Protegendo servidores FTP

Sumário

Índice de tabelas

Índice de Figuras

Capítulo 1

Protegendo servidores FTP

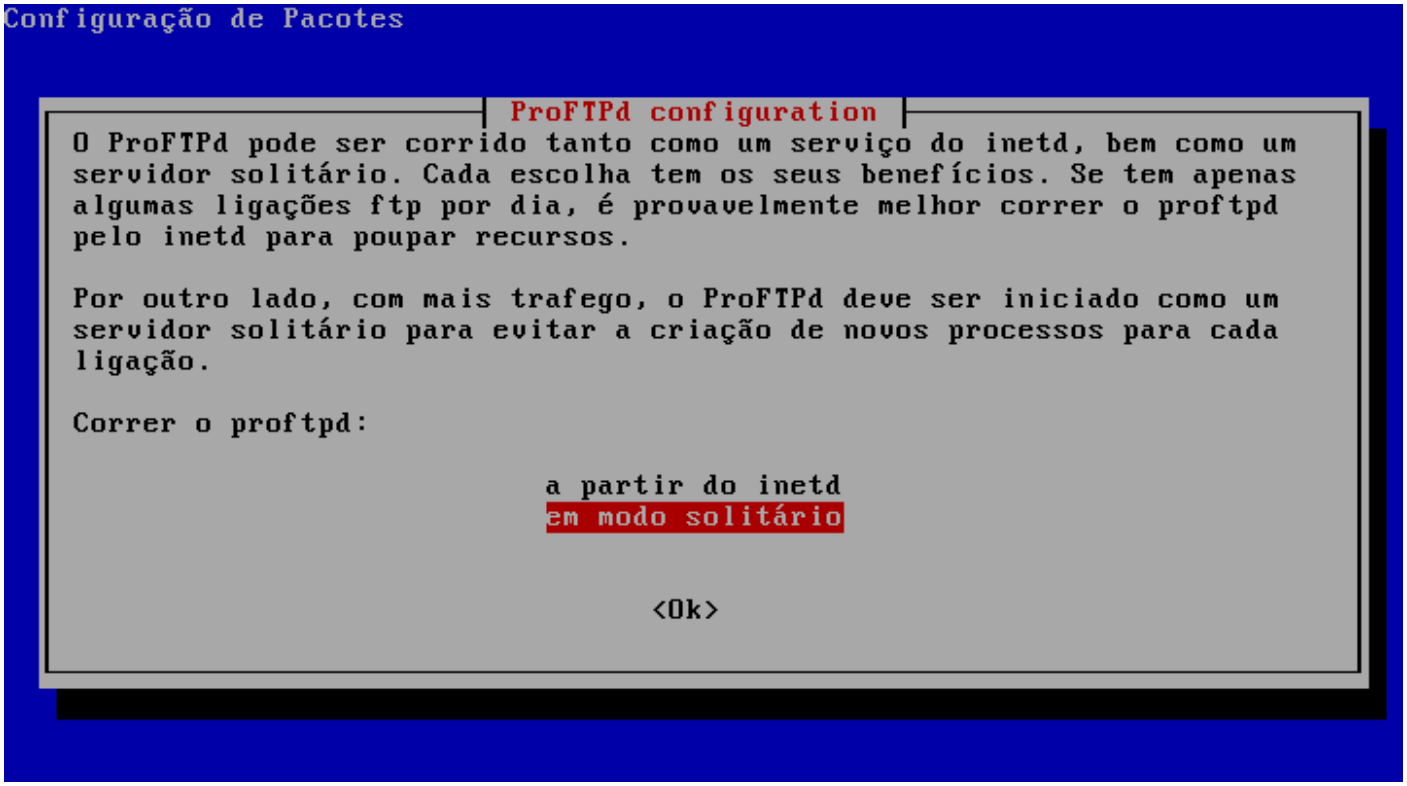
- Instalar e configurar o PROFTPD;
- Principais comandos do FTP.

1.1. Mãos a obra

A transferência de arquivos usando FTP, pode ser feita de varias maneiras ao lado do cliente, como por exemplo utilizando um navegador ou um cliente de FTP para realizar downloads e uploads. Ao lado do servidor podemos implementar um serviço de FTP utilizando diversos programs, como o Proftpd, VSftpd, pure-ftpd, entre outros. Vamos na pratica instalar e configurar o ProFTPD.

Instalando o pacote

```
# aptitude install proftpd
```



Na instalação é possível escolher como o ProFTPD ira trabalhar, selecione a opção “em modo solitário” para trabalhar em standalone.

