Administração de Redes de Computadores

- **xinetd**
- **Wu-FTP**: servidor de FTP

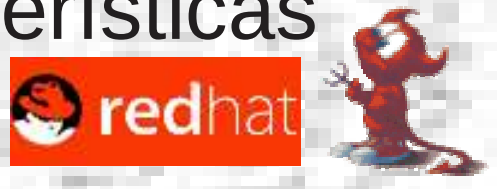
Alexssandro C. Antunes
(Alexssandro.Antunes@unisul.br)

Introdução

Um dos mais freqüentes, e mais fortes motivos para um indivíduo utilizar uma rede de comunicação de dados, ou uma rede de computadores, são os serviços de conectividade e de comunicação que o usuário da rede, em geral, tem disponível

Internet Daemon

- O inet, internet super Server, é responsável por vários serviços básicos de um sistema, os quais são disponibilizados em uma rede. Dentre estes serviços podemos citar o telnet e o ftp.
- O xinetd é o substituto do inetd, incorporando algumas características como a segurança.



Arquivos de configuração do xinetd

/etc/xinetd.conf

(Extended Internet Services Daemon configuration file)

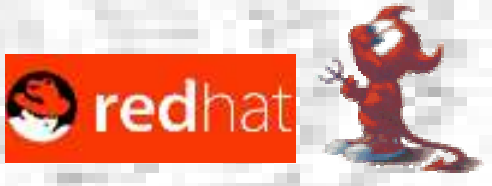
- O arquivo xinetd.conf é o arquivo de configuração que determina os serviços providos pelo xinetd
- Por definição, o xinetd.conf contém um conjunto básico de configuração, os quais são aplicados à todos os serviços

Exemplo do xinetd.conf

```
defaults
{
        instances               = 60
        log_type                = SYSLOG authpriv
        log_on_success          = HOST PID
        log_on_failure          = HOST
        cps                     = 25 30
}
```

Aspectos do xinetd.conf

- **instances**: seleciona o número máximo de requisições de um serviço particular pode manipular; isto pode evitar um DoS (Deniel of Service);
- **log_type**: diz ao xinted como o mesmo deverá realizar o log das requisições; neste caso, o xinetd utilizará o authpriv log, especificado no arquivo /etc/syslog.conf que aponta para /var/log/secure por definição.



Aspectos do xinetd.conf(cont.)

- **log_on_success**: diz ao xinetd que informações devem ser capturadas do usuário, caso o logon seja com sucesso; por definição o endereço de IP remoto e o número/identificação do processo (process ID) do servidor são gravados;

Aspectos do xinetd.conf(cont.)

- **log_on_failure**: diz ao xinetd que devem ser capturadas no caso de falha de logon;
- **cps**: diz ao xinetd para não permitir mais que 25 conexões por segundo para um dado serviço. Se o limite for alcançado, o serviço é suspenso por 30 segundos.

Arquivos do diretório /etc/xinetd.d

- Os arquivos do diretório /etc/xinetd.d são lidos toda vez que o xinetd é inicializado

Listagem parcial dos arquivos no diretório:

```
[root@host175 xinetd.d]# ls -la
total 60
drwxr-xr-x   2 root    root       4096 Jul 16 14:20 .
drwxr-xr-x  51 root    root       4096 Jul 16 15:28 ..
-rw-r--r--   1 root    root        563 Apr 16 14:05 chargen
-rw-r--r--   1 root    root        580 Apr 16 14:05 chargen-udp
-rw-r--r--   1 root    root        419 Apr 16 14:05 daytime
-rw-r--r--   1 root    root        438 Apr 16 14:05 daytime-udp
-rw-r--r--   1 root    root        341 Apr 16 14:05 echo
-rw-r--r--   1 root    root        360 Apr 16 14:05 echo-udp
-rw-r--r--   1 root    root        317 Jun 25  2002 rsync
-rw-r--r--   1 root    root        312 Apr 16 14:05 servers
-rw-r--r--   1 root    root        314 Apr 16 14:05 services
-rw-r--r--   1 root    root        392 Aug 11  2002 sgi_fam
-rw-r--r--   1 root    root        497 Apr 16 14:05 time
-rw-r--r--   1 root    root        518 Apr 16 14:05 time-udp
```

