el resultat:

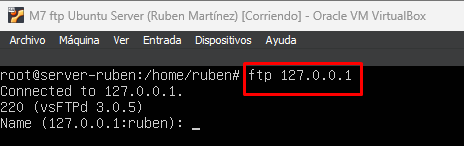
nmap localhost



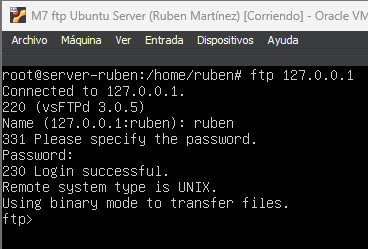
Quins ports apareixen oberts?

A quins serveis pertanyen?

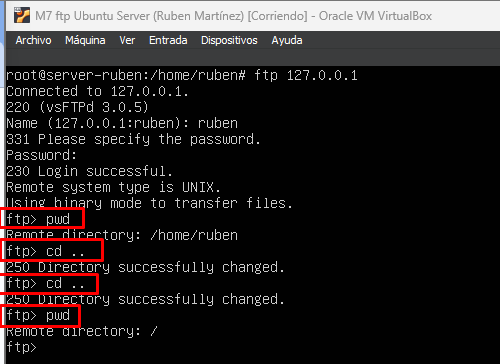
* + - 1. Accés de lectura exclusivament als usuaris locals
         1. ftp 127.0.0.1



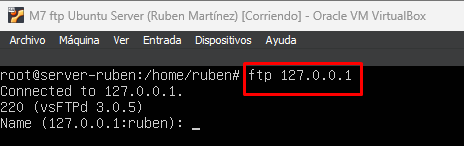
* + - * 1. connexió amb el teu usuari.



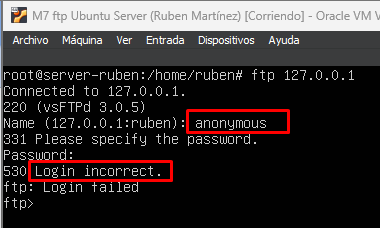
* + - * 1. Comprovació d’engabiament, et pots moure pel sistema de fitxers?



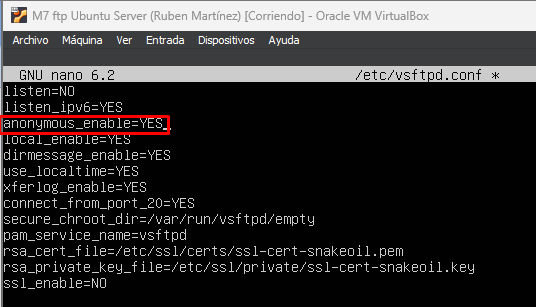
* + - 1. L’usuari anonymous es troba engabiat si s’activa.
         1. ftp 127.0.0.1



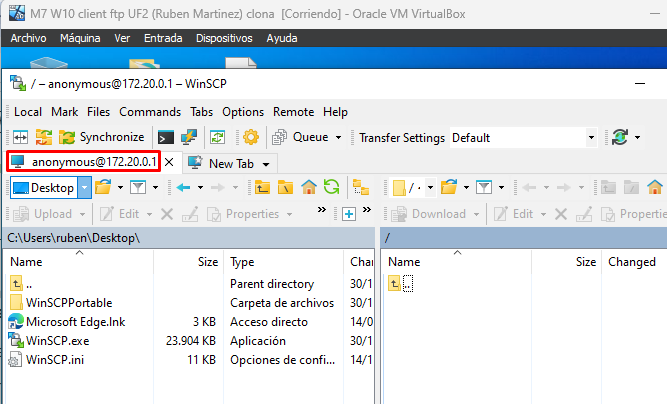
* + - * 1. usuari anonymous/ftp amb qualsevol password



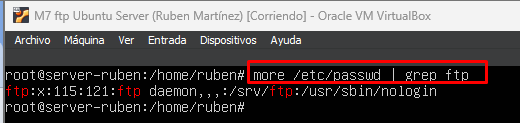
* + - * 1. Comprovació directiva anonymous\_enable.



* + 1. Avalua a quines directives del fitxer de configuració “/etc/vsftpd.conf” (paraula clau més paràmetre) queden reflectits aquests paràmetres.
    2. Entra des d’un ordinador client amb usuari anonymous sense contrasenya i comprova si es pot moure pel sistema de fitxers del servidor.



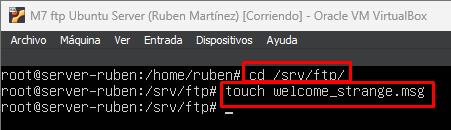
* + 1. Esbrina on es troba el directori arrel del usuari anonymous (o ftp). Quina és la seva ruta absoluta?
       1. Escriu la comanda: more /etc/passwd | grep ftp



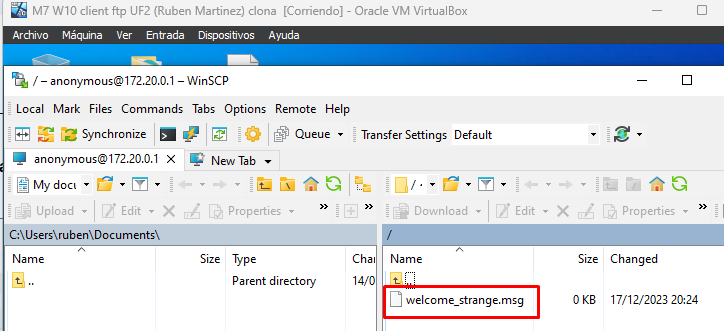
* + - * 1. Què estàs comprovant?
        2. Quin és el home de l’usuari ftp?

**/srv/ftp**

* + - 1. Ves a aquest directori (home usuari ftp) i genera un fitxer anomenat welcome\_stranger.msg.



* + - 1. Torna’t a connectar des del client i comprova que realment podem trobar el fitxer que hem generat.



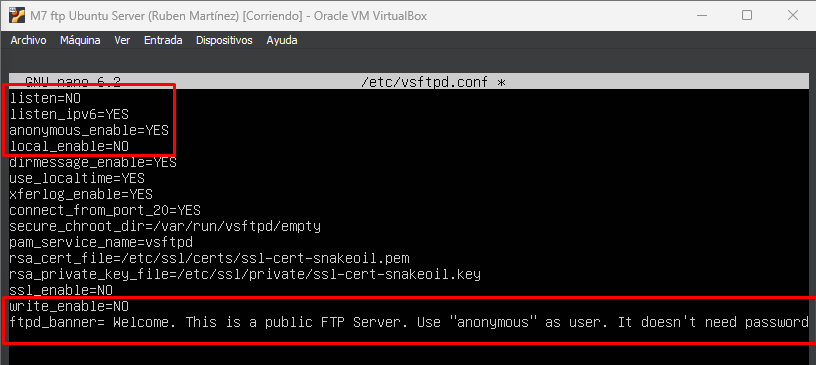
**Modificació de paràmetres del servei FTP**

1. Modificació dels paràmetres per fer que el nostre servidor sigui públic i estigui configurat amb uns paràmetres mínims de seguretat:
   1. Basant-nos en els paràmetres per defecte buscarem i/o afegirem els següents paràmetres. També els comprovarem des del nostre client amb Filezilla.
      1. Paràmetres default:

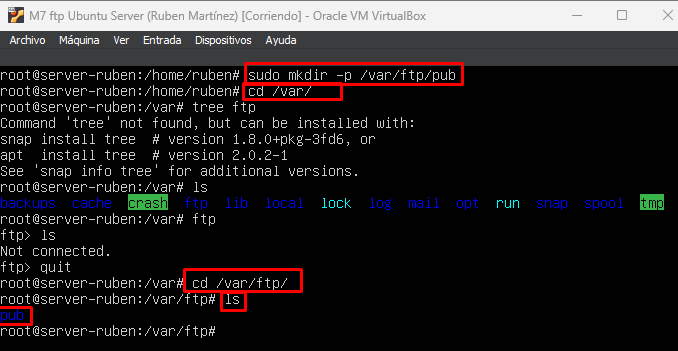
listen=NO

listen\_ipv6=YES  
 local\_enable=NO   
 anonymous\_enable=YES  
 write\_enable=NO

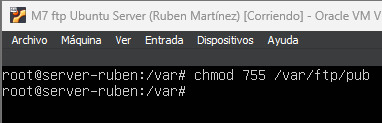
ftpd\_banner= Welcome. This is a public FTP Server. Use “anonymous” as user. It doesn’t need password.



* + 1. Modificació de la ruta arrel de l’usuari anonymous:
       1. Genera un directori anomenat /var/ftp/pub



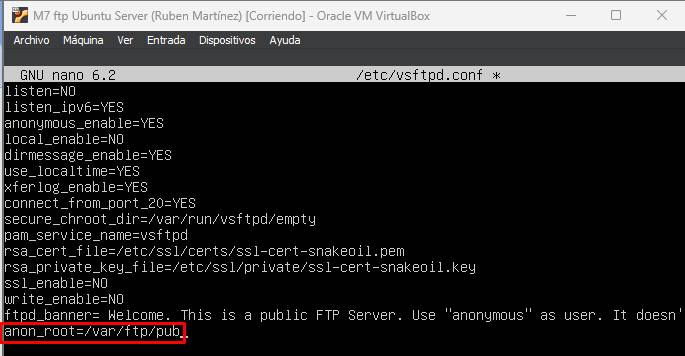
* + - 1. Permisos chmod 755 /var/ftp/pub



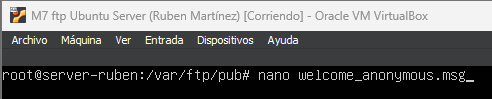
* + - 1. al fitxer de configuració de vsftpd afegeix les següents línies:

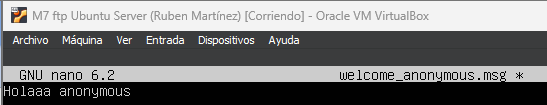
#Changing characteristics for public access

anon\_root=/var/ftp/pub (recorda que l’usuari ftp/anonymous hauria de poder llegir, així que mira els permisos “ls -l” i modifica’ls si fos necessari).

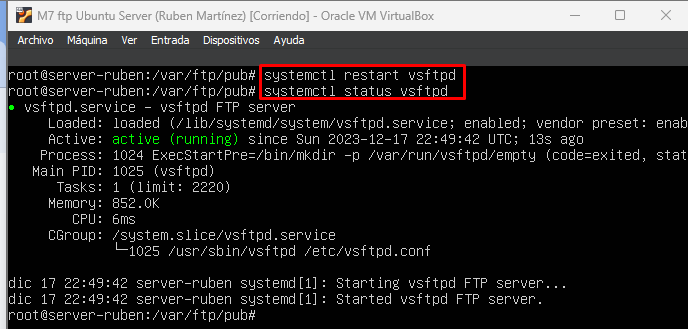


* + - 1. Escriu a dins un fitxer anomenat welcome\_anonymous.msg.

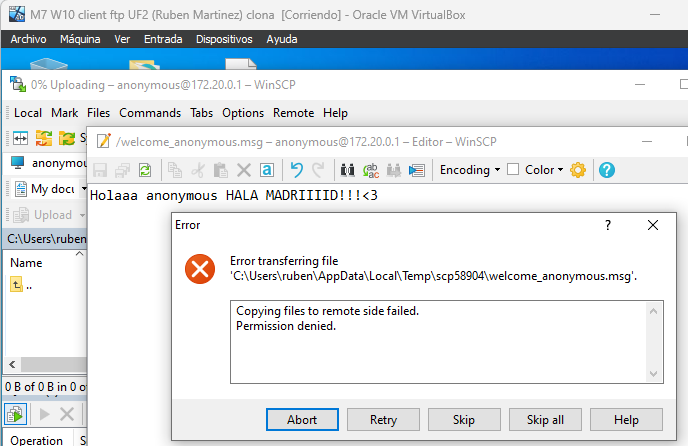




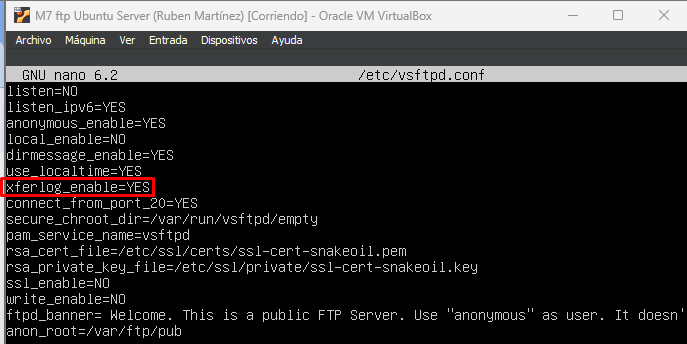
* + - 1. Reinicia el servei.



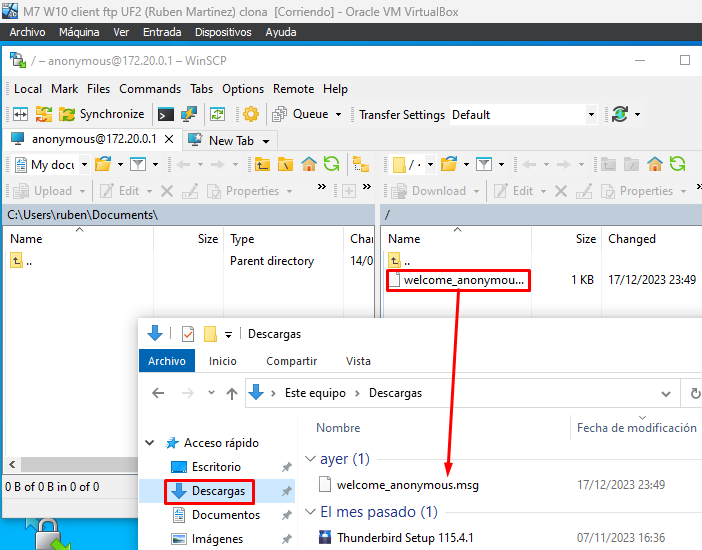
* + - 1. Prova la configuració des del client amb **Software específic**.

