*Red Hat Enterprise Linux 3*

# Guia de Administração do Sistema

**Red Hat Enterprise Linux 3: Guia de Administração do Sistema**




Red Hat, Inc.

1801 Varsity Drive Raleigh NC 27606-2072 USA Telefone: +1 919 754 3700 Telefone: 888 733 4281 Fax: +1 919 754 3701 PO Box 13588 Research Triangle Park NC 27709 USA

rhel-sag(PT_BR)-3-Print-RHI (2003-07-25T17:10)



O número do código de segurança GPG em security@redhat.com é:

CA 20 86 86 2B D6 9D FC 65 F6 EC C4 21 91 80 CD DB 42 A6 0E

# Índice

# Introdução

Bem-vindo ao *Guia de Administração do Sistema do Red Hat Enterprise Linux*. Caro usuário, Devido a incontingências no processo de construção deste manual, alguns trechos são apresentados no idioma Inglês. Desculpe-nos por qualquer inconveniência que isto possa lhe causar.

O *Guia de Administração do Sistema do Red Hat Enterprise Linux* contém informações sobre a personalização do seu sistema Red Hat Enterprise Linux para atender às suas necessidades. Se você está à procura de um guia passo-a-passo para configurar e personalizar seu sistema, este é o manual certo. Este manual aborda diversos tópicos intermediários, como os seguintes:

- Configurando uma placa de interface de rede (network interface card, NIC)
- Executando uma Instalação Kickstart
- Configurando as partilhas do Samba
- Administrando seu software com RPM
- Determinando as informações sobre seu sistema
- Atualizando (upgrade) seu kernel

Este manual é dividido nas seguintes categorias principais:

- Referências Relacionadas à Instalação
- Referências Relacionadas à Rede
- Configuração do Sistema
- Administração de Pacotes

Este guia assume que você tem um conhecimento básico de seu sistema Red Hat Enterprise Linux. Se você precisa de ajuda para instalar o Red Hat Enterprise Linux, consulte o *Guia de Instalação do Red Hat Enterprise Linux*. Para informações mais gerais sobre a administração de sistemas, consulte o *Introdução à Administração de Sistemas Red Hat Enterprise Linux*. Se precisar de documentação mais avançada, como uma visão geral de sistemas de arquivo, consulte o *Guia de Referência do Red Hat Enterprise Linux*. Para informações sobre segurança, consulte o *Guia de Segurança do Red Hat Enterprise Linux*.

As versões HTML, PDF e RPM dos manuais estão disponíveis no CD de Documentação do Red Hat Enterprise Linux e online: http://www.redhat.com/docs/.

**Nota**

Apesar deste manual refletir as informações mais recentes possíveis, leia as *Notas da Versão do Red Hat Enterprise Linux* para acessar as informações que não estavam disponíveis antes da finalização de nossa documentação. Elas podem ser encontradas no CD 1 do Red Hat Enterprise Linux e online: http://www.redhat.com/docs/.

## 1. Alterações deste Manual

A versão anterior deste manual era chamada *Red Hat Linux Customization Guide* (não traduzida para o Português). Foi renomeado como *Guia de Administração do Sistema do Red Hat Enterprise Linux* para melhor refletir os tópicos abordados, assim como para definir claramente seu papel no conjunto de documentação da Red Hat.

Também foi expandido para incluir novas funcionalidades do Red Hat Enterprise Linux 3 e tópicos pedidos por nossos leitores. As mudanças mais significativas deste manual incluem:

Capítulo 7

Este capítulo explica como usar o devlabel.

Capítulo 8

Este capítulo explica como usar listas de controle de acesso para arquivos e diretórios.

Capítulo 9

Este capítulo foi atualizado para incluir as novas diretivas do kickstart.

Capítulo 10

Este capítulo foi atualizado para incluir as novas opções da **Configurador do Kickstart**.

Capítulo 14

Este capítulo novo explica como executar uma instalação PXE.

Capítulo 15

Este capítulo novo explica como criar um ambiente sem disco.

Capítulo 24

Este capítulo foi atualizado para o Samba 3.0 e agora explica como montar as partilhas do Samba.

Capítulo 32

Este capítulo novo explica a **Ferramenta de Configuração do Teclado**.

Capítulo 33

Este capítulo novo explica a **Ferramenta de Configuração do Mouse**.

Capítulo 34

Este capítulo novo explica a **Ferramenta de Configuração do X**.

Capítulo 38

Este capítulo foi atualizado para explicar as novas funcionalidades da **Visualizador de Registro**.

Capítulo 39

Este capítulo foi atualizado para explicar os novos pacotes do kernel e como atualizá-lo nas arquiteturas além da x86.

Capítulo 43

Este capítulo novo explica como usar o perfilador de sistema OProfile.

## 2. Convenções de Documentos

Ao ler este manual, determinadas palavras estão representadas com fontes, tipos, tamanhos e pesos diferentes. Este destaque é sistemático; palavras diferentes são representadas no mesmo estilo para indicar sua inclusão em uma categoria específica. Os tipos de palavras representadas desta maneira incluem as seguintes:

`comando`

Os comandos do Linux (e comandos de outros sistemas operacionais, quando usados) são representados desta maneira. Este estilo indica que você pode digitar a palavra ou frase na linha de comandos e pressionar [Enter] para invocar um comando. Às vezes o comando contém palavras que serão exibidas em um estilo diferente por si só (como nomes de arquivos). Nestes casos, estas são consideradas parte do comando, e então a frase inteira será exibida como um comando. Por exemplo:

Use o comando `cat testfile` para visualizar o conteúdo de um arquivo chamado `testfile`, no diretório de trabalho atual.

`nome do arquivo`

Nomes de arquivos, diretórios, localidades de arquivos e nomes de pacotes RPM são representados desta maneira. Este estilo indica que existe um determinado arquivo ou diretório com aquele nome no seu sistema. Exemplos:

O arquivo `.bashrc` do seu diretório 'home' contém definições da janela de comandos tipo bash e apelidos para seu uso pessoal.

O arquivo `/etc/fstab` contém informações sobre os dispositivos e sistemas de arquivo diferentes do sistema.

Instale o RPM `webalizer` se você quiser usar um programa de análise do arquivo de registro do servidor Web.

**aplicação**

Este estilo indica que o programa é uma aplicação direcionada ao usuário final (ao contrário do software do sistema). Por exemplo:

Use o **Mozilla** para navegar na Web.

[tecla]

Uma tecla do teclado é exibida neste estilo. Por exemplo:

Para usar a tecla complementar [Tab], digite um caracter e então pressione a tecla [Tab]. Seu terminal exibe uma lista dos arquivos contidos no diretório que começam com esta letra.

[tecla]-[combinação]

Uma combinação de sequência de teclas é representada desta maneira. Por exemplo:

A combinação de teclas [Ctrl]-[Alt]-[Espaço] termina sua sessão gráfica, retornando à tela ou ao console da autenticação gráfica.

**texto exibido em uma interface GUI (gráfica)**

Um título, palavra ou frase na tela ou janela da interface GUI é exibida neste estilo. O texto exibido neste estilo é usado na identificação de uma tela GUI específica ou um elemento de uma tela GUI (como o texto associado a uma caixa de verificação ou campo). Exemplo:

Selecione a caixa de verificação **Solicitar Senha** se você deseja que seu protetor de tela solicite uma senha antes de ser desbloqueado.

**nível superior de um menu em uma tela ou janela GUI**

Uma palavra neste estilo indica que a palavra está no nível superior de um menu suspenso (pull-down menu). Se você clicar na palavra na tela GUI, o resto do menu deverá aparecer. Por exemplo:

Abaixo de **Arquivo** em um terminal do GNOME, você verá a opção **Nova Aba**, que permite a você abrir diversos prompts de comando na mesma janela.

Se você precisar digitar uma sequência de comandos a partir de um menu GUI, eles são exibidos como o exemplo a seguir:

Vá para **Botão do Menu Principal** (no Painel) => **Programação => Emacs** para iniciar o editor de texto **Emacs**.

**botão em uma tela ou janela GUI**

Este estilo indica que o texto pode ser encontrado em um botão clicável de uma tela GUI. Por exemplo:

Clique no botão **Voltar** para retornar à última página web que você visitou.

`output do computador`

Texto neste estilo indica o texto exibido em uma janela de comandos, como mensagens de erro e respostas a comandos. Por exemplo:

O comando `ls` exibe o conteúdo de um diretório:

```
Desktop                about.html       logs          paulwesterberg.png
Mail                   backupfiles      mail          reports
```

O output exibido em resposta ao comando (neste caso, o conteúdo do diretório) é apresentado neste estilo.

`prompt`

Um prompt (ou janela de comandos), uma forma computacional de dizer que o computador está pronto para você inserir algo (input), será exibido desta maneira. Exemplos:

```
$
#
[stephen@maturin stephen]$
leopard login:
```

**`input do usuário`**

O texto que o usuário precisa digitar, na linha de comandos ou em uma caixa de texto em uma tela GUI, é apresentado neste estilo. No exemplo a seguir, **`text`** é exibido neste estilo:

Para inicializar seu sistema no programa de instalação em modo texto, você deve digitar o comando **`text`** no prompt `boot:`.

*`substituível`*

Texto usado para exemplos que devem ser subtituídos com dados providos pelo usuário são apresentados neste estilo. No exemplo a seguir, *<version-number>* é exibido neste estilo:

O diretório da fonte do kernel é `/usr/src/`*<version-number>*`/`, onde *<version-number>* é a versão do kernel instalado neste sistema.

Adicionalmente, nós utilizamos diversas estratégias diferentes para chamar sua atenção a determinadas partes da informação. De acordo com o quão crucial as informações são para seu sistema, elas são apresentadas como uma nota (lembrete), dica, importante, atenção ou um aviso. Por exemplo:

**Nota**

Lembre-se que o Linux é sensível a maiúsculas e minúsculas. Em outras palavras, uma rosa não é uma ROSA nem uma rOsA.


**Dica**

O diretório `/usr/share/doc/` contém documentação adicional para os pacotes instalados em seu sistema.


**Importante**

Se você modificar o arquivo de configuração do DHCP, as alterações não tomarão efeito até que você reinicie o daemon do DHCP.


**Atenção**

Não execute tarefas de rotina como root — use uma conta de usuário comum, a não ser que você precise usar a conta root para tarefas de administração do sistema.


**Aviso**

Cuidado para remover somente as partições necessárias do Red Hat Enterprise Linux. Remover outras partições pode resultar na perda de dados ou num ambiente de sistema corrompido.

## 3. Mais por vir

O *Guia de Administração do Sistema do Red Hat Enterprise Linux* é parte do compromisso crescente da Red Hat em oferecer suporte útil e oportuno para usuários do Red Hat Enterprise Linux. De acordo com o lançamento de novas ferramentas e aplicações, este manual será expandido para incluí-las.

### 3.1. Envie-nos Seu Retorno

Se você encontrar um erro de digitação no *Guia de Administração do Sistema do Red Hat Enterprise Linux* ou se pensar numa maneira de melhorar este manual, nos adoraríamos saber! Por favor submeta um relatório no Bugzilla (http://bugzilla.redhat.com/bugzilla/) sobre o componente `rhel-sag`.