Instalando e configurando o servidor de telnet

- verificando o diretório /etc/xinetd.d
- instalando o telnet server
  - rpm -iv telnet-server-0.17-23.i386.rpm
- verificando novamente o diretório /etc/xinetd.d

Listando o conteúdo de /etc/xinetd.d/telnet

```
service telnet
{
        flags           = REUSE
        socket_type     = stream
        wait            = no
        user            = root
        server          = /usr/sbin/in.telnetd
        log_on_failure  += USERID
        disable         = yes
}
```

Realizando o acesso via telnet

```
[antunes@ar antunes]$ telnet 192.168.1.1
Trying 192.168.1.1...
Connected to 192.168.1.1.
Escape character is '^]'.
Red Hat Linux release 8.0 (Psyche)
Kernel 2.4.18-14 on an i686
login: antunes
Password:
Last login: Wed Jul 16 17:07:45 from ar
[antunes@host175 antunes]$
```

Verificando os logs de acesso

Segundo as configurações do arquivo xinetd.conf o atributo log_type especifica aonde o xinetd deve realizar o log das requisições; neste caso, em /var/log/secure

Log de acesso:

Jul 16 17:14:58 host175 xinetd[1201]: START: telnet pid=1911 from=192.168.1.2

Obs.: verificar ->/etc/rc.d/init.d/syslog status

/etc/hosts.deny

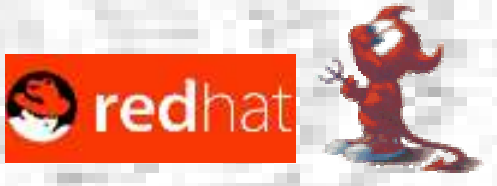
Se incluirmos o IP remoto no arquivo hosts.deny (All:192.168.1.2), a conexão não será realizada. Segue abaixo a tentativa de conexão e o log.

```
[antunes@ar antunes]$ telnet 192.168.1.1
Trying 192168.1.1...
Connected to 192.168.1.1.
Escape character is '^]'.
Connection closed by foreign host.
[antunes@ar antunes]$
```

Verificando novamente os logs de acesso

Log de acesso:

Jul 16 17:19:19 host175 xinetd[1987]: FAIL: telnet libwrap from=192.168.1.2



/etc/hosts.allow

Sua sintaxe é semelhante ao do arquivo /etc/hosts.deny

Exemplo:

#libera localhost a conectar nos serviços FTP e TELNET

in.ftpd:localhost

in.telnetd:localhost

#libera todos os serviços para a máquina 200.158.118.169

All:200.158.118.169

Utilizando o nmap

(The 1596 ports scanned but not shown below are in state: closed)

Port	State	Service
22/tcp	open	ssh
23/tcp	***open***	***telnet***
80/tcp	open	http
111/tcp	open	sunrpc
1024/tcp	open	kdm
6000/tcp	open	X11

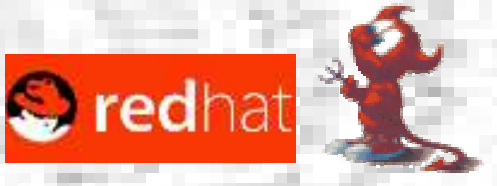
Servidor de FTP

Um dos principais métodos de tranferência de arquivos de um ponto da internet a outro é o protocolo de tranferência de arquivos (FTP).

Desenvolvido mais especificamente para a transferência de arquivos maiores que os transferidos via HTTP. Este também é capaz de realizar outras tarefas que o HTTP não é capaz