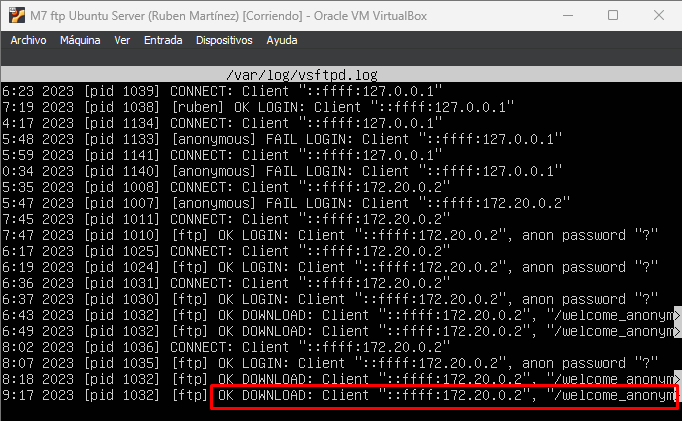


* + 1. Activarem el log del sistema per poder fer un seguiment dels accessos al mateix.
       1. Comprova que la directiva xferlog\_enable=YES. El log estarà com es costum a /var/log: /var/log/vsftpd.log



* + - 1. Descarrega un fitxer amb l’usuari anonymous i comprova el log. Quina és la informació i format que apareix al aquest log?

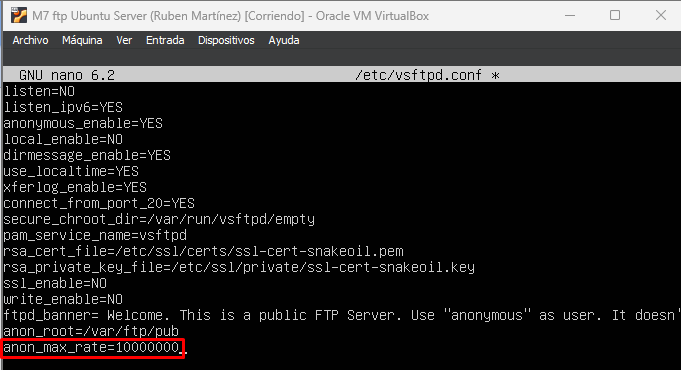




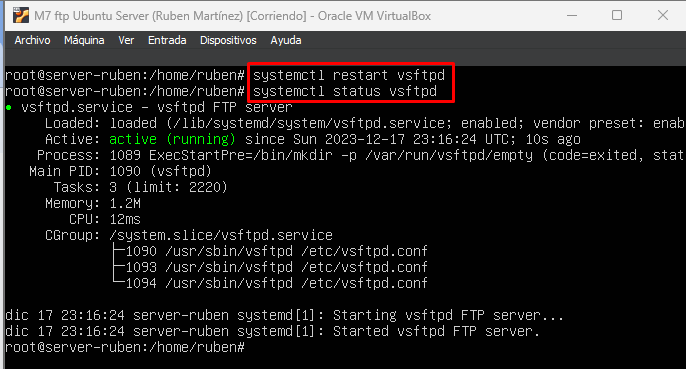
* + 1. Limitació de l’ample de banda per usuaris anònims a 10MBps.
       1. Fes els càlculs per saber quants bytes són 10MB.

10 MB = 10.000.000 de bytes

* + - 1. Afegeix aquest valor amb la directiva anon\_max\_rate=valor\_trobat.

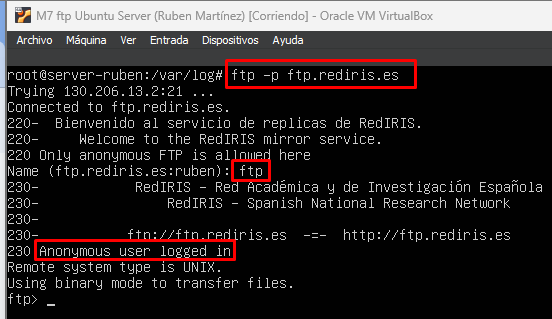


* + - 1. Reinicia el servei.

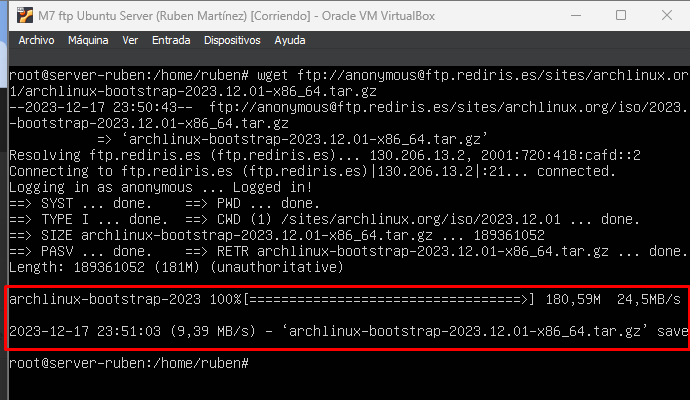


* + - 1. Al servidor:
         1. fent servir el client ftp del servidor accedeix a ftp.rediris.es de manera passiva (El servidor accedeix amb NAT a internet, si cal canvia la interfície a Bridge per poder accedir al serrvidor ftp.rediris.es en mode passiu):

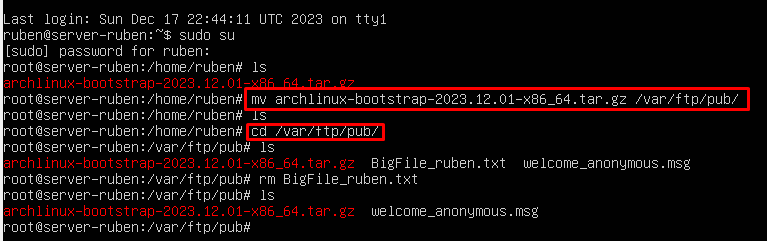
ftp -p ftp.rediris.es



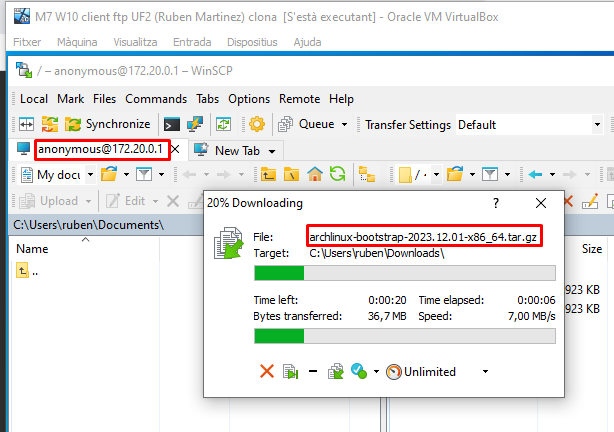
* + - * 1. descarrega un fitxer gran (100 MB o més), busca’l amb WinSCP a l’ordinador amfitrió, serà més fàcil.



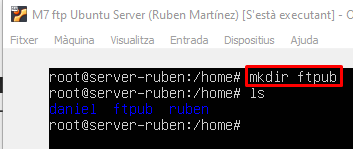
* + - * 1. Fica aquest fitxer al directori arrel de l’usuari anonymous
        2. cp fitxer\_gran /var/ftp/pub/BigFile\_NOM\_ALUMNE.txt.



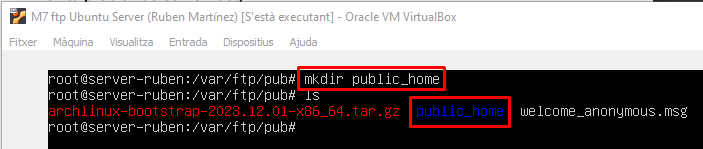
* + - 1. Realitza un accés des del client i fes una descàrrega. Comprova els resultats i la limitació de velocitat.