Certifique-se de mencionar o identificador deste manual:

```
rhel-sag(PT_BR)-3-Print-RHI (2003-07-25T17:10)
```

Ao fazê-lo, nós saberemos exatamente qual versão do guia você possui.

Se você tem alguma sugestão para melhorar a documentação, tente ser o mais específico possível. Se encontrou um erro, por favor inclua o número da seção e alguns trechos do texto próximo ao erro para que possamos encontrá-lo facilmente.

## 4. Registre-se para obter Suporte

Se você possui uma edição do Red Hat Enterprise Linux 3, por favor lembre de registrar-se para obter os benefícios a que tem direito como cliente da Red Hat.

Você poderá usufruir de qualquer um ou de todos os benefícios a seguir, dependendo do produto que adquiriu:

- Suporte da Red Hat — Obtenha ajuda da equipe de suporte da Red Hat, Inc. nas questões de instalação.
- Red Hat Network — Atualize seus pacotes facilmente e receba avisos de segurança personalizados para o seu sistema. Visite http://rhn.redhat.com para mais detalhes.
- *Under the Brim: A E-Newsletter da Red Hat* — Receba mensalmente as últimas notícias e informações sobre produtos diretamente da Red Hat.

Para registrar-se, visite http://www.redhat.com/apps/activate/. Você encontrará o número de identificação do seu produto em um cartão preto, vermelho e branco dentro da caixa do Red Hat Enterprise Linux.

Para ler mais sobre o suporte técnico do Red Hat Enterprise Linux, consulte o apêndice *Obtendo Suporte Técnico* no *Manual de instalação do Red Hat Enterprise Linux;*.

Boa sorte e obrigado por escolher o Red Hat Enterprise Linux!

*Equipe de Documentação da Red Hat*

# I. Sistemas de Arquivo

*Sistema de arquivo* refere-se aos arquivos e diretórios armazenados em um computador. Um sistema de arquivo pode ter formatos diferentes chamados *tipos de sistema de arquivo*. Estes formatos determinam de que maneira as informações são armazenadas como arquivos e diretórios. Alguns tipos de sistema de arquivo armazenam cópias redundantes dos dados, enquanto outros tipos tornam mais rápido o acesso ao disco rígido. Esta parte aborda os tipos de sistema de arquivo ext3, swap, RAID e LVM. Também fala sobre o `parted`, um utilitário usado para administrar partições; e `devlabel`, um utilitário para o usuário criar nomes de dispositivos e acessar as listas de controle (ACLs) para personalizar as permissões de arquivo.

## Índice

redhat

# Capítulo 1.

# O Sistema de Arquivo ext3

O sistema de arquivo default é o *ext3* journaling.

## 1.1. Características do ext3

O sistema de arquivo ext3 é essencialmente uma versão melhorada do sistema de arquivo ext2. Estas melhorias oferecem as seguintes vantagens:

Disponibilidade

Após uma queda de energia ou queda do sistema inesperada (também chamada de *desligamento impróprio do sistema*), cada sistema de arquivo ext2 montado na máquina deve ter sua consistência verificada pelo programa `e2fsck`. Este processo leva tempo e pode demorar significativamente o tempo de inicialização, especialmente com volumes grandes contendo um grande número de arquivos. Durante este período, quaisquer dados dos volumes estão indisponíveis.

O journaling provido pelo sistema de arquivo ext3 significa que este tipo de verificação não é mais necessário após um desligamento impróprio do sistema. Os únicos momentos em que ocorrem verificações de consistência usando o ext3 são em raros casos de falha de hardware, como falhas no disco rígido. O tempo para recuperar um sistema de arquivo ext3 após um desligamento impróprio do sistema não depende do tamanho do sistema de arquivo ou do número de arquivos, mas sim do tamanho do *journal* usado para manter a consistência. O journal de tamanho default leva aproximadamente um segundo para recuperar, dependendo da velocidade do hardware.

Integridade dos Dados

O sistema de arquivo ext3 oferece alta integridade dos dados no caso de um desligamento impróprio do sistema. Além disso, permite que você escolha o tipo e nível de proteção para seus dados. Por default, os volumes ext3 são configurados para manter um alto nível de consistência dos dados em relação ao estado do sistema de arquivo.

Velocidade

Apesar de gravar alguns dados mais de uma vez, o ext3 tem maior produtividade em relação ao ext2 na maioria dos casos, pois o journaling do ext3 otimiza a movimentação da cabeça do disco rígido. Você pode escolher dentre três modos de journaling para otimizar a velocidade, mas ao fazer isso diminui a integridade dos dados.

Transição Fácil

É fácil mudar do ext2 parta o ext3 e obter os benefícios de um sistema de arquivo robusto sem a reformatação. Consulte a Seção 1.3 para detalhes sobre a execução desta tarefa.

Se você executou uma nova instalação, o sistema de arquivo default atribuído às partições do sistema Linux é ext3. Se você atualizou de uma versão que usa partições ext2, o programa de instalação permite que você converta estas partições para ext3 sem a perda de dados. Consulte o apêndice intitulado *Atualizando Seu Sistema Atual* no *Guia de Instalação do Red Hat Enterprise Linux* para mais detalhes.

As seções a seguir trazem os passos para a criação e ajuste das partições ext3. Para partições ext2, pule as seções de particionamento e formatação abaixo e vá direto para a Seção 1.3.

## 1.2. Criando um Sistema de Arquivo ext3

Após a instalação, às vezes é necessário criar um novo sistema de arquivo ext3. Por exemplo: se você adicionar um novo drive de disco ao sistema, pode querer particionar o drive e usar o sistema de arquivo ext3.

Os passos para a criação de um sistema de arquivo ext3 são os seguintes:

1. Criar a partição usando `parted` ou `fdisk`.
2. Formatar a partição com o sistema de arquivo ext3 usando `mkfs`.
3. Nomear a partição usando `e2label`.
4. Criar o ponto de montagem.
5. Adicionar a partição a `/etc/fstab`.

Consulte o Capítulo 5 para informações sobre a execução destes passos.

## 1.3. Convertendo para um Sistema de Arquivo ext3

O programa `tune2fs` pode adicionar um journal em um sistema de arquivo ext2 existente sem alterar os dados já contidos na partição. Se o sistema de arquivo já está montado ao ser transicionado, o journal será visto como o arquivo `.journal` no diretório raiz do sistema de arquivo. Se o sistema de arquivo não está montado, o journal será escondido e não aparecerá de modo algum no sistema de arquivo.

Para converter um sistema de arquivo ext2 para ext3, autentique-se como root e digite:

```
/sbin/tune2fs -j /dev/hdbX
```

No comando acima, substitua /dev/*hdb* pelo nome do dispositivo e *X* pelo número da partição.

Após fazer isso, certifique-se de alterar o tipo de partição de ext2 para ext3 no `/etc/fstab`.

Se você está transicionando seu sistema de arquivo root, terá que usar uma imagem `initrd` (ou disco RAM) para inicializar a máquina. Para criá-la, execute o programa `mkinitrd`. Para informações sobre o uso do comando `mkinitrd`, digite `man mkinitrd`. Também certifique-se de que a configuração de seu GRUB ou LILO carregue o `initrd`.

Se você não conseguir executar esta alteração, o sistema ainda inicializará, mas o sistema de arquivo será montado como ext2 ao invés de ext3.

## 1.4. Revertendo para um Sistema de Arquivo ext2

Como o ext3 é relativamente novo, alguns utilitários de disco ainda não o suportam. Por exemplo: você pode precisar diminuir uma partição com o `resize2fs`, que ainda não suporta o ext3. Nesta situação talvez seja necessário reverter um sistema de arquivo para ext2.

Para reverter uma partição, você deve primeiramente desmontar a partição se autenticando como root e digitando:

```
umount /dev/hdbX
```

No comando acima, substitua /dev/*hdb* pelo nome do dispositivo e *X* pelo número da partição. Para o restante desta seção, os exemplos de comandos utilizarão o *hdb1* para estes valores.

Em seguida, mude o tipo do sistema de arquivo para ext2 digitando o seguinte comando como root:

```
/sbin/tune2fs -O ^has_journal /dev/hdb1
```

Verifique se há erros na partição, digitando o seguinte comando como root:

```
/sbin/e2fsck -y /dev/hdb1
```

Então, monte a partição novamente como sistema de arquivo ext2, digitando:

```
mount -t ext2 /dev/hdb1 /mount/point
```

No comando acima, substitua */mount/point* pelo ponto de montagem da partição.

Em seguida, remova o arquivo `.journal` no nível da raiz da partição, mudando para o diretório onde está montada e digitando:

```
rm -f .journal
```

Agora você tem uma partição ext2.

Se você alterar a partição para ext2 permanentemente, lembre-se de atualizar o arquivo `/etc/fstab`.

redhat

Capítulo 2.

# Espaço Virtual (swap space)

## 2.1. O que é Espaço Virtual?

O *Espaço Virtual* no Linux é usado quando a memória física (RAM) está ocupada. Se o sistema precisar de mais recursos de memória e a memória física estiver cheia, páginas inativas na memória são movidas para o espaço virtual. Enquanto o espaço virtual pode ajudar uma máquina com pequena quantidade de RAM, não deve ser considerado uma substituição de mais RAM. O espaço virtual está localizado nos discos rígidos, que têm um tempo de acesso mais lento do que a memória física.

O espaço virtual pode ser uma partição virtual (swap) dedicada (recomendado), um arquivo virtual ou uma combinação de partições e arquivos virtuais.

O tamanho de seu espaço virtual deve ser igual ao dobro da memória RAM de seu computador ou 32 MB, o que for maior. Mas não deve ser maior que 2048 MB (ou 2 GB).

## 2.2. Adicionando Espaço Virtual

Às vezes é necessário adicioanar mais espaço virtual após a instalação. Por exemplo: você pode aumentar a quantidade de RAM do seu sistema de 64 MB para 128 MB, mas há somente 128 MB de espaço virtual. Pode ser vantajoso aumentar a quantidade de espaço virtual para 256 MB se você executa operações ou aplicações que requerem muita memória.

Você tem duas opções: adicionar uma partição virtual ou um arquivo virtual. É recomendado adicionar uma partição virtual, mas isto pode ser difícil se você não tiver espaço livre disponivel.

Para adicionar uma partição virtual (assumindo que `/dev/hdb2` é a partição virtual que você quer adicionar):

1. O disco rígido não pode estar em uso (partições não podem ser montadas e o espaço virtual não pode ser ativado). A tabela de partições não deve ser modificada enquanto for usada porque o kernel pode não reconhecer as alterações corretamente. Os dados poderiam ser sobrescritos ao gravar na partição errada, pois a tabela de partições e as partições montadas não coincidem. A maneira mais fácil de fazer isso é inicializar seu sistema no modo de recuperação (rescue mode). Consulte o Capítulo 11 para obter instruções sobre a inicialização no modo de recuperação. Quando você for questionado para montar o sistema de arquivo, selecione **Pular**.

   Alternativamente, se o disco não contém nenhuma partição em uso, você pode desmontar (unmount) as partições e desligar todo o espaço virtual do disco rígido com o comando `swapoff`.