Conhecendo os arquivos do ProFTPD

Vamos conhecer a função dos arquivos de configuração do ProFTPD, para isso liste o conteúdo do diretório /etc/proftpd.

```
# ls -l /etc/proftpd
```

```
-rw-r--r-- 1 root root  663 Nov 10 15:19 ldap.conf
-rw-r--r-- 1 root root 1453 Nov 10 15:19 modules.conf
-rw-r--r-- 1 root root 4731 Nov 10 15:19 proftpd.conf
-rw-r--r-- 1 root root  862 Nov 10 15:19 sql.conf
-rw-r--r-- 1 root root 1715 Nov 10 15:19 tls.conf
```

Descrição dos arquivos:

ldap.conf → Arquivo que contem uma amostra de como usar LDAP como base de dados para autenticar usuários no ProFTPD;

modules.conf → Arquivo de configuração para gerenciar os módulos do ProFTPD;

proftpd.conf → Arquivo principal de configuração do ProFTPD;

sql.conf → Arquivo que contem uma amostra de como usar SQL como base de dados para autenticar usuários no ProFTPD;

tls.conf → Arquivo que contem uma amostra de como usar TLS nas conexões do ProFTPD.

Configurar o ProFTPD

Abra o arquivo de configuração do servidor e e veja a descrição das opções:

```
# vim /etc/proftpd/proftpd.conf
```

Módulos incluídos

Include /etc/proftpd/modules.conf

Suporte a IPv6

UseIPv6 on

Define o nome do servidor

ServerName "Debian"

Modo de trabalho do servidor (inetd ou standalone)

ServerType standalone

Desativa mensagens de boas vindas

DeferWelcome off

Ativa o modo “chroot” deixando o usuário preso em seu diretório home

DefaultRoot ~

Exige ou não que os usuários tenham um shell valido em /etc/shells

RequireValidShell off

Define a porta padrão do servidor

Porta 21

Define o numero máximo de conexões simultâneas

MaxInstances 30

Define qual usuário e grupo para o servidor quando for executado

User proftpd

Group nogroup

Define a mascara para criação de novos arquivos e diretórios

Umask 022 022

Define o arquivo de log que ira registrar as transferências de arquivos

TransferLog /var/log/proftpd/xferlog

Define o arquivo de log que ira registrar o comportamento do servidor

SystemLog /var/log/proftpd/proftpd.log

Define a configuração dos módulos

<IfModule nome_do_modulo>>

</IfModule>

Define a configuração de acesso a usuários anônimos

<Anonymous ~ftp>

</Anonymous>

Prática: Acessar o servidor em modo texto e browser

Modo texto

No terminal da maquina cliente, digite ftp ip_do_servidor. Exemplo:

 # ftp 192.168.200.10

```
Connected to 192.168.200.10.
220 ProFTPD 1.3.1 Server (Debian) [::ffff:192.168.200.10]
Name (192.168.200.10:root): aluno
331 Password required for aluno
Password:
230 User aluno logged in
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> _
```

Principais comandos do FTP

help → Lista os comandos disponíveis;

help Comando → Mostra uma ajuda para o comando; Exemplo:

ftp> help get

ls → Lista os arquivos no servidor;

!ls → Lista os arquivos da maquina local;

cd → Troca de diretório no servidor; Exemplo:

ftp> cd teste

lcd → Troca de diretório da maquina local; Exemplo:

ftp> lcd /tmp

pwd → Exibe o diretório atual no servidor;

!pwd → Exibe o diretório atual na maquina local;

get → Faz download de um arquivo do servidor para a maquina local; Exemplo:

ftp> get lista.txt

mget → Faz download de mais de um arquivo;

ftp> mget *

put → Faz upload de um arquivo da maquina local para o servidor; Exemplo:

ftp> put agenda.pdf

mput → Faz upload de mais de um arquivo; Exemplo:

ftp> mput *

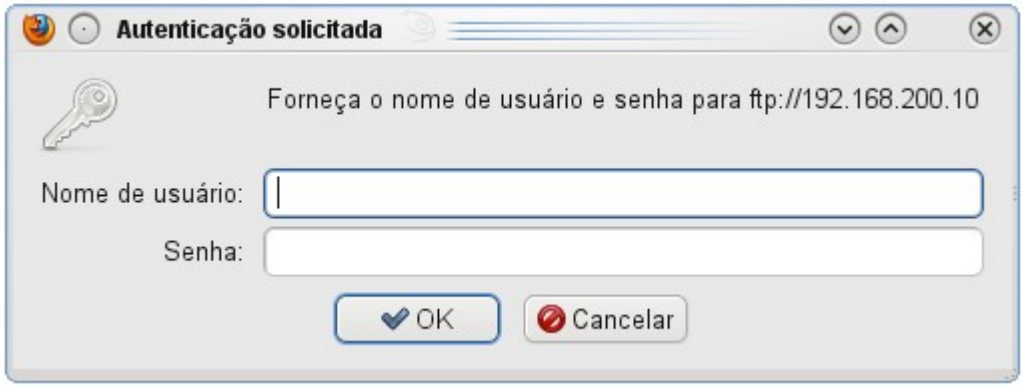
prompt → Ativa ou desativa o modo interativo para downloads e uploads;

quit → Abandona o prompt de comandos do FTP.