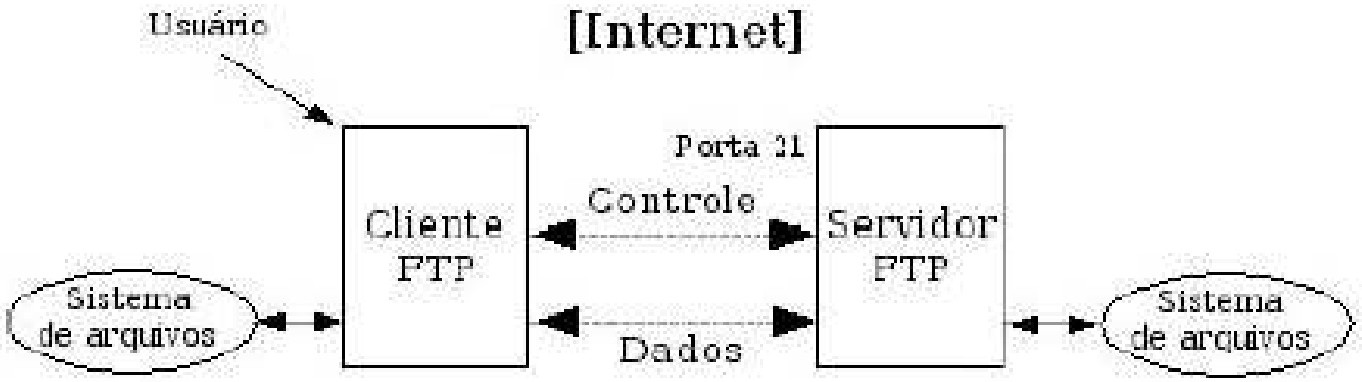
FTP x HTTP

Características	FTP	HTTP
Baseado em sessão	Sim	Não
Autenticação de usuários incorporada ou embutida	Sim	Não
Voltado primeiramente para transeferência	De grandes arquivos binários	Pequenos arquivos texto
Modelo de conexão	Dupla	Simples
Suporta modos de transferência ASCII e binário	Sim	Não
Suporta operações de sistema de arquivos (mkdir, rm, dentre outros)	Sim	Não



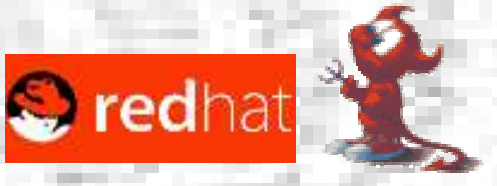
Servidor de FTP (cont.)

O protocolo de transferência de arquivos (**F**ile **T**ransfer **P**rotocol) é um método de transferência de arquivos entre máquinas em uma rede e/ou na internet.



FTP – Tipos de dados

- ASCII: é o valor padrão assumido pelo FTP e deve estar disponível em todas as suas versões.
- Binary/Image: os dados deste tipo são considerados um conjunto binário contínuo de bits.



Sessão FTP por linha de comando

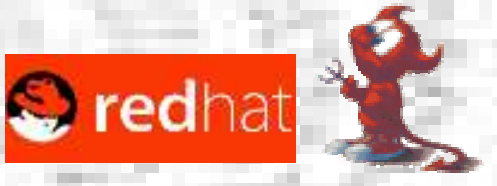
C:\WINDOWS>**ftp 192.168.7.9**
Conectado a 192.168.7.9.
220 localhost.localdomain FTP server (Version wu-2.6.2-8) ready.
Usuario (192.168.7.9:(none)): antunes
331 Password required for antunes.
Senha:
230 User antunes logged in. Access restrictions apply.
....
....

Comandos de usuários

- Vários comandos de usuários estão disponíveis no FTP, de maneira similar aos comandos do shell de usuário: *ls, cd, mkdir, pwd,* dentre outros
- O que realmente acontece é que os comandos dos usuários são traduzidos para os comandos do cliente FTP (como: RETR, STOR, CWD, LIST);

Acesso de forma autenticada ou anônima

Quando um usuário que possui uma conta no servidor realiza o processo de login (inicia a sessão) via FTP com o seu usuário e senha, o servidor provê o acesso ao seu respectivo diretório *home* e todos os seus arquivos; o usuário pode utilizar o *ls* para verificar os mesmos.



Acesso de forma autenticada ou anônima (cont.)