2. Crie a partição virtual (swap) usando o `parted`:

   - Como root, digite o seguinte em uma janela de comandos: `parted /dev/`*`hdb`*, onde /dev/*`hdb`* é o nome do dispositivo para o disco rígido com espaço livre.
   - No prompt `(parted)`, digite **`print`** para visualizar as partições existentes e a quantidade de espaço livre. Os valores de início e fim estão em megabytes. Determine o quanto de espaço livre há no disco rígido e o quanto você quer designar para uma nova partição virtual.
   - No prompt `(parted)`, digite **`mkpartfs`** ***`part-type`*** **`linux-swap`** ***`start end`***, onde *`part-type`* é primária, extendida ou lógica, *`start`* é o ponto de início da partição, e *`end`* é o ponto final da partição.


**Aviso**

As alterações têm efeito imediato; cuidado ao digitar.

- Saia do prompt `parted` digitando **`quit`**.

3. Agora que você criou uma partição virtual, use o comando `mkswap` para configurar esta partição. Digite o seguinte em uma janela de comandos, como root:
   ```
   mkswap /dev/hdb2
   ```
4. Para ativar a partição virtual imediatamente, digite o seguinte comando:
   ```
   swapon /dev/hdb2
   ```
5. Para ativá-la no momento da inicialização da máquina, edite `/etc/fstab` para incluir:
   ```
   /dev/hdb2               swap                    swap    defaults        0 0
   ```
   Na próxima vez em que o sistema for reiniciado, a partição virtual será ativada.
6. Após adicionar e ativar a nova partição virtual, verifique se ela está habilitada visualizando o output do comando `cat /proc/swaps` ou `free`.

Para adicionar um arquivo virtual:

1. Determinar o tamanho do novo arquivo virtual em megabytes e multiplicar por 1024 para determinar o tamanho do bloco. Por exemplo: o tamanho do bloco de um arquivo virtual de 64 MB é 65536.
2. Em uma janela de comandos, como root, digite o seguinte comando com `count` sendo igual ao tamanho do bloco desejado:
   ```
   dd if=/dev/zero of=/swapfile bs=1024 count=65536
   ```
3. Configure o arquivo virtual com o comando:
   ```
   mkswap /swapfile
   ```
4. Para habilitar o arquivo virtual imediatamente, mas não automaticamente no momento da inicialização:
   ```
   swapon /swapfile
   ```
5. Para ativá-la no momento da inicialização da máquina, edite `/etc/fstab` para incluir:
   ```
   /swapfile               swap                    swap    defaults        0 0
   ```
   Na próxima vez que o sistema for iniciado, habilitará o novo arquivo virtual.
6. Após adicionar e ativar o novo arquivo virtual, verifique se ele está ativado visualizando o output do comando `cat /proc/swaps` ou `free`.

## 2.3. Removendo Espaço Virtual

Para remover uma partição virtual:

1. O disco rígido não pode estar em uso (partições não podem ser montadas e o espaço virtual não pode ser ativado). A maneira mais fácil de fazer isso é inicializar seu sistema no modo de recuperação (rescue mode). Consulte Capítulo 11 para obter instruções sobre a inicialização no modo de recuperação. Quando você for questionado para montar o sistema de arquivo, selecione **Pular**.

   Alternativamente, se o disco não contém nenhuma partição em uso, você pode desmontar (unmount) as partições e desligar todo o espaço virtual do disco rígido com o comando `swapoff`.
2. Em uma jenla de comandos, execute o segunte comando como root para certificar-se de que a partição virtual está desabilitada (onde `/dev/hdb2` é a partição virtual):

```
swapoff /dev/hdb2
```

3. Remova sua entrada de `/etc/fstab`.
4. Remova a partição usando o `parted`:
   - Em uma janela de comandos digite, como root, o comando `parted /dev/`*`hdb`*, onde `/dev/`*`hdb`* é o nome do dispositivo do disco rígido que contém a partição virtual a ser removida.
   - No prompt `(parted)`, digite **`print`** para visualizar as partições existentes e determinar o número menor da partição virtual que você deseja apagar.
   - No prompt `(parted)`, digite **`rm`** ***`MINOR`***, onde *`MINOR`* é o menor número da partição que você deseja remover.

     
     **Aviso**

     As alterações têm efeito imediato, portanto você deve digitar o menor número corretamente.
   - Digite **`quit`** para sair do `parted`.

Para remover um arquivo virtual:

1. Em uma janela de comandos, execute o seguinte comando como root para desabilitar o arquivo virtual (onde `/swapfile` é o arquivo virtual):
   ```
   swapoff /swapfile
   ```
2. Remova sua entrada de `/etc/fstab`.
3. Remova o arquivo real:
   ```
   rm /swapfile
   ```

## 2.4. Movendo Espaço Virtual

Para mover espaço virtual entre duas localidades, siga os passos para remover o espaço virtual e então siga os passos para adicionar espaço virtual.

redhat

Capítulo 3.

# Conjunto Redundante de Discos Independentes (RAID - Redundant Array of Independent Disks)

## 3.1. O que é RAID?

A idéia básica por trás do RAID é combinar diversos discos pequenos e de custo baixo em um conjunto, para atingir objetivos de desempenho ou redundância inatingíveis com um disco grande e de custo alto. Este conjunto de discos aparece para o computador como uma única unidade ou disco de armazenamento lógico.

O RAID é um método no qual as informações são espalahadas por diversos discos, usando técnicas como o *striping de disco* (RAID nível 0), o *mirroring de disco* (RAID nível 1) e o *striping de disco com paridade* (RAID nível 5) para atingir redundância, menor latência e/ou aumentar largura de banda para acessar ou gravar em discos, e maximizar a habilidade de recuperação de quebras de disco rígido.

O conceito fundamental do RAID é que os dados podem ser distribuídos ao longo de cada disco do conjunto de maneira consistente. Para fazer isso, primeiramente os dados precisam ser quebrados em *pedaços* de tamanho consistente (geralmente de 32 K ou 64 K, apesar de poder usar tamanhos diferentes). Cada pedaço é então gravado em um disco rígido no RAID, conforme o nível do RAID usado. Quando os dados tiverem que ser acessados, o processo é revertido, dando a impressão de que os discos múltiplos são um disco grande.

## 3.2. Quem Deve Usar o RAID?

Todas as pessoas que precisam armazenar grandes quantidades de dados à mão (tal como um administrador de sistemas) se beneficiarão ao usar a tecnologia RAID. As principais razões para usar o RAID incluem:

- Aumenta a velocidade
- Aumenta a capacidade de armazenamento usando um único disco virtual
- Impacto reduzido de uma falha de disco

## 3.3. Hardware RAID versus Software RAID

Estas são as duas abordagens possíveis do RAID: Hardware RAID e Software RAID.

### 3.3.1. Hardware RAID

O sistema baseado no hardware administra o sub-sistema RAID independentemente da máquina e apresenta apenas um disco por conjunto RAID à máquina.

Um exemplo de dispositivo de Hardware RAID é aquele que se conecta a um controlador SCSI e apresenta os conjuntos RAID como um único disco SCSI. Um sistema de RAID externo move toda a "inteligência" de tratamento do RAID para um controlador alocado no sub-sistema do disco externo. O sub-sistema inteiro é conectado à máquina através de um controlador SCSI normal e aparece para a máquiina como um único disco.

Os controladores RAID também vêm na forma de placas que *atuam* como um controlador SCSI para o sistema operacional, mas executam todas as comunicações do disco. Nestes casos, você conecta

(pluga) todos os discos ao controlador RAID, exatamente como faria com um controlador SCSI, mas deve adicioná-los à configuração do controlador RAID; o sistema operacional nunca saberá a diferença.

### 3.3.2. Software RAID

O software RAID implementa os diversos níveis do RAID no código do disco (dispositivo de bloco) do kernel. Oferece a solução mais barata possível, já que controaldores de disco caros ou chassis hot swap [1] não são necessários. O software RAID também funciona com discos IDE e discos SCSI mais baratos. Com as CPUs rápidas de hoje, o desempenho do software RAID pode ultrapassar o Hardware RAID.

O driver de MD no kernel do Linux é um exemplo de solução RAID copletamente independente de hardware. O desempenho de um conjunto baseado no software é dependente do desempenho e carga da CPU do servidor.

Para informações sobre a configuração do Software RAID durante a instalação, consulte o Capítulo 12.

Se você estiver interessado em aprender mais sobre o que o Software RAID tem a oferecer, aqui está uma rápida lista de suas características mais importantes:

- Processo threaded rebuild
- Configuração baseada no kernel
- Portabilidade dos conjuntos entre máquinas Linux sem reconstrução
- Reconstrução de conjuntos no background usando recursos ociosos do sistema
- Suporte ao disco hot-swappable (pode ser substituído sem desligar a máquina)
- Detecção automática da CPU para aproveitar determinadas otimizações da CPU

## 3.4. Níveis do RAID e Suporte Linear

O RAID suporta várias configurações, incluindo os níveis 0, 1, 4, 5 e linear. Estes tipos de RAID são definidos da seguinte maneira:

- *Nível 0* — O RAID nível 0, geralmente chamado de "striping," é uma técnica de mapeamento de dados "fatiados" (stripped) orientada para o desempenho. Isto significa que os dados sendo salvos no conjunto são quebrados em fatias e salvos ao longo dos discos membros do conjunto, permitindo o alto desempenho I/O a um custo essencialmente baixo, mas não provém redundância. A capacidade de armazenamento de um conjunto de nível 0 é igual à capacidade total dos discos membros de um Hardware RAID ou à capacidade total das partições pertencentes a um Software RAID.
- *Nível 1* — O RAID de nível 1, ou "mirroring," tem sido usado há mais tempo que qualquer outra forma de RAID. O nível 1 oferece redundância ao salvar os dados idênticos aos dados de cada disco membro do conjunto, deixando uma cópia "espelhada" (mirrored) em cada disco. O mirroring continua popular devido sua simplicidade e alto nível de disponibilidade dos dados. O nível 1 opera com dois ou mais discos que podem usar acesso paralelo para altas taxas de transferência de dados ao acessá-los, mas normalmente operam independentemente para oferecer altas taxas de transações

1. Um chassis hot-swap permite que você remova um disco rígido sem precisar desligar seu sistema.

I/O. O nível 1 oferece alta confiabilidade de dados e melhora o desempenho de aplicações intensamente usadas para acessar dados, porém a um custo relativamente alto. [2] A capacidade de armazenamento do conjunto de nível 1 é igual à capacidade de um dos discos espelhados em um Hardware RAID ou à capacidade de uma das partições espelhadas em um Software RAID.