Modo gráfico

Abra um navegador e digite ftp://ip_do_servidor, entre com o nome do usuário e senha. Exemplo:

ftp://192.168.200.10

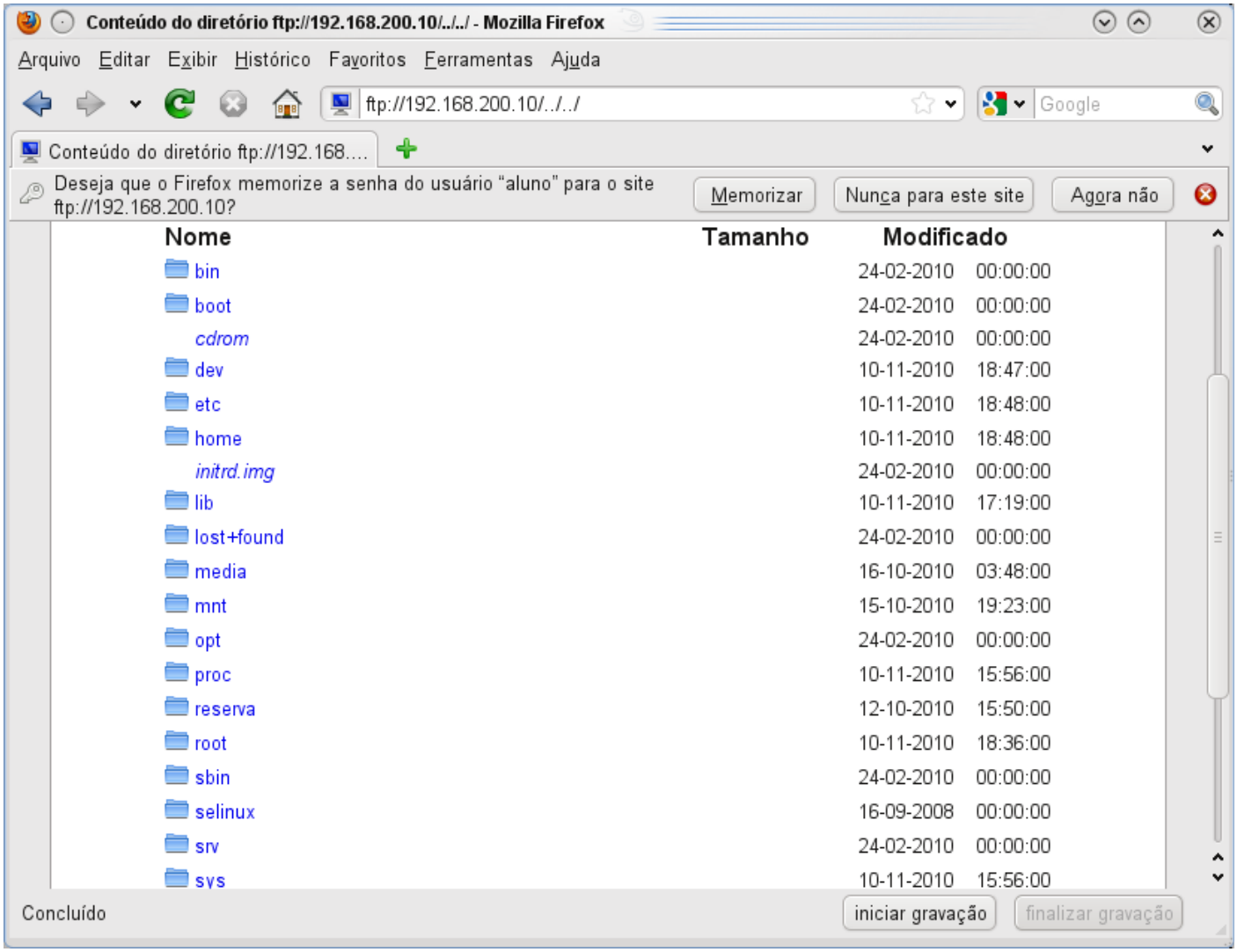


Dica de segurança: No arquivo de configuração do ProFTPD descomente a opção "DefaultRoot" para deixar o usuário logado preso em sua home.

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

O que pode acontecer caso não descomente esta opção?

O usuário logado poderá navegar por toda a estrutura de diretórios do servidor, clicando em "Um diretório acima". Exemplo:



Por padrão o ProFTP apenas aceita logins de usuários com uma conta valida no servidor!