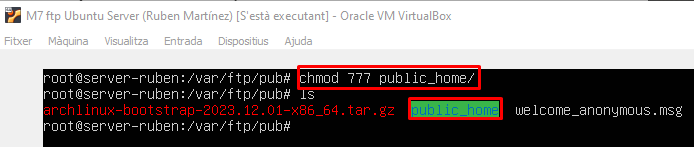
* + 1. Realitzar una operació que permeti als usuaris del sistema ficar fitxers que volen compartir amb la resta del món.
       1. Genera el directori /home/ftpub



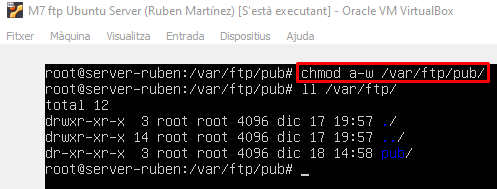
* + - 1. Genera un directori nou a l’arrel del anonymous /var/ftp/pub/public\_home.



* + - * 1. modifica els permisos chmod 777 /var/ftp/pub/public\_home. Què ha passat?



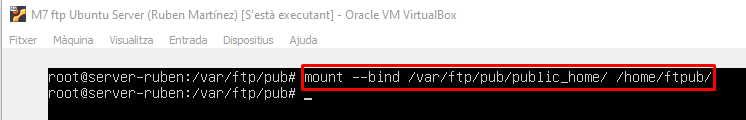
* + - 1. Modifica els permisos de /var/ftp/pub de manera que cap usuari pugui escriure (chmod a-w /var/ftp/pub). Això evita problemes amb chroot().



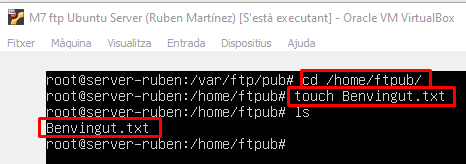
* + - 1. Ves a la consola i fes servir la comanda següent:

mount --bind /var/ftp/pub/public\_home /home/ftpub

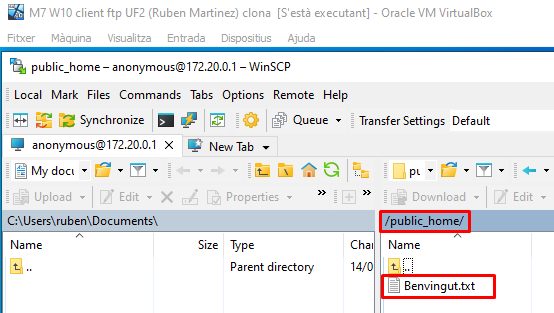
* + - 1. Acabem de realitzar una unitat que permetrà ficar els fitxers que els usuaris desitgin compartir i evitarà les duplicitats de fitxers que provocaria el copiar directament a la ruta arrel de l’usuari anonymous.



* + - 1. Fent servir un usuari del sistema accedeix a la carpeta /home/ftpub i genera un fitxer.

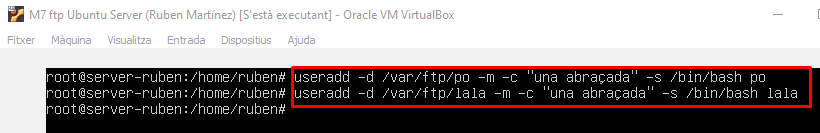


* + - 1. Accedeix amb el client FTP i comprova que realment pots veure aquest fitxer.

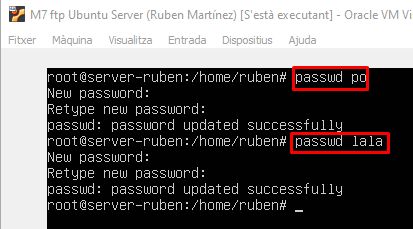


**Preparació del servidor FTP privat**

1. Preparació del servidor FTP per l’accés privat. A continuació prepararem el nostre servidor per permetre als usuaris del sistema l’accés al nostre servidor.
   1. El primer pas serà generar dos usuaris amb el directori canviat: Po i Lala
      1. useradd -d /var/ftp/Po -m -c “una abraçada” -s /bin/bash Po
      2. useradd -d /var/ftp/Lala -m -c “una abraçada” -s /bin/bash Lala

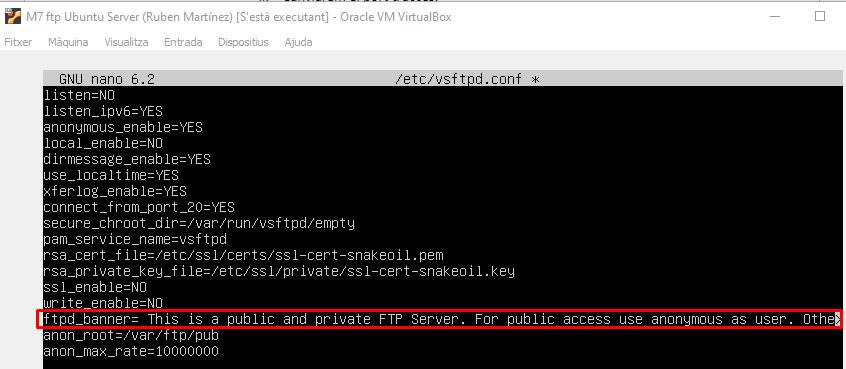


* 1. Crearem una contrasenya per a aquests usuaris
     1. passwd usuari
     2. Posem ‘Teletubi” com a contrasenya



* 1. Canvis a la configuració del FTP:
     1. Canvi del missatge de benvinguda:

ftpd\_banner=This is a public and private FTP server. For public access use anonymous as user. Otherwise use a valid username and password.

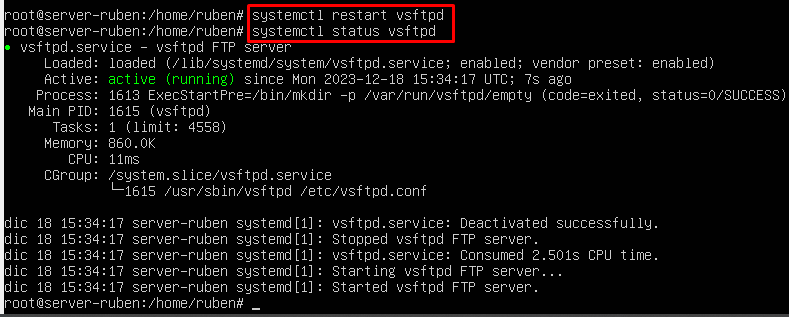


* + 1. Canviarem el port d’accés:

listen\_port=21000

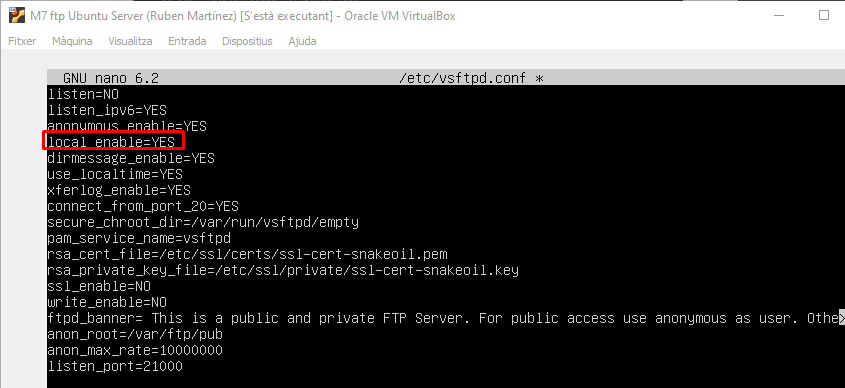


* + - 1. Reinicia el servei i comprova que el canvi és correcte.