- *Nível 4* — O nível 4 usa paridade [3] concentratada em um único disco para proteger os dados. É mais indicado para as transaçõesI/O do que para transferências de arquivos pesados. Como o disco de paridade dedicada representa um gargalo essencial, o nível 4 é raramente usado sem tecnologias associadas, como o write-back caching. Apesar do RAID de nível 4 ser uma opção de alguns esquemas de particionamento RAID, não é uma opção permitida em instalações RAID do Red Hat Enterprise Linux. [4] A capacidade de armazenamento do Hardware RAID de nível 4 é igual à capacidade dos discos membros, menos a capacidade de um disco membro. A capacidade de armazenamento do Software RAID de nível 4 é igual à capacidade da partições-membro, menos o tamanho de uma das partições se tiverem o mesmo tamanho.
- *Nível 5* — Este é o tipo mais comum de RAID. Através da distribuição de paridade ao longo de alguns ou de todos os drives dos discos membros do conjunto, o RAID de nível 5 elimina o gargalo de gravação inerente ao nível 4. O único gargalo de desempenho é o processo de cálculo da paridade. Com CPUs e Software RAID modernos, isso geralmente não representa um grande problema. Assim como no nível 4, o resultado é o desempenho assimétrico, com acesso substancial e alto desempenho de gravação. O nível 5 é geralmente usado com o write-back caching para reduzir a assimetria. A capacidade de armazenamento do Hardware RAID de nível 5 é igual à capacidade dos discos membros, menos a capacidade de um disco membro. A capacidade de armazenamento do Software RAID de nível 5 é igual à capacidade das partições-membro, menos o tamanho de uma das partições se elas tiverem o mesmo tamanho.
- *RAID Linear* — O RAID linear é um agrupamento simples dos discos para criar um disco virtual maior. No RAID linear, os pedaços são alocados sequencialmente de um disco membro, e vão para o próximo disco somente quando o primeiro estiver completamente cheio. Este agrupamento não provém nenhum benefício em termos de desempenho e é improvável que qualquer operação I/O seja separada entre discos membros. O RAID linear também não oferece redundância e, na prática, reduz a confiabilidade — se algum disco membro cair, o conjunto inteiro fica inutilizado. A capacidade é o total de todos os discos membros.

2. O RAID de nível 1 tem um custo alto porque você salva as mesmas informações em todos os discos do conjunto, o que gasta bastante espaço em disco. Por exemplo: se você tem o RAID de nível 1 configurado de modo que sua partição root (`/`) existe em dois discos rígidos de 40G, tem um total de 80G, mas só pode acessar 40G destes 80G. Os outros 40G atuam como um espelho dos primeiros 40G.
3. As informações de paridade são calculadas com base no conteúdo do resto dos discos membros do conjunto. Estas informações podem ser usadas para reconstruir os dados quando um disco do conjunto falhar. Os dados reconstruídos podem então ser usados para satisfazer os requisitos de I/O para o disco falho antes que seja substituído e para re-preencher o disco falho após ele ser substituído.
4. O RAID de nível 4 ocupa o mesmo espaço que o RAID de nível 5, mas o nível 5 tem mais vantagens. Por este motivo, o nível 4 não é suportado.

Capítulo 4.

# Gerenciador de Volume Lógico (LVM)

## 4.1. O que é LVM?

LVM é um método de alocar espaço do disco rígido em volumes lógicos que podem ser facilmente redimensionados, ao contrário das partições.

Com o LVM, o disco rígido ou conjunto de discos rígidos é alocado em um ou mais *volumes físicos*. Um volume físico não pode ultrapassar mais de um disco.

Os volumes físicos são combinados em *grupos de volume lógico*, com exceção da partição `/boot/`. A partição `/boot/` não pode estar em um grupo de volume lógico porque o gestor de início não pode acessá-lo. Se a partição root `/` estiver em um volume lógico, crie uma partição `/boot/` separada, que não seja parte de um grupo de volume.

Já que um volume físico não pode ultrapassar mais de um disco, crie um ou mais volumes físicos por disco para poder ultrapassar este limite.

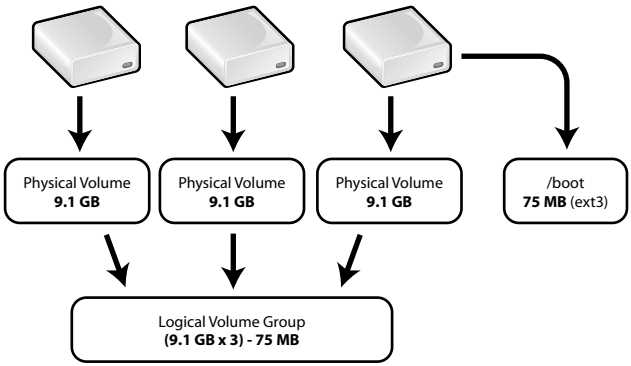


**Figura 4-1. Grupo de Volume Lógico**

O grupo de volume lógico é dividido em *volumes lógicos*, aos quais são atribuídos pontos de montagem, tais como `/home` e `/`, e tipos de sistemas de arquivo como o ext3. Quando as "partições" atingirem sua capacidade total, é possível adicionar espaço livre do grupo de volume lógico ao volume lógico para aumentar o tamanho da partição. Quando um novo disco rígido (hard drive) é adicionado ao sistema, pode ser adicionado ao grupo de volume lógico, e os volumes lógicos que são partições podem ser expandidos.

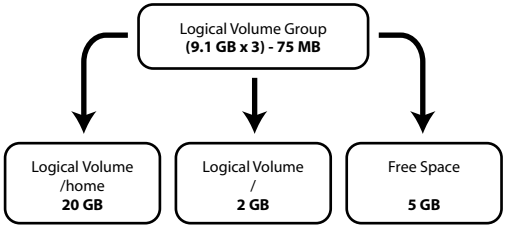


**Figura 4-2. Volumes Lógicos**

Por outro lado, se um sistema é particionado com o sistema de arquivo ext3, o disco rígido é dividido em partições de tamanhos definidos. Se uma partição ficar cheia, não é fácil expandir seu tamanho. Mesmo se a partição for movida para outro disco rígido, o espaço original em disco deve ser realocado como uma partição diferente ou não-usada.

O suporte ao LVM deve ser compilado no kernel. O kernel default da Red Hat é compilado com suporte ao LVM.

Para aprender a configurar o LVM durante o processo de instalação, consulte o Capítulo 13.

## 4.2. Recursos Adicionais

Use estes recursos para aprender mais sobre o LVM:

### 4.2.1. Documentação Instalada

- `rpm -qd lvm` — Este comando exibe toda a documentação disponibilizada pelo pacote `lvm`, inclusive as páginas man.

### 4.2.2. Sites Úteis

- http://www.sistina.com/products_lvm.htm — O site do LVM, que contém uma visão geral, link para as listas de discussão e outros.
- http://tldp.org/HOWTO/LVM-HOWTO/ — *LVM HOWTO* do Projeto de Documentação do Linux.

redhat.

Capítulo 5.

# Gerenciando Armazenamento de Disco

Muitos usuários precisam visualizar a tabela de partições exsitente, alterar o tamanho das partições, removê-las ou adicionar partições em espaço vazio ou discos rígidos adicionais. O utilitário `parted` permite que usuários executem estas tarefas. Este capítulo descreve como usar o `parted` para executar tarefas relacionadas a sistemas de arquivo.

Se você deseja visualizar o uso do espaço no disco do sistema ou monitorá-lo, consulte a Seção 42.3.

Você deve ter o pacote `parted` instalado para usar o utilitário `parted`. Para iniciar o `parted`, vá para uma janela de comandos, e como root, digite o comando `parted` */dev/hdb*, onde */dev/hdb* é o nome do dispositivo para o disco que você quer configurar. O prompt do `(parted)` aparecerá. Digite `help` para visualizar uma lista dos comandos disponíveis.

Se você deseja criar, remover ou redimensionar uma partição, o dispositivo não pode estar em uso (as partições não podem ser montadas e o espaço virtual não pode ser habilitado). A tabela de partição não deve sofrer modificações enquanto for usada, pois o kernel talvez não as reconheça. Os dados podem ser sobrescritos se gravados na partição errada, porque a tabela de partições e as partições montadas não coincidem. A maneira mais fácil de fazer isso é inicializar seu sistema no modo de recuperação. Consulte o Capítulo 11 para instruções sobre a inicialização no modo de recuperação. Quando for questionado para montar o sistema de arquivo, selecione **Pular**.

Alternativamente, se o disco não contém nenhuma partição em uso, você pode desmontá-las com o comando `umount` e desativar todo o espaço virtual (swap) do disco rígido como comando `swapoff`.

A Tabela 5-1 contém uma lista dos comandos `parted` comumente usados. A seção a seguir explica alguns deles em mais detalhes.

| Comando | Descrição |
|---|---|
| `check` *minor-num* | Executa uma verificação simples do sistema de arquivo |
| `cp` *de para* | Copia o sistema de arquivo de uma partição para outra; *de* e *para* são os menores números das partições |
| `help` | Exibe uma lista dos comandos disponíveis |
| `mklabel` *label* | Cria uma etiqueta de disco para a tabela de partições |
| `mkfs` *minor-num file-system-type* | Cria um sistema de arquivo do tipo *file-system-type* |
| `mkpart` *part-type fs-type start-mb end-mb* | Cria uma partição sem criar um novo sistema de arquivo |
| `mkpartfs` *part-type fs-type start-mb end-mb* | Cria uma partição e o sistema de arquivo especificado |
| `move` *minor-num start-mb end-mb* | Move a partição |
| `name` *minor-num name* | Nomeia a partição somente para etiquetas de disco do Mac e PC98 |
| `print` | Exibe a tabela de partições |

| Comando | Descrição |
|---|---|
| `quit` | Sai do `parted` |
| `rescue` *`start-mb end-mb`* | Recupera uma partição perdida de *`start-mb`* para *`end-mb`* |
| `resize` *`minor-num start-mb end-mb`* | Redimensiona a partição de *`start-mb`* para *`end-mb`* |
| `rm` *`minor-num`* | Remove a partição |
| `select` *`device`* | Seleciona um dispositivo diferente para configurar |
| `set` *`minor-num flag state`* | Define a bandeira de uma partição; o *`estado`* é ligado ou desligado |

**Tabela 5-1. comandos `parted`**

## 5.1. Visualizando a Tabela de Partições

Após iniciar o `parted`, digite o seguinte comando para visualizar a tabela de partições:

```
print
```

Aparece uma tabela semelhante à seguinte:

```
Disk geometry for /dev/hda: 0.000-9765.492 megabytes
Disk label type: msdos
Minor    Start       End     Type      Filesystem  Flags
1          0.031    101.975  primary   ext3        boot
2        101.975    611.850  primary   linux-swap
3        611.851    760.891  primary   ext3
4        760.891   9758.232  extended              lba
5        760.922   9758.232  logical   ext3
```

A primeira linha exibe o tamanho do disco; a segunda exibe o tipo da etiqueta de disco e o output restante exibe a tabela de partições. Nesta tabela, **Menor** é o número da partição. Por exemplo: a partição de número menor 1 corresponde a `/dev/hda1`. Os valores de **Início** e **Fim** são apresentados em megabytes. O **Tipo** é primária, extendida ou lógica. O campo **Sistema de Arquivo** traz o tipo de sistema de arquivo, que pode ser ext2, ext3, FAT, hfs, jfs, linux-swap, ntfs, reiserfs, hp-ufs, sun-ufs ou xfs. As coluna das **Bandeiras** lista as bandeiras definidas para a partição. As bandeiras disponíveis são boot, root, swap, hidden, raid, lvm ou lba.

**Dica**

Para selecionar um dispositivo diferente sem precisar reiniciar o `parted`, use o comando `select` seguido pelo nome do dispositivo, como `/dev/hdb`. Então, você poderá visualizar sua tabela de partições e configurá-la.