Entretanto, o FTP anônimo provê uma maneira em que um usuário possa realizar o processo de conexão ao servidor sem uma conta. Este realizará o processo *login* com o usuário *anonymous* ou *ftp* e como senha qualquer string de texto (normalmente o e-mail do usuário)

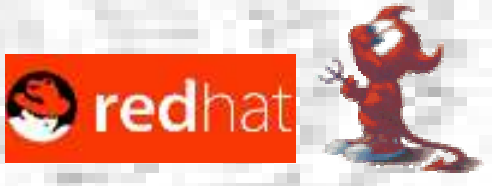
Acesso de forma autenticada ou anônima

Há diferenças fundamentais entre uma conta de um usuário regular e um usuário ftp anônimo.

O FTP anônimo é um *chroot "jail"* por definição, significando para aquele usuário que /var/ftp aparenta ser o raiz do servidor, ou seja, /. Nada além de /var/ftp está acessível ou visível.

Sessão FTP anônimo

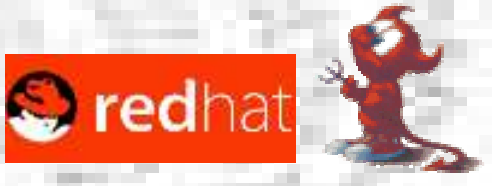
```
C:\WINDOWS>ftp 192.168.7.9
Conectado a 192.168.7.9.
220 localhost.localdomain FTP server (Version wu-2.6.2-8) ready.
Usuario (192.168.7.9:(none)): anonymous
331 Guest login ok, send your complete e-mail address as
    password.
Senha:
230-Teste com o arquivo /welcome.msg para o ftpd via o ftpaccess
230-
230-Alexssandro C. Antunes
230-21/06/2004
230-
230 Guest login ok, access restrictions apply.
```



wu-ftpd

O servidor de FTP utilizado para apresentar os conceitos do protocolo de transferência de arquivos é o wu-ftpd (wu-ftpd-2.6.2-8.src.rpm).

Há outros servidores de FTP, tal como o ProFTPD. Maiores informações sobre o ProFTPD podem ser obtidas em http://www.proftpd.org



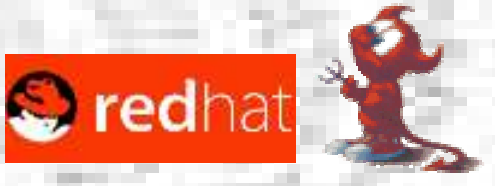
wu-ftpd

O wu-ftpd (http://www.wu-ftpd.org/) possui características que incluem o registro (log) de transferências, de comandos, comprenssão e arquivamento, classificação de usuários por tipo e localização, dentre outras funcionalidades.

anonftp

O servidor de FTP anônimo utilizado é o anonftp (anonftp-4.0-12.src.rpm); este servidor é somente de leitura, i.e., *read-only*, e permite que qualquer um realize o download de arquivos.

O FTP anônimo é uma maneira popular de tornar público determinados arquivos via internet



Configurando o servidor de ftp

- O serviço de FTP envolve um considerável número de arquivos de configuração. A maioria destes se encontra no diretório /etc e alguns em /var/ftp/etc.
- O primeiro item a ser configurado ou verificado é a porta e o serviço de FTP; normalmente localizado em /etc/services

Configurando o servidor de ftp

(cont)

- Após verificar ou incluir esta linha no arquivo *services*, deve-se verificar o arquivo de informações referente ao processo que irá servir o serviço de transferência de arquivos (FTP).

- Este arquivo, chamado wu-ftpd, está localizado no diretório /etc/xinetd.d.

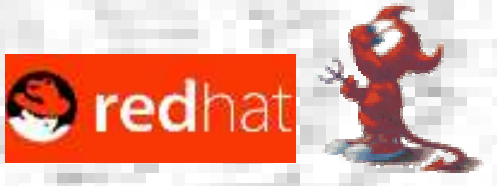
Conteúdo do arquivo

```
service ftp
{
        socket_type             = stream
        wait                    = no
        user                    = root
        server                  = /usr/sbin/in.ftpd
        server_args             = -l -a
        log_on_success          += DURATION
        nice                    = 10
        disable                 = no
}
```

Arquivos do /etc

- /etc/ftpaccess: o arquivo de configuração ftpaccess pode definir regras para controlar o acesso, informações, logs, permissões;

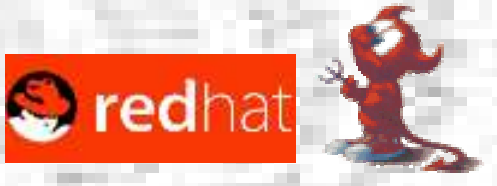
- /etc/ftpusers: lista de usuários que não devem possuir acesso ao serviço de FTP;



Arquivos do /etc (cont)

- /etc/ftphosts: utilizado para permitir ou negar acesso de certas contas de várias máquinas;

- /etc/ftpconversions: define as possíveis conversões a serem realizadas nos arquivos.