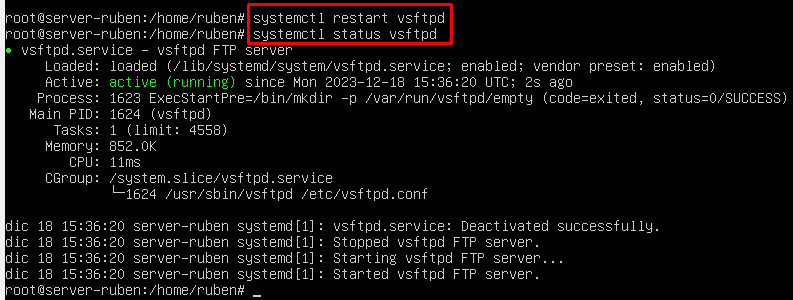


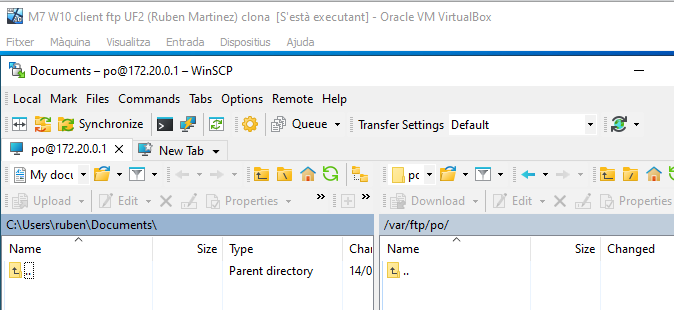
* + 1. Canvi dels permisos dels usuaris del sistema. Busca les següents directives i canvia-les:

local\_enable=YES



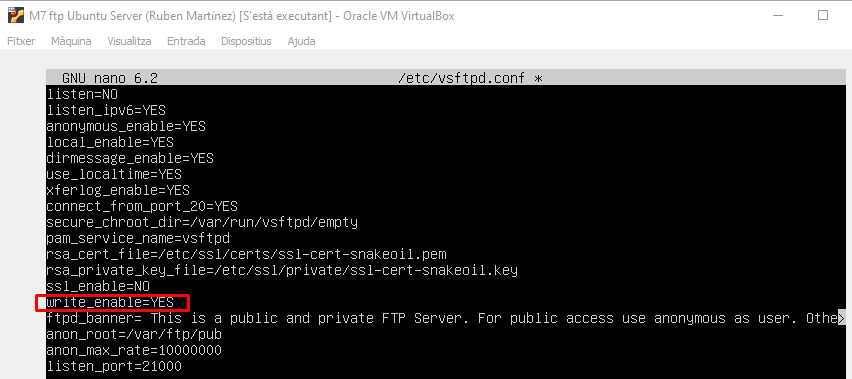
* + - 1. Reinicia el servei i comprova des del client que els usuaris es puguin logejar al servei FTP.



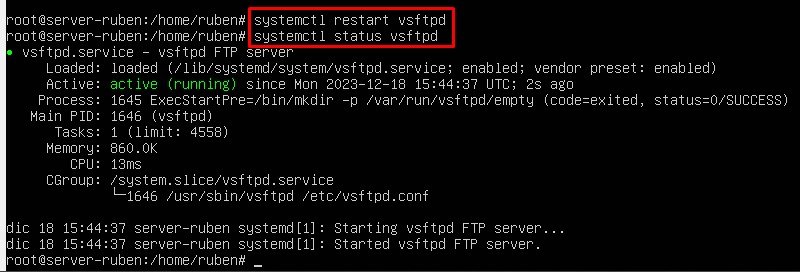


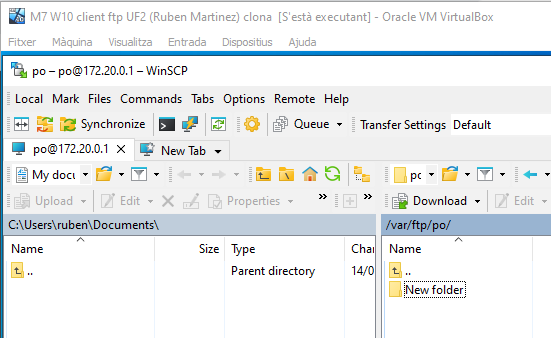
* + 1. Canvi de permisos d’escriptura dels usuaris

write\_enable=YES

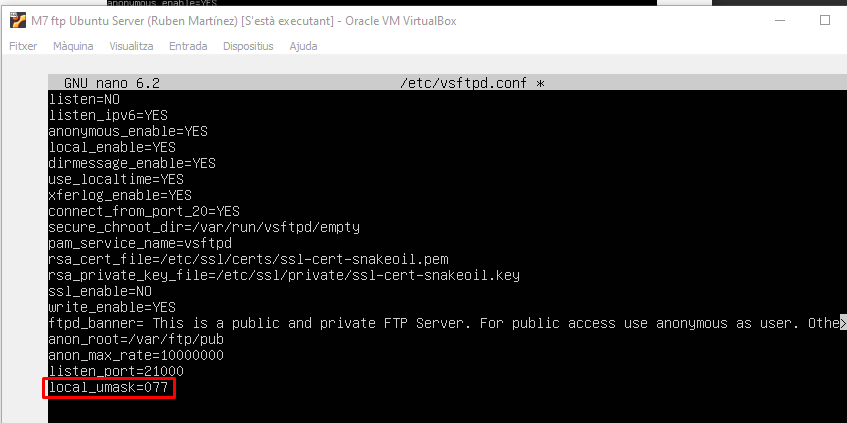


* + - 1. Reinicia el servei i comprova des del client que els usuaris es puguin logejar al servei FTP i que puguin pujar fitxers.

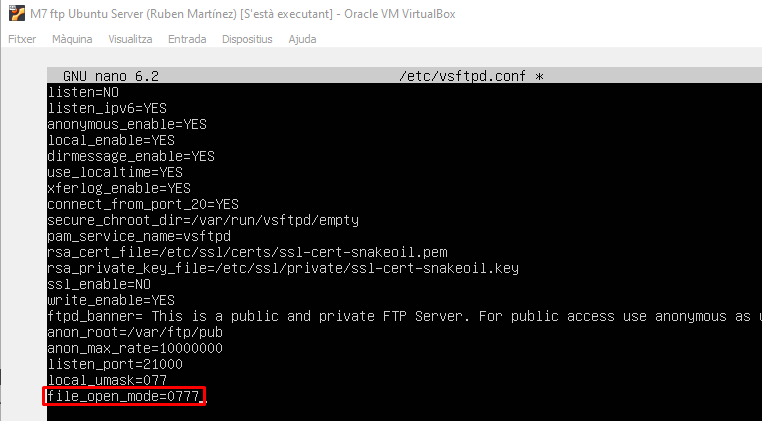




* + 1. Canvi a la màscara que es farà servir quan es pugi un fitxer [local\_umask](https://superuser.com/questions/441515/how-does-local-umask-and-file-open-mode-work)
       1. Normalment treballem amb un Software específic (WinSCP,Filezilla,..) però per fer aquestes proves hem de fer servir **el terminal** (recorda ls -la)
       2. Ara busca l’opció local\_umask per als usuaris locals i comprova el valor que per defecte vsftpd fa servir.