## 5.2. Criando uma Partição


**Atenção**

Não tente criar uma partição em um dispositivo que esteja em uso.

Antes de criar uma partição, inicialize no modo de recuperação (ou desmonte quaisquer partições do dispositivo e desabilite qualquer espaço virtual no dispositivo).

Inicie o `parted`, onde /dev/*hda* é o dispositivo no qual criar a partição:

```
parted /dev/hda
```

Visualize a tabela de partições corrente para determinar se há espaço livre suficiente:

```
print
```

Se não houver espaço livre suficiente, você pode redimensionar uma partição existente. Consulte a Seção 5.4 para detalhes.

### 5.2.1. Criando a partição

Na tabela de partições, determine os pontos inicial e final da nova partição e qual o seu tipo. Você pode ter apenas quatro partições primárias (sem nenhuma partição extendida) em um dispositivo. Se precisar de mais de quatro partições, você pode ter três partições primárias, uma partição extendida e diversas partições lógicas dentro da extendida. Para uma visão geral das partições de disco, consulte o apêndice *Uma Introdução às Partições de Disco* no *Guia de Instalação do Red Hat Enterprise Linux*.

Por exemplo: para criar uma partição primária com um sistema de arquivo ext3 de 1024 megabytes até 2048 megabytes de um disco rígido, digite o seguinte comando:

```
mkpart primary ext3 1024 2048
```


**Dica**

Se, ao invés disso, você usar o comando `mkpartfs`, o sistema de arquivo é criado após a criação da partição. Entretanto, o `parted` não suporta a criação de um sistema de arquivo ext3. Consequentemente, se você deseja criar um sistema de arquivo ext3, use `mkpart` e crie o sistema de arquivo com o comando `mkfs`, conforme descrito mais adiante. O `mkpartfs` funciona para o tipo de sistema de arquivo linux-swap.

As alterações têm efeito assim que você pressionar [Enter], portanto reveja o comando antes de executá-lo.

Após criar a partição, use o comando `print` para confirmar que ela está na tabela com o tipo de partição, tipo de sistema de arquivo e tamanho corretos. Também lembre-se do número menor da partição nova para que você possa etiquetá-lo. Você também deve visualizar o output de

```
cat /proc/partitions
```

para garantir que o kernel reconheça a partição nova.

### 5.2.2. Formatando a Partição

A partição ainda não tem um sistema de arquivo. Crie o sistema de arquivo:

```
/sbin/mkfs -t ext3 /dev/hdb3
```


**Atenção**

Formatar a partição destrói permanentemente quaisquer dados que existam nesta partição.

### 5.2.3. Etiquetando a Partição

Em seguida, dê uma etiqueta para a partição. Por exemplo: se a nova partição é `/dev/hda3` e você deseja etiquetá-la como `/work`:

```
e2label /dev/hda3 /work
```

Por default, o programa de instalação usa o ponto de montagem da partição como a etiqueta para garantir que esta seja única. Você pode usar qualquer etiqueta que quiser.

### 5.2.4. Criando o Ponto de Montagem

Como root, crie o ponto de montagem:

```
mkdir /work
```

### 5.2.5. Adicione a `/etc/fstab`

Como root, edite o arquivo `/etc/fstab` para incluir a nova partição. A nova linha deve se parecer com o seguinte:

```
LABEL=/work           /work                ext3    defaults        1 2
```

A primeira coluna deve conter `LABEL=` seguida pela etiqueta que você deu à partição. A segunda coluna deve conter o o ponto de montagem da nova partição, e a coluna seguinte deve ter o tipo de sistema de arquivo (ex.: ext3 ou swap). Se você precisa de mais informações sobre o formato, leia a página man do comando `man fstab`.

Se a quarta coluna é a palavra `defaults`, a partição é montada no momento da inicialização. Para montar a partição sem re-inicializar, digite o seguinte comando como root:

```
mount /work
```

## 5.3. Removendo uma Partição

 **Atenção**

Não tente remover uma partição de um dispositivo em uso.

Antes de remover a partição, inicialize no modo de recuperação (ou desmonte quaisquer partições do dispositivo e desabilite o espaço virtual do dispositivo).

Inicie `parted`, onde /dev/*hda* é o dispositivo do qual remover a partição:

```
parted /dev/hda
```

Visualize a tabela de partições corrente para determinar o número menor da partição a remover:

```
print
```

Remova a partição com o comando `rm`. Por exemplo: para remover a partição com número menor 3:

```
rm 3
```

As alterações têm efeito assim que você pressionar [Enter], portanto reveja o comando antes de invocá-lo.

Após remover a partição, use o comando `print` para confirmar a remoção da tabela de partições. Você também deve visualizar o output de

```
cat /proc/partitions
```

para garantir que o kernel saiba da remoção da partição.

O último passo é removê-la do arquivo `/etc/fstab`. Encontre a linha que declara a partição removida, e remova-a do arquivo.

## 5.4. Redimensionando uma Partição

 **Atenção**

Não tente redimensionar uma partição de um dispositivo em uso.

Antes de redimensionar uma partição, inicialize no modo de recuperação (ou desmonte quaisquer partições do dispositivo e desabilite o espaço virtual no dispositivo).

Inicie `parted`, onde /dev/*hda* é o dispositivo no qual redimensionar a partição:

```
parted /dev/hda
```

Visualize a tabela de partições corrente para determinar o número menor da partição a redimensionar, assim como os pontos inicial e final da partição:

```
print
```


**Atenção**

O espaço usado pela partição a redimensionar não pode ser maior do que o novo espaço.

Para redimensionar a partição, use o comando `resize` seguido pelo número menor da partição, o ponto inicial e o ponto final em megabytes. Por exemplo:

```
resize 3 1024 2048
```

Após redimensionar a partição, use o comando `print` para confirmar o redimensionamento correto da partição, seu tipo e seu tipo de sistema de arquivo.

Após reinicializar o sistema no modo normal, use o comando `df` para assegurar que a partição foi montada e que é reconhecida com o novo tamanho.

Capítulo 6.

# Implementando Quotas de Disco

O espaço em disco pode ser resrito através da implementação de quotas de disco, para que o administrador do sistema seja alertado antes de um usuário consumir muito espaço ou uma partição ficar cheia.

Quotas de disco podem ser configuradas para usuários individuais e também para grupos de usuários. Este tipo de flexibilidade possibilita dar a cada usuário uma pequena quota para armazenar arquivos "pessoais" (como relatórios e e-mails), enquanto permite que os projetos nos quais eles trabalham tenham quotas maiores (assumindo que os projetos sejam dados para seus grupos).

Além disso, as quotas podem ser definidas não só para controlar o número de blocos de disco consumidos, mas também para controlar o número de 'inodes'. Como os 'inodes' são usados para guardar informações relacionadas aos arquivos, isto permite controle sobre o número de arquivos que podem ser criados.

O RPM `quota` deve estar instalado para implementar quotas de disco. >>>>>> 1.1.2.4 Para mais informações sobre a instalação dos pacotes RPM, consulte a Parte III.

## 6.1. Configurando Quotas de Disco

Para implementar quotas de disco, use os seguintes passos:

1. Habilite quotas por sistema de arquivo modificando o `/etc/fstab`
2. Remonte o(s) sistema(s) de arquivo
3. Crie os arquivos de quota e gere a tabela de uso do disco
4. Atribua quotas

Cada um destes passos é abordado em detalhes nas seções seguintes.

### 6.1.1. Habilitando Quotas

Em um editor de texto, edite o arquivo `/etc/fstab` como root e adicione as opções `usrquota` e/ou `grpquota` aos sistemas de arquivo que requerem quotas.

```
LABEL=/           /              ext3    defaults        1 1
LABEL=/boot       /boot          ext3    defaults        1 2
none              /dev/pts       devpts  gid=5,mode=620  0 0
LABEL=/home       /home          ext3    defaults,usrquota,grpquota 1 2
none              /proc          proc    defaults        0 0
none              /dev/shm       tmpfs   defaults        0 0
/dev/hda2         swap           swap    defaults        0 0
/dev/cdrom        /mnt/cdrom     udf,iso9660 noauto,owner,kudzu,ro 0 0
/dev/fd0          /mnt/floppy    auto    noauto,owner,kudzu 0 0
```

Neste exemplo, o sistema de arquivo `/home` tem ambos, quotas de usuário e de grupo habilitadas.

### 6.1.2. Remontando os Sistemas de Arquivo

Após adicionar as opções `userquota` e `grpquota`, remonte cada sistema de arquivo cuja entrada `fstab` foi modificada. Se o sistema de arquivo não estiver em uso por nenhum processo, utilize o comando `umount` seguido pelo `mount` para remontar o sistema de arquivo. Se o sistema de arquivo estiver em uso, o método mais facil de remontá-lo é reinicializar o sistema.

### 6.1.3. Criando Arquivos de Quota

Após remontar cada sistema de arquivo habilitado com quotas, o sistema é capaz de trabalhar com quotas de disco. Entretanto, o próprio sistema de arquivo ainda não está pronto para suportar quotas. O próximo passo é executar o comando `quotacheck`.

O comando `quotacheck` examina os sistemas de arquivo habilitados com quotas e cria uma tabela do uso corrente do disco por sistema de arquivo. A tabela é então usada para atualizar o uso do disco na cópia do sistema operacional. Além disso, os arquivos de quota de disco do sistema de arquivo são atualizados.

Para criar os arquivos de quota (`aquota.user` e `aquota.group`) no sistema de arquivo, use a opção `-c` do comando `quotacheck`. Por exemplo: se as quotas de usuário e de grupo são habilitadas para a partição `/home`, crie os arquivos no diretório `/home`:

```
quotacheck -acug /home
```

A opção `-a` significa que todos os sistemas de arquivo não-NFS do `/etc/mtab` são verificados para saber se as quotas estão habilitadas. A opção `-c` especifica que os arquivos de quota devem ser criados para cada sistema de arquivo que tenha quotas habilitadas; a opção `-u` pede a verificação de quotas de usuário e a opção `-g` pede a verificação de quotas de grupo.

Se nenhuma das opções `-u` ou `-g` for especificada, somente o arquivo de quota do usuário é criado. Se especificar somente a opção `-g`, somente o arquivo de quota do grupo é criado.

Após criar os arquivos, execute o seguinte comando para gerar a tabela de uso corrente do disco por sistema de arquivo com quotas habilitadas:

```
quotacheck -avug
```

As opções usadas são as seguintes:

- `a` — Verifica todos os sistemas de arquivo montados localmente com quotas habilitadas
- `v` — Exibe informações verbais de status enquanto a verificação de quotas procede
- `u` — Verifica informações de quotas de disco do usuário
- `g` — Verifica informações de quotas de disco do grupo

Após o fim da execução do comando `quotacheck`, os arquivos de quota correspondentes às quotas habilitadas (de usuário e/ou de grupo) são preenchidos com dados de cada sistema de arquivo habilitado com quotas, como `/home`.

### 6.1.4. Atribuindo Quotas por Usuário

O último passo é atribuir as quotas de disco com o comando `edquota`.