O arquivo /etc/ftpaccess

O arquivo ftpaccess é usado para configurar as operações do *daemon* de FTP

O arquivo /etc/ftpaccess

message <path> {<when> {<class> ...}}

Define um arquivo **<path>** que o daemon FTP irá mostrar ao usuário no momento em que este efetuar o login ou quando o mesmo mudar o diretório de trabalho.

O parâmetro **<when>** pode ser LOGIN ou CWD=<dir>. Se <when> for CWD=<dir>, <dir> especifica o diretório que irá disparar a notificação/mensagem ao usuário.

O parâmetro opcional **<classe>** permite que possa ser apresentada apenas para membros de uma classe em particular. Mais do que uma classe pode ser especificada.

Controlando Acesso /etc/ftpaccess

class

- Formato: class <classname> <typelist> <addrglob>

  <classname> - Nome da Classe

  <typelist>

  anonymous

  guest

  real

  <addrglob> - Enderecos permitidos

- Exemplo: ***class anonclass anonymous ****

  class localclass real 192.168.0.*

Controlando Acesso /etc/ftpaccess

- deny - Nega o serviço a certos hosts

  Formato: deny <addrglob> <message_file>

  Exemplo: **deny www.sun.com /etc/negado**

- limit - Limita a quantidade de conexões simultâneas em um dado período.

  Formato: limit <class> <n> <time> <message_file>

  Exemplo:

limit anonclass 10 MoTuWeTh,Fr0000-1700 /etc/message.muitos

Controlando Acesso /etc/ftpaccess

- loginfail - número de tentativas de login com falha.
  - Formato: loginfails <n>
  - Exemplo: loginfails 5

Controlando Mensagens

- **banner - Mensagem mostrada logo após a conexão ao servidor.**

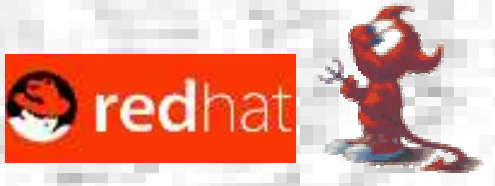
  Formato: banner <path>

  Exemplo: **banner /etc/ftpmsg**

- **email - Endereço do administrador do site.**

  Formato: email <address>

  Exemplo: **email ftp@curso.br**



Controlando Mensagens

- **message - Indica mensagens mostradas ao usuário quando loga ou muda de diretório.**
  - Formato: message <path> <quando> [<class>]

    <path> - Caminho do arquivo com a mensagem

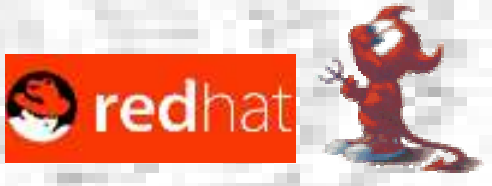
    <quando> - Situação para exibição do arquivo

    LOGIN

    CWD=<dir>
  - **Exemplo: message /welcome.msg LOGIN**

Controlando Mensagens

- **Flags Especiais**
  - **%T – Hora local**
  - **%C – Diretório atual**
  - **%E – Endereço de email do administrador**
  - **%R – Nome da máquina cliente**
  - **%L – Nome do servidor**
  - **%U – Nome do usuário fornecido no login**
  - **%M – Núm. máximo de usuários permitido**
  - **%N – Núm. atual de usuários conectados**