Como habilitar o acesso a usuários anônimos?

Abra o arquivo de configuração do servidor e descomente as linhas de <Anonymous ~ftp> a </Anonymous>. Isso poderá ser feito de forma manual apagando linha a linha, ou de forma prática e rápida com o vim. Vamos a prática:

```
# vim /etc/proftpd/proftpd.conf
```

Com o arquivo aberto numere as linhas usando :set nu, e procure a linha da opção <Anonymous ~ftp> e a linha da opção </Anonymous>.

No exemplo deste documento as opções para usuário anonimo inicia na linha 132 e termina na linha 171. Para descomentar use o comando :132,171 s/^#/

Grave as alterações e restarte o serviço com o comando:

```
# invoke-rc.d proftpd restart
```

Testando o acesso:

```
# ftp 192.168.200.10
```

```
Connected to 192.168.200.10.
220 ProFTPD 1.3.1 Server (Debian) [::ffff:192.168.200.10]
Name (192.168.200.10:root): anonymous
331 Anonymous login ok, send your complete email address as your password
Password:
230-Welcome, archive user anonymous@::ffff:192.168.200.5 !
230-
230-The local time is: Wed Nov 10 19:25:30 2010
230-
230-This is an experimental FTP server.  If you have any unusual problems,
230-please report them via e-mail to <root@server.empresa.com.br>.
230-
230 Anonymous access granted, restrictions apply
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> _
```

Para bloquear o acesso a usuários anônimos, novamente abra o arquivo e comente das linhas 132 a 171 com o comando 132,171 s/^/# e não esqueça de restartar o serviço.

Como configurar quais usuários não terão acesso ao FTP?

Isso é possível adicionando o nome de um ou mais usuários no arquivo /etc/ftpuser.

```
# /etc/ftpusers: list of users disallowed FTP access. See ftpusers(5).

root
daemon
bin
sys
sync
games
man
lp
mail
news
uucp
nobody
```

Capítulo 2

Gerenciando

2.1. Objetivos

•Trobleshooting: Utilizar regras do PAM com o FTP.

2.1. Troubleshooting

Como posso configurar regras do PAM para FTP?

Isso é possível através do arquivo /etc/pam.d/proftpd que é criado na instalação do pacote, nele podemos adicionar módulos e controles do PAM, além de argumentos. Vamos a prática:

Abra o arquivo com o comando vim

```
# vim /etc/pam.d/proftpd
```

```
#%PAM-1.0
auth       required     pam_listfile.so item=user sense=deny file=/etc/ftpusers
onerr=succeed
@include common-auth

# This is disabled because anonymous logins will fail otherwise,
# unless you give the 'ftp' user a valid shell, or /bin/false and add
# /bin/false to /etc/shells.
#auth       required    pam_shells.so

@include common-account
@include common-session
```

O arquivo já vem com uma regra usando o módulo pam_listfile.so para bloquear o acesso a determinados usuários. Vamos a descrição dos argumentos utilizados:

item → Usado para verificar o nome de usuário;

sense → Nega o acesso se o usuário existir no arquivo especificado;

file → Nome do arquivo que contém a lista de usuários;

onerr → Indica sucesso no login, caso o nome não exista na lista de usuários.

Outras configurações estão inclusas dos arquivos common-auth, common-account e common-session, todos localizados em /etc/pam.d

Limitar acesso ao FTP por horário

Antes de configurar modulo pam_time.so, é necessário habilitar a autenticação por PAM no ProFTPD. Abra o arquivo de configuração e descomente a opção “AuthOrder”. Exemplo:

```
# This is required to use both PAM-based authentication and local passwords
AuthOrder                       mod_auth_pam.c* mod_auth_unix.c
```

Grave as alterações e restarte o serviço com o comando:

```
# invoke-rc.d proftpd restart
```

Agora podemos configurar o acesso por horario, vamos a prática:

1 – Abra o arquivo de configuração em /etc/pam.d/proftpd

```
# vim /etc/pam.d/proftpd
```

2 – Adicione a linha abaixo:

```
account    required     pam_time.so
```

3 – Abra o arquivo de configuração do módulo em /etc/security/time.conf, e configure os dias e horários que os usuários poderão realizar acesso via FTP. Exemplo:

```
proftpd;*;aluno;Al0800-1800
```

Em nosso exemplo o usuário aluno esta autorizado a acessar o servidor FTP das 08:00 as 18:00. Veja o que acontece quando um usuário tenta acessar o servidor fora do horário.

```
Connected to 192.168.200.10.
220 ProFTPD 1.3.1 Server (Debian) [::ffff:192.168.200.10]
Name (192.168.200.10:root): aluno
331 Password required for aluno
Password:
530 Login incorrect.
Login failed.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> _
```