Para configurar a quota de um usuário, execute o seguinte comando, como root:

```
edquota username
```

Execute este passo para cada usuário que precise de uma quota. Por exemplo: se uma quota é habilitada no `/etc/fstab` para a partição `/home` (`/dev/hda3`) e o comando `edquota testuser` é executado, o seguinte é exibido no editor configurado como o default do sistema:

```
Disk quotas for user testuser (uid 501):
  Filesystem          blocks       soft       hard     inodes     soft     hard
  /dev/hda3           440436          0          0      37418        0        0
```

**Nota**

O editor de texto definido pela variável de ambiente EDITOR é usada pelo `edquota`. Para mudar o editor, configure a variável EDITOR para a localização exata de seu editor predileto.

A primeira coluna é o nome do sistema de arquivo com uma quota habilitada. A segunda coluna mostra quantos blocos o usuário está usando no momento. As próximas duas colunas são usadas para definir limites de blocos suaves e rígidos para o usuário no sistema de arquivo. A coluna `inodes` mostra quantos 'inodes' o usuário está usando no momento. As duas últimas colunas são usadas para definir limites de 'inodes' suaves e rígidos para o usuário no sistema de arquivo.

Um limte rígido é a quantidade máxima absoluta de espaço em disco que um usuário ou grupo pode usar. Uma vez alcançado este limite, não é possível usar mais espaço em disco.

O limite suave determina a quantidade máxima de espaço em disco que pode ser usada. No entanto, ao contrário do limite rígido, o limite suave pode ser ultrapassado por um determinado período de tempo. Este período é conhecido como *período de carência*. O período de carência pode ser expressado em segundos, minutos, horas, dias, semanas ou meses.

Se algum dos valores é 0, este limite não está definido. Altere os limites desejados em um editor de texto. Por exemplo:

```
Disk quotas for user testuser (uid 501):
  Filesystem          blocks       soft       hard     inodes     soft     hard
  /dev/hda3           440436     500000     550000      37418        0        0
```

Para checar se a quota foi definida para o usuário, use o comando:

```
quota testuser
```

### 6.1.5. Atribuindo Quotas por Grupo

As quotas também podem ser atribuídas por grupo. Por exemplo: para configurar uma quota para o grupo `devel`, use o comando (o grupo deve existir antes de configurar a quota):

```
edquota -g devel
```

Este comando exibe a quota existente para o grupo no editor de texto:

```
Disk quotas for group devel (gid 505):
  Filesystem          blocks       soft       hard     inodes     soft     hard
  /dev/hda3           440400          0          0      37418        0        0
```

Modifique os limites, salve o arquivo e então configure a quota.

Para verificar se a quota do grupo foi definida, use o comando:

```
quota -g devel
```

### 6.1.6. Atribuindo Quotas por Sistema de Arquivo

Para atribuir quotas baseando-se em cada sistema de arquivo habilitado com quotas, use o comando:

```
edquota -t
```

Como os outros comandos `edquota`, este abre as quotas correntes do sistema de arquivo no editor de texto:

```
Grace period before enforcing soft limits for users:
Time units may be: days, hours, minutes, or seconds
  Filesystem             Block grace period     Inode grace period
  /dev/hda3                     7days                  7days
```

Altere o período de carência do bloco ou do 'inode', salve as alterações do arquivo e saia do editor de texto.

## 6.2. Administrando Quotas de Disco

Se as quotas forem implementadas, precisam de alguma manutenção — principalmente monitorá-las para verificar se são ultrapassadas e garantir que estejam exatas. Obviamente, se os usuários ultrapassarem suas quotas repetidamente ou alcançarem seus limites suaves constantemente, um administrador de sistemas tem poucas alternativas, dependendo do tipo de usuários e o quanto o espaço em disco impacta suas atividades. O administrador pode ajudar o usuário a determinar como usar menos espaço ou aumentar seu espaço em disco, se necessário.

### 6.2.1. Reportando em Quotas de Disco

Criar um relatório de uso do disco envolve rodar o utilitário `repquota`. Por exemplo: o comando `repquota /home` produz o seguinte output:

```
*** Report for user quotas on device /dev/hda3
Block grace time: 7days; Inode grace time: 7days
                        Block limits                File limits
User            used    soft    hard  grace    used  soft  hard  grace
----------------------------------------------------------------------
root      --      36       0       0              4     0     0
tfox      --     540       0       0            125     0     0
testuser  --  440400  500000  550000          37418     0     0
```

Para visualizar o relatório de uso do disco com todos os sistemas de arquivo habilitados com quotas, use o comando:

```
repquota -a
```

Apesar do relatório ser de fácil leitura, alguns pontos devem ser explicados. O `--` exibido após cada usuário é uma maneira rápida de determinar se os limites de blocos ou de 'inodes' foram ultrapassados. Se algum dos limites suaves é ultrapassado, aparece um `+` no lugar do `-` correspondente. O primeiro `-` representa o limite do bloco e o segundo representa o limite do 'inode'.

As colunas `grace` estão normalmente em branco. Se um limite suave foi ultrapassado, a coluna contém uma especificação de tempo igual à quantidade de tempo remanescente no período de carência. Se o período de carência expirou, aparece `none` em seu lugar.

### 6.2.2. Mantendo as Quotas Exatas

Sempre que um sistema de arquivo não é montado adequadamente (devido uma queda do sistema, por exemplo), é necessário rodar o `quotacheck`. No entanto, o `quotacheck` pode ser executado regularmente, mesmo que o sistema não tenha sofrido uma queda. Rodar o comando a seguir periodicamente mantém as quotas mais exatas (as opções usadas foram descritas na Seção 6.1.1):

```
quotacheck -avug
```

A maneira mais fácil de executá-lo periodicamente é usar o `cron`. Como root, use o comando `crontab -e` para agendar um `quotacheck` periódico ou inserir um script que execute o `quotacheck` em qualquer um dos diretórios a seguir (usando o intervalo que melhor atenda às suas necessidades):

- `/etc/cron.hourly`
- `/etc/cron.daily`
- `/etc/cron.weekly`
- `/etc/cron.monthly`

As estatísticas mais exatas das quotas podem ser obtidas quando o(s) sistema(s) de arquivo analisado(s) não estiverem em uso ativo. Portanto, a tarefa cron deve ser agendada para um período em que o(s) sistema(s) de arquivo seja(m) menos usado(s). Se este período varia para diferentes sistemas de arquivo com quotas, execute o `quotacheck` para cada sistema de arquivo em momentos diferentes com tarefas cron múltiplas.

Consulte o Capítulo 37 para mais informações sobre a configuração do `cron`.

### 6.2.3. Habilitando e Desabilitando

É possível desabilitar quotas sem definí-las para 0. Para desligar todas as quotas de usuário e de grupo, use o seguinte comando:

```
quotaoff -vaug
```

Se não especificar as opções `-u` ou `-g`, somente as quotas de usuário são desabilitadas. Se especificar só a opção `-g`, somente as quotas de grupo são desabilitadas.

Para habilitar as quotas novamente, use o comando `quotaon` com as mesmas opções.

Por exemplo: para habilitar as quotas de usuário e de grupo para todos os sistemas de arquivo:

```
quotaon -vaug
```

Para habilitar as quotas de um sistema de arquivo específico, como `/home`:

```
quotaon -vug /home
```

Se não especificar as opções `-u` ou `-g`, somente as quotas de usuário são habilitadas. Se especificar só a opção `-g`, somente as quotas de grupo são habilitadas.

## 6.3. Recursos Adicionais

Para mais informações sobre quotas de disco, consulte os seguintes recursos.

### 6.3.1. Documentação Instalada

- As páginas man do `quotacheck`, `edquota`, `repquota`, `quota`, `quotaon` e do `quotaoff`.

### 6.3.2. Livros Relacionados

- *Introdução à Administração de Sistemas Red Hat Enterprise Linux*; Red Hat, Inc. — Disponível no site http://www.redhat.com/docs/ e no CD de Documentação, este manual contém informações fundamentais sobre a administração do armazenamento (inclusive quotas de disco) para novos administradores de sistemas Red Hat Enterprise Linux.

redhat

Capítulo 7.

# Nomes de Dispositivos definidos pelo Usuário

O diretório `/dev/` contém arquivos virtuais que representam dispositivos. Cada arquivo virtual representa um dispositivo do sistema, tal como dispositivo de armazenamento, dispositivo USB e impressora. Estes arquivos virtuais são chamados *nomes de dispositivos*.

Nomes de dispositivos do tipo IDE começam com `hd`, e nomes de dispositivos do tipo SCSI começam com `sd`. O prefixo é seguido de uma letra, começando por a, representando a ordem dos discos. Por exemplo: `/dev/hda` é o primeiro disco rígido IDE, `/dev/hdb` é o segundo disco rígido IDE, `/dev/hdc` é o terceiro disco IDE e assim por diante.

Se o nome do dispositivo for seguido de um número, este representa o número da partição. Por exemplo: `/dev/hda1` representa a primeira partição do primeiro disco IDE.

Se um disco rígido for movido fisicamente para uma localidade diferente dentro da máquina, ou se for removido ou se falhar na inicialização, alguns nomes de dispositivos serão alterados, potencialmente deixando referências inválidas nos nomes dos dispositivos. Veja o exemplo da Figura 7-1 - se um sistema tem três discos rígidos SCSI e o segundo destes discos é removido, `/dev/sdc` torna-se `/dev/sdb`, fazendo com que quaisquer referências a `/dev/sdc` tornem-se inválidas. Referências a `/dev/sdb` também tornam-se inválidas desde que seja um disco diferente.

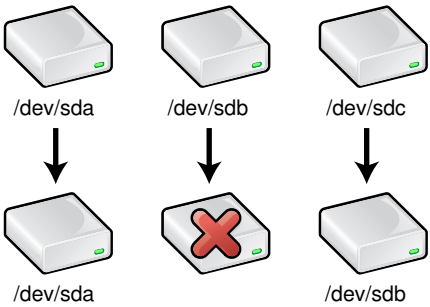


**Figura 7-1. Removendo um Disco Rígido**

Todo disco rígido tem um identificador úncio associado a ele, chamado *UUID*. Para resolver o problema da troca de nomes dos dispositivos, `devlabel` considera somente nomes de dispositivos definidos pelo usuário que estejam associados a estes UUIDs. Uma ligação (link) simbólica é criada entre o nome do dispositivo definido pelo usuário e o nome real do dispositivo. Se o nome real do dispositivo for alterado, a ligação simbólica é atualizada para apontar para o mesmo disco de acordo com seu UUID. Portanto, ambos dispositivos de armazenamento, IDE e SCSI, podem ser referenciados por seus nomes definidos pelo usuário.

O `devlabel` também considera dispositivos hotplug de montagem automática como discos rígidos, e dispositivos USB como placas de memória para câmeras digitais. Se configurado para ser montado automaticamente, após o dispositivo ser plugado, este será montado com o nome definido pelo usuário.

## 7.1. Configurando o `Devlabel`

Nomes de dispositivos definidos pelo usuário podem ser criados baseados no nome do dispositivo, no nome da partição, ou no UUID do disco.