* + - 1. Afegeix la opció file\_open\_mode=0777. (El 0 inicial indica que la nomenclatura és octal)

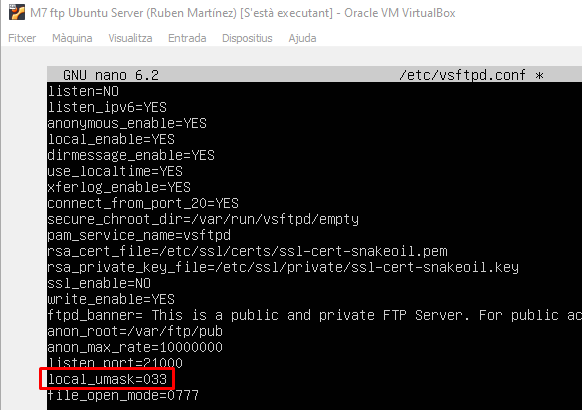


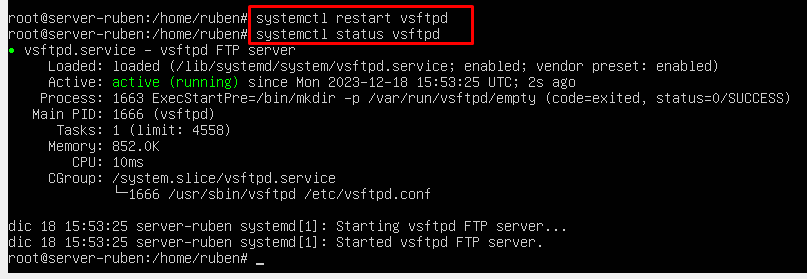
* + - 1. Els permisos s’atorguen de la següent manera:

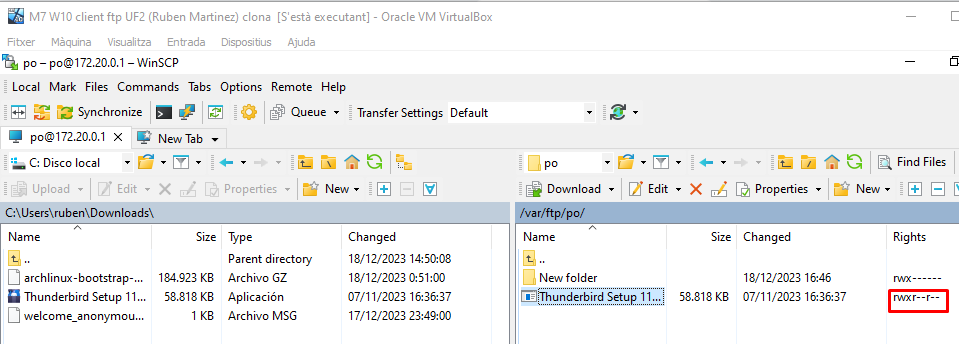
valor file\_open\_mode - permisos que volem donar = valor local\_umask.

Suposem que volem que al afegir un fitxer aquest tingui permís 0700. Donc bé, amb vsftpd haurem de calcular el paràmetre a partir de la següent operació: 777 - 700 = valor de local\_umask. A l’exemple seria 777-0700=0077. Comprova-ho. Nota: si no apareixen els permisos d’execució, teniu en compte que per motius de seguretat, alguns sistemes operatius no permeten crear fitxers amb permisos d’execució.

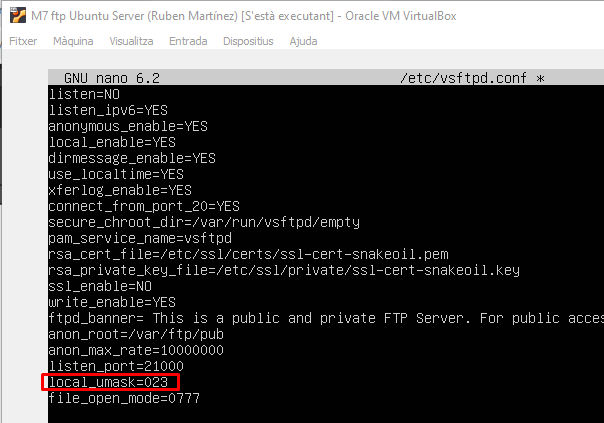
* + - 1. Ara fes que local\_umask sigui 033. Reinicia el servei. Puja un fitxer amb un dels usuaris. Vés al servidor i comprova els permisos del fitxer que hi ha al servidor.



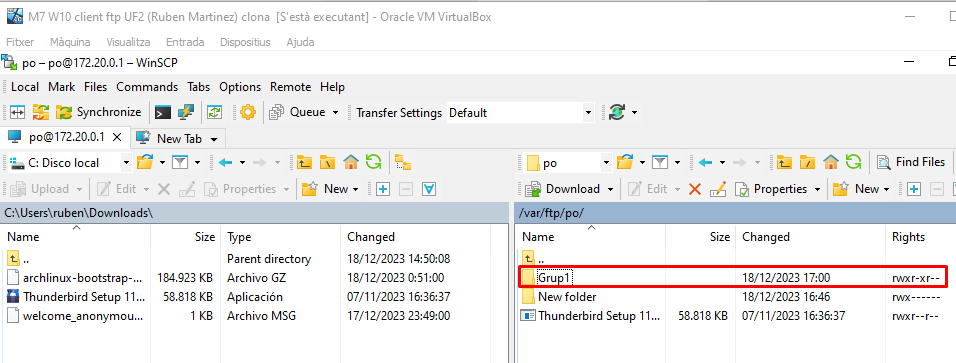




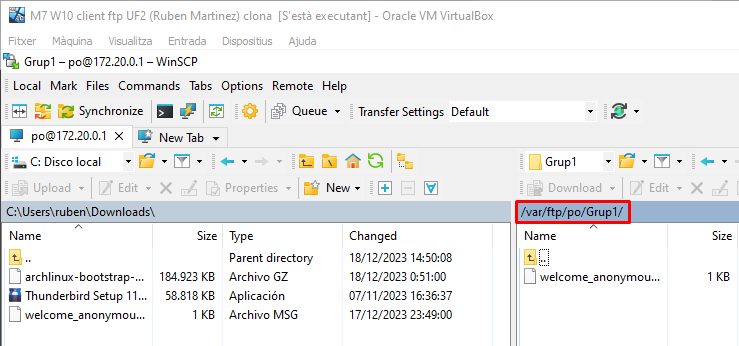
* + - 1. Quin paràmetre seria el correcte si desitjo uns permisos 754 per als directoris? Comprova-ho.