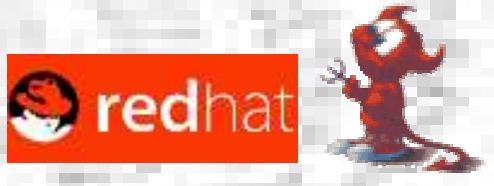


Controlando Mensagens

- **readme - Especifica as condições dentro das quais clientes são notificados de alterações em certos arquivos do diretório corrente.**

  Formato: readme <path> <quando> [<class>]

  Exemplo: **readme README* login**



Controlando Logs

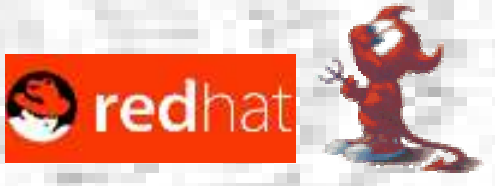
- **log commands - Armazena todas as ações de certos usuários do Servidor.**
  - Formato: log commands <typelist>

    <typelist>

    anonymous

    real

    guest
  - Exemplo: **log commands anonymous, guest**



Controlando Logs

- **log transfers - Armazena informações apenas sobre transferências de arquivos**

  Formato: log transfers <typelist> <direcao>

  <typelist> - mesmo de log commands

  <direcao>

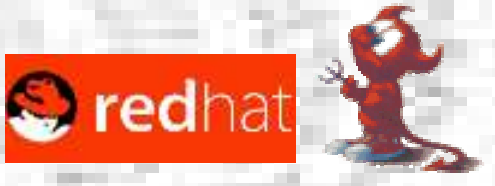
  inbound

  outbound

- Exemplo: **log transfers anonymous inboud**
  - Os logs são colocados em /var/log/

O arquivo /etc/ftphosts

- Controla o acesso ao servidor FTP
- Permite ou nega que determinados usuários conectem-se a partir de determinadas máquinas.
- Formato: allow <usuario> <endereco>
- deny <usuario> <endereco>
- Exemplo: *allow aluno 192.168.0.2*



A árvore de diretórios /var/ftp

- /etc/ftp/bin: este diretório contém comandos como o ls dentre outros executáveis necessários. O comando ls deve estar presente para gerar uma listagem do conteúdo de diretórios;

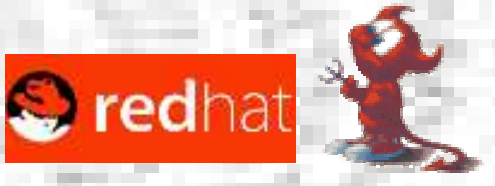
- /var/ftp/etc/passwd, /var/ftp/etc/group: são cópias dos arquivos /etc/passwd e /etc/group com o propósito de exibir, através do comando ls, os nomes dos proprietários dos arquivos em vez dos uid.

A árvore de diretórios /var/ftp

(cont)

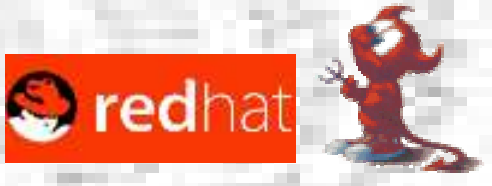
- /var/ftp/pub: visível aos usuários anônimos como /pub; local onde os arquivos para download estão disponíveis;

- /var/ftp/lib: neste diretório estão contidas as bibliotecas que serão utilizadas pelos programas localizados em /var/ftp/bin.



Parâmetros utilizados pelo *daemon*

Parâmetro	Descrição
-l	Cada sessão FTP é registrada no syslog
-T <timeout>	Define o tempo máximo de inatividade permitido
-a	Habilita o uso do arquivo de configuração /etc/ftpaccess
-A	Desabilita o uso do arquivo de configuração /etc/ftpaccess
-L	Indica que os comandos enviados para o servidor ftpd serão registrados no syslog
-i	Indica que os arquivos recebidos pelo servidor ftpd serão registrados no xferlog (FTP server transfer logfile)
-o	Define que os arquivos transmitdos pelo servidor ftpd serão registrados no xferlog
-	Utilizado para executar o ftpd em primeiro plano, ou seja, em foreground
-S	Utilizado para executar o ftpd em segundo plano, ou seja, em background




Fim
redhat