Use a seguinte sintaxe para adicionar um nome de dispositivo de armazenamento definido pelo usuário. O dispositivo especificado pode ser o dispositivo inteiro ou uma única partição no dispositivo.

```
devlabel add -d <device> -s <symlink>
```

Por exemplo: para adicionar uma ligação simbólica `/dev/work` para representar a partição `/dev/hdb1`, use o seguinte comando:

```
devlabel add -d /dev/hdb1 -s /dev/work
```

Se o comando for bem-sucedido, o seguinte será exibido:

```
Created symlink /dev/work -> /dev/hdb1
Added /dev/work to /etc/sysconfig/devlabel
```

Para adicionar um nome de dispositivo baseado em um UUID, use a seguinte sintaxe:

```
devlabel add -u <uuid> -s <symlink>
```

Para usar o `devlabel` para recuperar o UUID de um dispositivo (ou para certificar-se de que ele tenha um), use o seguinte comando:

```
devlabel printid -d <device>
```

Os nomes das ligações simbólicas deme ser únicos. Se você tentar adicionar uma ligação simbólica com um nome que já existe, o arquivo de configuração não é modificado e o seguinte será exibido:

```
The file /dev/work already exists.
Failure. Could not create a symlink.
```

Para remover uma ligação simbólica da lista do `devlabel`, use o seguinte comando:

```
devlabel remove -s <symlink>
```

A entrada é removida do arquivo de configuração e a ligação simbólica é apagada.

Para determinar o status das ligações simbólicas `devlabel`, use o seguinte comando:

```
devlabel status
```

Retornará um output similar a:

```
lrwxrwxrwx    1 root            9 Apr 29 13:20 /dev/work -> /dev/hdb1
lrwxrwxrwx    1 root            9 Apr 29 13:41 /dev/tcf -> /dev/hda1
```

### 7.1.1. Dispositivos Hotplug

Um programa chamado *hotplug* executa ações quando um evento do sistema, tal como a adição ou remoção de hardware, ocorre enquanto o sistema está rodando. Por exemplo: se um disco rígido ou placa de leitura de mídia USB está conectada ao sistema, o `hotplug` notifica os usuários registrando uma mensagem no arquivo de registro do sistema (`/var/log/messages`) e carrega os módulos apropriados do kernel para que o dispositivo funcione.

Quando um dispositivo PCI, USB ou IEEE 1394 (também conhecido como FireWire) é plugado, os scripts do `hotplug` também reiniciam o `devlabel` para que a mídia removível de armazenamento receba um nome de dispositivo definido pelo usuário (como `/dev/usbcard`), e opcionalmente pode montar o dispositivo de armazenamento automaticamente.

Após inserir o cartão de leitura USB na porta USB do computador, submeta o seguinte comando como root (onde `/dev/sda1` é o nome do dispositivo para a placa de mídia e `/dev/usbcard` é o nome do dispositivo a utilizar, definido pelo usuário):

```
devlabel add -d /dev/sda1 -s /dev/usbcard --automount
```

Este comando adiciona uma entrada para o ponto de montagem de `/etc/sysconfig/devlabel` e cria uma ligação simbólica de `/dev/usbcard` para `/dev/sda1`. A opção `--automount` do `devlabel` especifica que o dispositivo deve ser automaticamente montado quando o `devlabel` reiniciar, se uma entrada para ele for localziada em `/etc/fstab` e se o dispositivo existir (se um dispositivo com o mesmo UUID for encontrado).

O `updfstab` é um programa que busca novos dispositivos nos canais IDE e SCSI e adiciona entradas para eles no `/etc/fstab`, caso elas já não existam. Também adiciona entradas para dispositivos USB desde que eles apareçam como dispositivos SCSI. Consulte a página man do `updfstab` para mais informações.

Quando um dispositivo USB é inserido, o `hotplug` roda o programa `updfstab`, que adiciona uma entrada no `/etc/fstab` para o dispositivo de armazenamento (como uma placa de mídia), se ela existir. (Se uma leitor de placa for inserido sem uma placa dentro, a entrada não será adicionada.) A linha adicionada contém o nome real do dispositivo (como `/dev/sda1`) e a opção `kudzu`. A opção `kudzu` diz ao **Kudzu** [1] que ele pode remover a linha se o dispositivo não existir. Já que a linha é requerida pelo `devlabel`, a opção `kudzu` deve ser removida para que a linha seja mantida no arquivo. Também altere o nome do dispositivo para o nome `devlabel` (tal como `/dev/usbcard`) e crie o ponto de montagem (como `/mnt/usbcard`).

Após modificar o arquivo, ele deve se parecer com o seguinte:

```
/dev/usbcard    /mnt/usbcard    auto    noauto,owner 0 0
```

Quando o `devlabel` é reiniciado, a mídia de armazenamento no dispositivo de leitura da placa USB é montada em `/mnt/usbcard` quando o dispositivo USB estiver plugado ao computador, por causa do `--automount`. O segredo é que quando o leitor da placa USB estiver plugado ao computador, a placa já deve estar no leitor. Caso contrário, o `devlabel` não poderá encontrar o dispositivo de armazenamento, e portanto não poderá montá-lo automaticamente.

Se o leitor da placa USB já estiver plugado sem uma placa, quando a placa for inserida, execute o comando `devlabel restart` como root para montar a placa de mídia.

## 7.2. Como Funciona

O comando `devlabel restart` é chamado pelo script `/etc/rc.sysinit` quando o sistema for inicializado e também pelos scripts apropriados no diretório `/etc/hotplug/`.

A opção `restart` do `devlabel` lê a lista de dispositivos no arquivo de configuração (`/etc/sysconfig/devlabel`) e segue a ligação simbólica para determinar se o dispositivo ainda existe em sua localização anterior, como `/dev/hdb1`, por exemplo. Se a ligação simbólica for inválida, será feita uma tentativa de encontrar uma nova localidade do disco baseada em seu UUID. Se for encontrado um disco com o mesmo UUID, a ligação simbólica é atualizada para apontar para a nova localidade do disco, o arquivo de configuração é atualizado com a nova localidade e uma mensagem similar à seguinte é exibida:

```
Device name incorrectly detected for symlink /dev/work!
The device /dev/hdb1 is now /dev/hdd1.
```

1. **Kudzu** é uma ferramenta de detecção de hardware executada no momento da inicialização da máquina para determinar qual hardware foi removido ao adicioando ao sistema.

```
The symlink /dev/work will now point to the new device name.
```

Se não for encontrado um disco com o UUID (se o disco foi removid, por exemplo), o seguinte será exibido:

```
The device /dev/hdb1 no longer seems to exist. Because of this, the
symlink /dev/work -> /dev/hdb1 will not be available. The reference
to this symlink in /etc/sysconfig/devlabel will be ignored.
```

A entrada do dispositivo não é removida do arquivo de confiuguração, é apenas ignorada para este caso.

## 7.3. Recursos Adicionais

Para mais informações relacionadas ao `devlabel`, consulte estas fontes.

### 7.3.1. Documentação Instalada

- `man devlabel` — A página man do `devlabel` aborda todas as opções e inclui uma breve descrição de como ele funciona.
- `man updfstab` — A página man do programa `updfstab`, que é chamado de `hotplug` quando um dispositivo USB é inserido.
- `man hotplug` — a página man do `hotplug`.

### 7.3.2. Websites Úteis

- http://www.dell.com/us/en/esg/topics/power_ps1q03-lerhaupt.htm — Em *Resolving Device Renaming Issues in Linux*, o desenvolvedor que escreveu o programa `devlabel` explica como ele funciona.
- http://www.lerhaupt.com/devlabel/devlabel.html — A página do desenvolvedor do projeto.

redhat.

Capítulo 8.

# Listas de Controle de Acesso

Arquivos e diretórios têm permissões para o proprietário do arquivo, para o grupo associado ao arquivo e para todos os outros usuários do sistema. Entretanto, estas definições de permissões têm limitações. Por exemplo: permissões diferentes não podem ser configuradas para usuários diferentes. Consequentemente, as *Listas de Controle de Acesso* (ACLs) foram introduzidas.

O kernel do Red Hat Enterprise Linux 3 oferece suporte à ACL para o sistema de arquivo ext3 e sistemas de arquivo exportados pelo NFS. As ACLs também são reconhecidas em sistemas de arquivo ext3 acessados através do Samba.

Juntamente ao suporte no kernel, é necessário ter o pacote `acl` para implementar as ACLs. Este contém os utilitários usados para adicionar, modificar, remover e recuperar informações da ACL.

Os comandos `cp` e `mv` copiam ou movem quaisquer ACLs associadas a arquivos e diretórios.

## 8.1. Montando Sistemas de Arquivo

Antes de usar ACLs para um arquivo ou diretório, sua partição deve ser montada com o suporte da ACL. Se for um sistema de arquivo ext3 local, pode ser montada com o seguinte comando:

```
mount -t ext3 -o acl <device-name> <partition>
```

Por exemplo:

```
mount -t ext3 -o acl /dev/hdb3 /work
```

Alternativamente, se a partição está listada no arquivo `/etc/fstab`, a entrada da partição pode incluir a opção `acl`:

```
LABEL=/work      /work       ext3    acl         1 2
```

Se um sistema de arquivo ext3 é acessado via Samba, e as ACLS foram habilitadas para tal, as ACLs são reconhecidas porque o Samba foi compilado com a opção `--with-acl-support`. Não são necessárias bandeiras especiais ao acessar ou montar uma partilha do Samba.

### 8.1.1. NFS

Por default, se o sistema de arquivo exportado por um servidor NFS suporta ACLs e o cliente NFS pode ler ACLs, estas são utilizadas pelo sistema cliente.

Para desabilitar ACLs nas partilhas NFS ao configurar o servidor, inclua a opção `no_acl` no arquivo `/etc/exports`. Para desabilitar ACLs nas partilhas NFS ao montá-las no cliente, monte-as com a opção `no_acl` através da linha de comando ou do arquivo `/etc/fstab`.

## 8.2. Definindo ACLs de Acesso

Há dois tipos de ACLs: *ACLs de acesso* e *ACLs default*. Uma ACL de acesso é a lista de controle de acesso a um arquivo ou diretório específico. Uma ACL default pode ser associada somente a um diretório; se um arquivo do diretório não tem uma ACL de acesso, usa as regras da ACL default do diretório. ACLs default são opcionais.

As ACLs podem ser configuradas:

1. Por usuário
2. Por grupo
3. Através da máscara de direitos efetivos (effective rights mask)
4. Para usuários fora do grupo de usuários do arquivo

O utilitário `setfacl` define ACLs para arquivos e diretórios. Use a opção `-m` para adicionar ou modificar a ACL de um arquivo ou diretório:

```
setfacl -m <rules> <files>
```

As regras (<*rules*>) deve estar no seguintes formatos. É possível especificar regras múltiplas no mesmo comando se forem separadas por vírgulas.

`u:`<*uid*>`:`<*perms*>

Defina a ACL de acesso para um usuário. Você pode especificar o nome ou ID do usuário. O usuário pode ser qualquer usuário válido do sistema.

`g:`<*gid*>`:`<*perms*>

Defina a ACL de acesso para um grupo. Você pode especificar o nome ou ID do grupo. O grupo pode ser qualquer grupo válido do sistema.