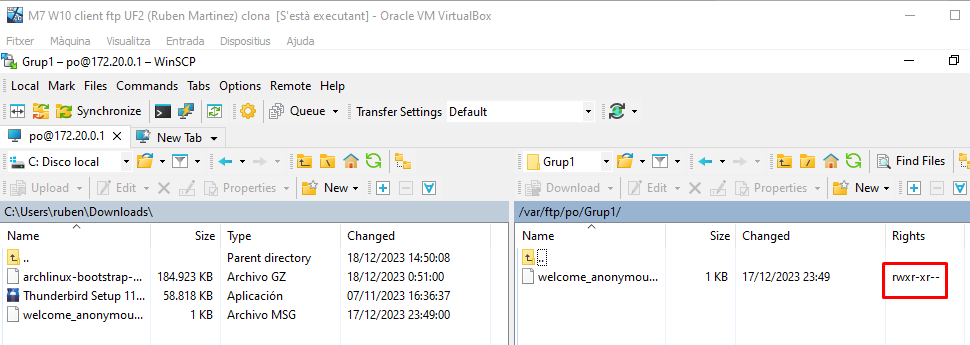
* + - * 1. Genera un directori



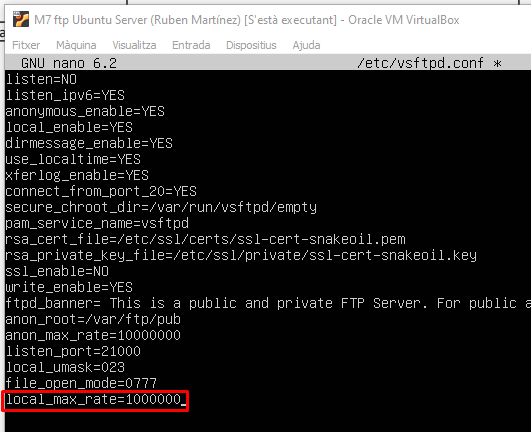
* + - * 1. Afegeix un fitxer a dins



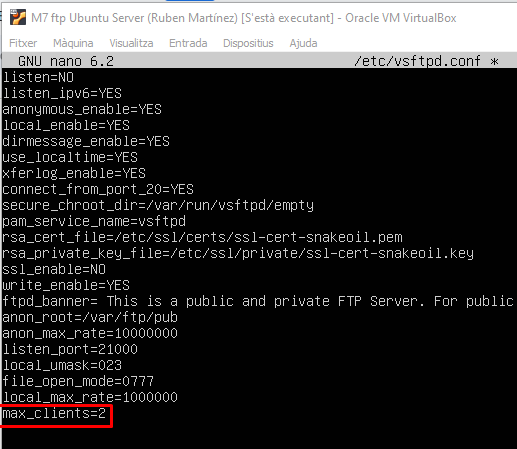
* + - * 1. Quins permisos tenen?



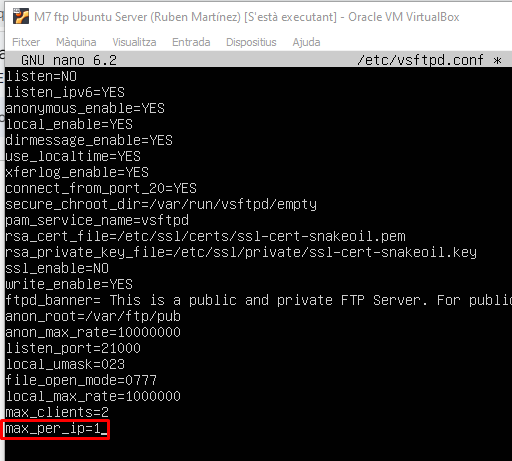
* + 1. Limitacions de velocitat pels usuaris del sistema.
       1. Afegeix la directiva local\_max\_rate per fer que els usuaris pugui descarregar a un màxim de 1MB



* + 1. Limitacions de clients màxims del servidor FTP.
       1. Afegeix la directiva “max\_clients = 2” per fer que el nombre màxim d’usuaris connectats sigui 2. Intenta fer tres connexions.

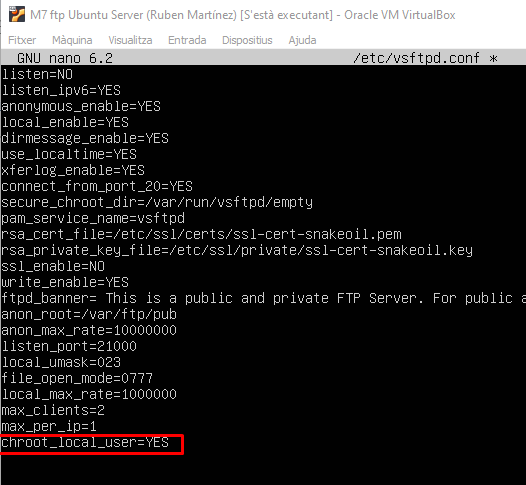


* + 1. Limitacions de clients màxims del servidor des d’una ip
       1. Afegeix la directiva “max\_per\_ip = 1” per fer que el nombre màxim d’usuaris connectats des d’una mateixa IP sigui 1. Intenta fer dues connexions des de la mateixa màquina.

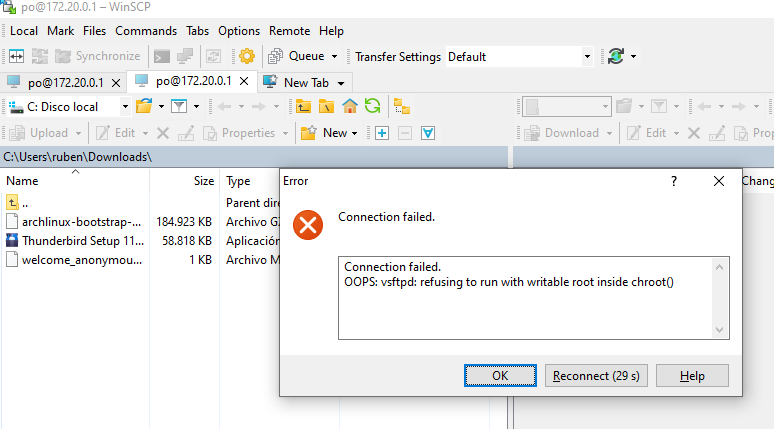


**Usuaris engabiats**

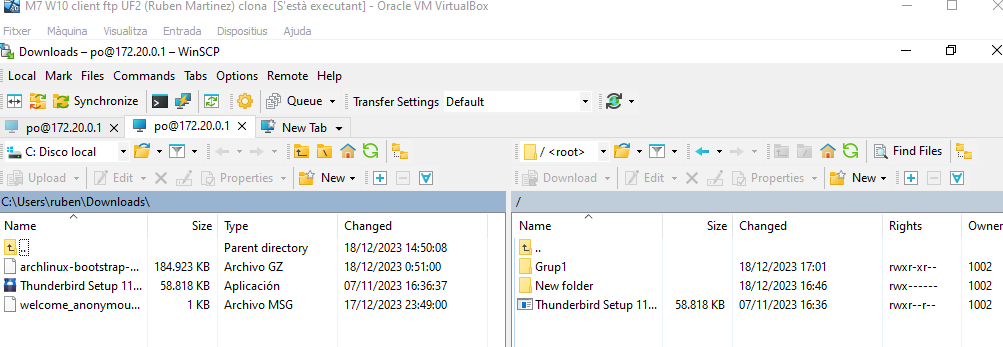
1. Engabiant usuaris. Finalment farem que els nostres usuaris ftp no puguin sortir del seu directori /home.
   1. Busca les directives chroot al fitxer de configuració.
   2. chroot\_local\_user=YES.



* + 1. Intenta connectar amb un dels usuaris locals. Quin error has obtingut? Per què?



