Instalação do Servidor de FTP (parte 2)

Prof. Dr. Márcio Andrey Teixeira
Instituto Federal de São Paulo – Campus Catanduva
Catanduva, SP
Membro Sênior do IEEE
marcio.andrey@ifsp.edu.br

Configurando o ftp anonymous

A princípio, apenas os usuários que tiverem logins válidos no servidor poderão acessar o FTP. Caso você queira abrir um FTP público, descomente as seguintes linhas do arquivo de configuração que estão entre:

<Anonymous ~ftp>

</Anonymous>

Com esta configuração, os usuários poderão logar no sistema como anônimos, onde o diretório **/srv/ftp** será o seu diretório raíz. Nesse caso, logado como anonymous, os usuários não poderão ver e muito menos escrever em outros lugares do sistema.

Configurando o ftp anonymous

Caso você esteja em outra distribuição e queira definir outro lugar para colocar o diretório ftp, execute os seguintes passos:

Crie o diretório que será o “diretório raiz” do servidor de ftp, por exemplo dentro de /var.

cd /var
mkdir ftp

Mude as permissões do grupo e dono para ftp
 # chown ftp ftp
 # chgrp ftp ftp

Agora, descomente as linhas referentes ao usuário anônimous e faça a seguinte modificação:

<Anonymous /var/ftp>

Reinicie o serviço de FTP:
sudo systemctl reload proftpd

Criando uma pasta para upload no servidor de FTP

Não é bom que os usuários que acessem o servidor de ftp gravem seus arquivos lá. Porém, pode acontecer que seja necessário por algum motivo, disponibilizar uma área pra que o usuário possa fazer isto.

Para isso, é de costume, configurar um local para os usuário gravarem seus arquivos. Por padrão esse diretório é o /incoming.

O diretório /incoming é criado no diretório raíz do servidor de FTP. Para criar esse diretório execute os seguintes comandos:

 # cd /var/ftp/

 # mkdir incoming

Feito isto, é necessário trocar o dono e o grupo deste diretório para ftp.

Criando uma pasta para upload no servidor de FTP

 # chown ftp incoming
 # chgrp ftp incoming

É necessário fazermos uma referência dentro da diretiva do anonymous deste diretório. Para tanto, insira as seguintes linhas depois de **</Limit>** e antes de **</Anonymous>** no arquivo proftpd.conf.

```
<Directory incoming>
  <Limit READ WRITE>
     DenyAll
  </Limit>
  <Limit STOR>
     AllowAll
  </Limit>
</Directory>
```

Criando usuários

Imagine que você queira fazer uma configuração mais complexa, com vários usuários, onde cada usuário tem acesso a uma pasta específica.

Vamos exemplificar da seguinte forma. Você criou um repositório para arquivos de vários sites. O mantenedor do site10 pode fazer upload para a sua pasta, e não deve ter acesso a outras pastas ou a arquivos do sistema.

A forma mais fácil de se fazer isso é criar os usuários que terão acesso ao FTP, colocando a pasta a que terão acesso como seu diretório home e bloqueando o uso do shell para que ele não possa ter acesso a máquina via login remoto (telnet, ssh ertc).

Criando usuários

Vamos fazer o seguinte, primeiramente vamos padronizar o lugar que será a pasta raiz do FTP. A pasta raiz estará localizada em **/home/ftp**. Para isso crie essa pasta da seguinte forma:

cd /home
 # mkdir ftp

Agora, vamos criar um usuário chamado site10

 # adduser site10
 # passwd site10
Changing password for user site10.
New password:
Retype new password:

Criando usuários

Feito isto, por padrão, o diretório foi criado no /home/site10. Abra o arquivo /etc/passwd e verifique que a seguinte linha foi adicionada ao arquivo:

site1:x:504:504::/home/site10:/bin/bash

Modifique para:

site1:x:504:504::/home/ftp/site10:/bin/false

Agora mova a pasta site1 para dentro de /home/ftp

 # mv site1/ ftp/

Criando usuários

Agora vamos modificar o arquivo proftpd.conf:

Para que o usuário anonymous tenhe acesso somente de leitura no diretório /home/ftp, faça o seguinte:

Troque a diretiva **<Anonymous /var/ftp>** para **<Anonymous /home/ftp>**

Descomente a seguinte linha:

DefaultRoot ~

O comando acima faz com que os usuários tenham acesso apenas aos seus diretórios padrões, não podendo acessar nenhum outro diretório. Feito isso, execute o seguinte comando

 # echo "/bin/false" >> /etc/shells

O comando acima habilita a utilização o shell **/false**

Feito isto, reinicie o proftpd e pronto.

Prof. Dr. Marcio Andrey Teixeira

marcio.andrey@ifsp.edu.br

http://marcioandrey.pro.br

Bibliografia

SILVA, G. M.. Segurança em sistemas Linux. 1. ed. Rio de Janeiro: Ciência Moderna, 2008. 240p.
THOMPSON, M. A.. Windows Server 2012: fundamentos. 1. ed. São Paulo: Érica, 2012. 232p.
VIANA, E. R. C.. Virtualização de servidores Linux para redes corporativas: guia prático. 1.
ed. Rio de Janeiro: Ciência Moderna, 2008. 342p.
6 - BIBLIOGRAFIA COMPLEMENTAR:
KUROSE, J. F.; ROSS, K. W.. Computer networking: a top-down approach. 6. ed. AddisonWesley, 2012. 864p.
SCHRODER, C.. Redes Linux: livro de receitas. 1. ed. Rio de Janeiro: Alta Books, 2006. 569p.