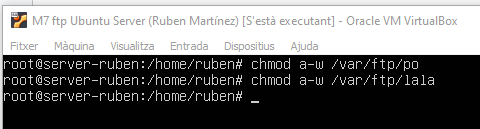
* + 1. A partir de la versió 3.0 de vsftpd es permet la directiva allow\_writeable\_chroot=YES, que permet a un usuari connectar-se amb ftp al seu home amb permís d’escriptura. Això, tot i fer operatiu el servidor genera una vulnerabilitat greu del sistema. Prova fer chroot\_local\_user = YES i allow\_writeable\_chroot=YES. Et pots connectar ara?



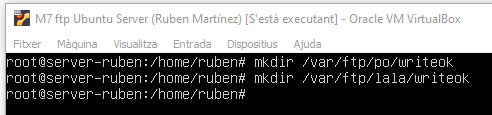
* 1. Chroot ofereix les següents combinacions amb chroot\_local\_user i chroot\_list\_enable
     1. chroot\_local\_user=NO & chroot\_list\_enable = NO, (valor per defecte) Cap usuari està engabiat.
     2. chroot\_local\_user=YES & chroot\_list\_enable = NO, Tots els usuaris està engabiat.
     3. chroot\_local\_user=NO & chroot\_list\_enable = YES, els usuaris de dins la llista estan engabiats i la resta no.
     4. chroot\_local\_user=YES & chroot\_list\_enable = YES, els usuaris de dins la llista no estan engabiats i la resta si.
  2. La directiva chroot\_local\_user activada, degut a la manera de funcionar del servei FTP, planteja problemes de seguretat.
     1. Prova accedir amb un usuari engabiat al sistema.
     2. Quin error apareix?
     3. A què es degut?
        1. [500OOPS](https://www.benscobie.com/fixing-500-oops-vsftpd-refusing-to-run-with-writable-root-inside-chroot/)
  3. Per reduir els perills de seguretat i poder escriure farem què els usuaris no tinguin permís d’escriptura a les seves carpetes home però si a un directori fill:

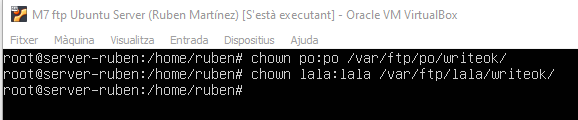
chmod a-w /var/ftp/Po

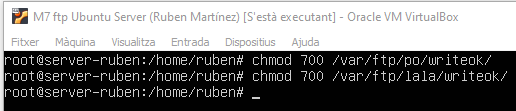
chmod a-w /var/ftp/Lala



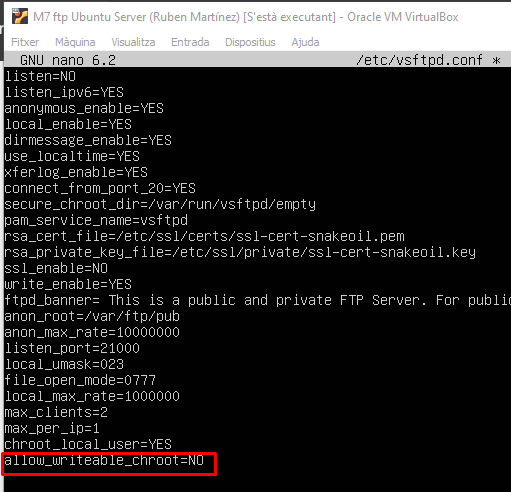
* + 1. Afegeix ara un directori writeok a dins de cada un dels directoris anteriors (assegura’t que els propietaris són Lala i Po). A aquests directoris és on es podrà escriure per tant dona permisos d’escriptura als propietaris.



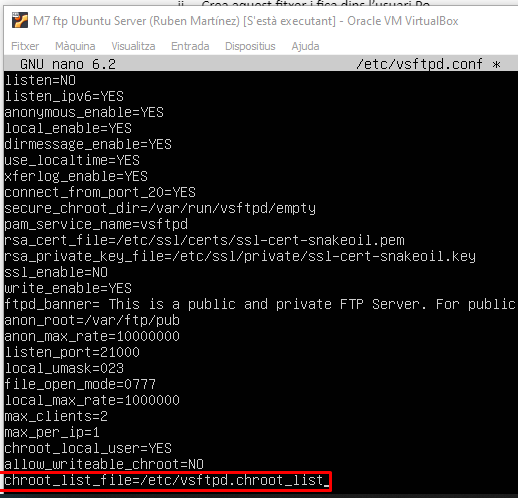




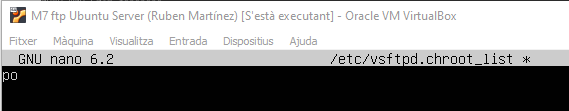
* + - 1. **Si no te’n surts amb els permisos de fitxers** i directoris sempre pots agafar una drecera per camuflar el problema amb les directives chroot\_local\_user = YES o allow\_writable\_chroot = YES. (NOTA: aquesta solució serà avaluada amb menys puntuació donat que provoca fallades de seguretat)



* 1. Posa a Po a la llista d’usuaris, de fet el fitxer només contindrà el seu nom.
     1. Descomenta la directiva: chroot\_list\_file=/etc/vsftpd.chroot\_list

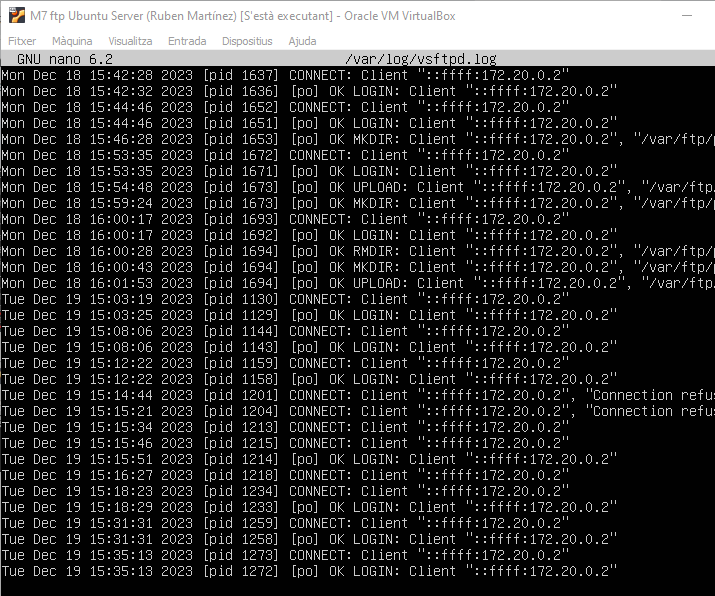


* + 1. Crea aquest fitxer i fica dins l’usuari Po.



* 1. Prova les quatre possibilitats proposades i comprova en cada cas quin usuari es pot moure i quin usuari no ho pot fer.

1. Cerca a /var/log/ i comprova si existeix algun registre propi de vsftp. Quina informació apareix?



**Links addicionals**

[FTP Server](https://help.ubuntu.com/lts/serverguide/ftp-server.html)

[Servidor FTP públic](http://www.linuxhispano.net/2011/02/17/configurar-un-servidor-de-ftp-anonimo-con-vsftpd/)

[chroot, SSL i virtual users on FTP](https://help.ubuntu.com/community/vsftpd)

Si per fer chroot no es volgués canviar els permisos de les carpetes, es podria fer una instal·lació com la següent:

1. sudo apt install python-software-properties
2. sudo add-apt-repository ppa:thefrontiergroup/vsftpd
3. sudo apt update
4. sudo apt install vsftpd
5. allow-writeable-chroot=YES