`m:`<*perms*>

Defina a máscara de direitos efetivos. A máscara é a união de todas as permissões do grupo proprietário e todas as entradas de usuário e grupo.

`o:`<*perms*>

Defina a ACL de acesso para usuários fora do grupo do arquivo.

Espaços em branco são ignorados. As permissões (<*perms*>) devem ser uma combinação dos caracteres `r`, `w` e `x` para ler (read), gravar (write) e executar (execute).

Se um arquivo ou diretório já tiver uma ACL e o comando `setfacl` é usado, as regras são adicionadas à ACL existente ou a regra existente é modificada.

Por exemplo: para dar permissões de leitura (read) e gravação (write) para o usuário tfox:

```
setfacl -m u:tfox:rw /project/somefile
```

Para remover todas as permissões de um usuário, de um grupo ou de outros, use a opção `-x` e não especifique nenhuma permissão:

```
setfacl -x <rules> <files>
```

Por exemplo: para remover todas as permissões do usuário com UID 500:

```
setfacl -x u:500 /project/somefile
```

## 8.3. Definindo ACLs Default

Para definir uma ACL default, adicione `d:` antes da regra e especifique um diretório ao invés de um nome de arquivo.

Por exemplo: para definir a ACL default do diretório `/share/` para leitua e gravação para usuários fora do grupo de usuários (uma ACL de acesso para um arquivo individual pode sobrescrevê-la):

```
setfacl -m d:o:rx /share
```

## 8.4. Recuperando ACLs

Para determinar as ACLs existentes de um arquivo ou diretório, use o comando `getfacl`:

```
getfacl <filename>
```

Este comando retorna um output similar ao seguinte:

```
# file: file
# owner: tfox
# group: tfox
user::rw-
user:smoore:r--
group::r--
mask::r--
other::r--
```

Se um diretório é especificado e tem uma ACL default, esta também é exibida, tal como:

```
# file: file
# owner: tfox
# group: tfox
user::rw-
user:smoore:r--
group::r--
mask::r--
other::r--
default:user::rwx
default:user:tfox:rwx
default:group::r-x
default:mask::rwx
default:other::r-x
```

## 8.5. Documentando Sistemas de Arquivo Com ACLs

**Atenção**

Os comandos `tar` e `dump` *não* fazem backup de ACLs.

O utilitário `star` é similar ao `tar`, pois pode ser usado para gerar a documentação de arquivos; entretanto, algumas de suas opções são diferentes. Consulte a Tabela 8-1 para uma lista das opções mais usadas. Para ver todas as opções disponíveis, consulte a página man do `star`. O pacote `star` é necessário para usar este utilitário.

| Opção | Descrição |
|---|---|
| Opção | Descrição |
| -c | Cria um arquivo de documentação. |
| -n | Não extrai os arquivos; use juntamente a -x para exibir o que a extração dos arquivos faz. |
| -r | Substitui arquivos na documentação. Os arquivos são gravados no fim do arquivo de documentação, substituindo todos os arquivos com a mesma localidade e nome. |
| -t | Exibe o conteúdo do arquivo de documentação. |
| -u | Atualiza o arquivo de documentação. Estes arquivos são gravados no fim da documentação, caso já não existam na documentação ou se os arquivos são mais novos que aqueles com o mesmo nome na documentação. Esta opção funciona somente se a documentação é um arquivo ou uma fita com blocos de tamanhos diferentes que pode ser acessada em qualquer ponto. |
| -x | Extrai arquivos da documentação. Se usado com -U e um arquivo da documentação for mais antigo que o correspondente no sistema de arquivo, o arquivo não é extraído. |
| -help | Exibe as opções mais importantes. |
| -xhelp | Exibe as opções menos importantes. |
| -/ | Não remova as barras iniciais dos nomes de arquivos ao extraí-los de uma documentação. Por default, elas são removidas quando os arquivos são extraídos. |
| -acl | Ao criar ou extrair, documentar ou armazenar todas as ACLs associadas a arquivos e diretórios. |

**Tabela 8-1. Opções de Linha de Comandos do `star`**

## 8.6. Compatibilidade com Sistemas mais Antigos

Se uma ACL foi definida em qualquer arquivo ou sistema de arquivo, o sistema de arquivo tem o atributo `ext_attr`. Este atributo pode ser visto usando o seguinte comando:

```
tune2fs -l <filesystem-device>
```

Um sistema de arquivo que adquiriu o atributo `ext_attr` pode ser montado com kernels mais antigos, mas aqueles kernels não reforçam nenhuma ACL que tenha sido definida.

As versões do utilitário `e2fsck` incluso nas versões 1.22 e mais recentes do pacote `e2fsprogs` (incluindo as versões no Red Hat Enterprise Linux 2.1 e 3) podem verificar um sistema de arquivo com o atributo `ext_attr`. Versões mais antigas recusam esta verificação.

## 8.7. Recursos Adicionais

Consulte os seguinte recursos para mais informações.

### 8.7.1. Documentação Instalada

- Página man do `acl` — Descrição das ACLs
- Página man do `getfacl` — Aborda como obter acesso de arquivo às listas de controle
- Página man do `setfacl` — Explica como definir o acesso de arquivo às listas de controle
- Página man do `star` — Explica mais sobre o utilitário `star` e suas várias opções

### 8.7.2. Sites Úteis

- http://acl.bestbits.at/ — site das ACLs
- http://www.fokus.gmd.de/research/cc/glone/employees/joerg.schilling/private/star.html — site do utilitário `star`

# II. Informações Relacionadas à Instalação

O *Guia de Instalação do Red Hat Enterprise Linux* aborda a instalação do Red Hat Enterprise Linux e a solução de alguns problemas básicos pós-instalação. No entanto, opções avançadas de instalação também são descritas neste manual. Esta parte oferece instruções para o modo de recuperação *kickstart* (uma técnica de instalação automatizada) do sistema (como inicializar seu sistema se não inicializar no nível de execução normal), como configurar o RAID durante a instalação, e como configurar o LVM durante a instalação. Use esta parte em conjunto com o *Guia de Instalação do Red Hat Enterprise Linux* para executar qualquer uma das tarefas avançadas de instalação.

## Índice

redhat.

# Capítulo 9.

# Instalações do Kickstart

## 9.1. O que são instalações do Kickstart?

Muitos administradores de sistemas preferem usar um método de instalação automatizado para instalar o Red Hat Enterprise Linux em suas máquinas. Para atender esta necessidade, a Red Hat criou o método de instalação do kickstart. Usando kickstart, um administrador pode criar um único arquivo contendo as respostas para todas as questões levantadas durante uma instalação típica.

Os arquivos kickstart podem ser guardados em um único sistema de servidor e lidos por computadores individuais durante a instalação. Este método de instalação pode suportar o uso de um único arquivo kickstart para instalar o Red Hat Enterprise Linux em diversas máquinas, tornando-o ideal para administradores de rede e de sistemas.

O kickstart oferece uma maneira para usuários automatizarem uma instalação do Red Hat Enterprise Linux.

## 9.2. Como Você Executa uma Instalação do Kickstart?

As instalações do kickstart podem ser executadas usando um CD-ROM e um disco rígido locais, ou através do NFS, FTP ou HTTP.

Para usar o kickstart, você deve:

1. Criar um arquivo kickstart.
2. Criar um disquete boot com o arquivo kickstart ou disponibilizar o arquivo kickstart na rede.
3. Disponibilizar a árvore de instalação.
4. Iniciar a instalação kickstart.

Este capítulo explica estes passos em detalhe.

## 9.3. Criando o Arquivo Kickstart

O arquivo kickstart é um arquivo texto simples contendo uma lista de itens, cada um identificado por uma palavra-chave. Você pode criá-lo editando uma cópia do arquivo `sample.ks` encontrado no diretório `RH-DOCS` do CD de Documentação do Red Hat Enterprise Linux, usando a aplicação **Configurador do Kickstart**, ou criando a partir do zero. O programa de instalação do Red Hat Enterprise Linux também cria uma amostra do arquivo kickstart baseado nas opções que você selecionou durante a instalação. É gravado no arquivo `/root/anaconda-ks.cfg`. Você pode editá-lo com qualquer editor ou processador de texto que salve arquivos no formato texto ASCII.

Primeiro, esteja ciente das questões seguintes ao criar seu arquivo kickstart:

- As seções devem ser especificadas *em ordem*. Os itens das seções não precisam estar em uma ordem específica a não ser que isto seja especificado. A ordem da seção é:
  - A seção comando — Consulte a Seção 9.4 para obter uma lista das opções do kickstart. Você deve incluir as opções requisitadas.
  - A seção `%packages` — Consulte a Seção 9.5 para detalhes.

  - As seções `%pre` e `%post` — Estas duas seções podem estar em qualquer ordem e não são requisitadas. Consulte a Seção 9.6 e a Seção 9.7 para detalhes.

- Os itens não requisitados podem ser omitidos.
- Omitir qualquer item requisitado fará com que o programa de instalação questione o usuário sobre o item específico, como aconteceria numa instalação típica. Assim que a resposta é dada, a instalação continuará sozinha (a não ser que encontre outro item faltando).
- As linhas começando com um jogo da velha (#) são tratadas como comentários e são ignoradas.
- Para *atualizações* do kickstart, são requisitados os seguintes itens:para
  - Idioma
  - Suporte ao Idioma
  - Método de instalação
  - Especificação do dispositivo (se este for necessário para executar a instalação)
  - Configuração do teclado
  - A palavra-chave `upgrade`
  - Configuração do gestor de início

  Se quaisquer outros itens forem especificados para a atualização, serão ignorados (note que isto inclui a seleção de pacotes).

## 9.4. Opções do Kickstart

As opções seguintes podem ser inseridas em um arquivo kickstart. Se você prefere usar uma interface gráfica para criar seu arquivo kickstart, pode usar a aplicação **Configurador do Kickstart**. Consulte o Capítulo 10 para mais detalhes.

**Nota**

Se a opção for seguida do sinal de igual (=), deve-se especificar um valor após este. Nos comandos de exemplo, as opções entre colchetes ([]) são argumentos opcionais do comando.

`autopart` (opcional)

Criar partições automaticamente — uma partição root (`/`) de 1 GB ou mais, uma partição swap e uma partição boot apropriada para a arquitetura. Um ou mais tamanhos das partições default podem ser redefinidos com a diretiva `part`.

`autostep` (opcional)

Similar ao `interactive`, exceto pelo fato de que vai para a próxima tela para você. É usado principalmente para a depuração.

`auth` ou `authconfig` (requisitado)

Configura as opções de autenticação para o sistema. É similar ao comando `authconfig`, que pode ser executado após a instalação. Por default, as senhas normalmente são criptografadas e não 'sombreadas' (shadowed).

`--enablemd5`

Usar criptografia md5 para senhas de usuário.

`--enablenis`

Ative o suporte ao NIS. Por defauilt, o `--enablenis` usa qualquer domínio que encontrar na rede. Um domínio quase sempre deve ser definido manualmente com a opção `--nisdomain=`.

`--nisdomain=`

Nome do domínio NIS para usar com serviços NIS.

`--nisserver=`

Servidor para usar com serviços NIS (transmite por default).

`--useshadow` ou `--enableshadow`

Usar senhas shadow.

`--enableldap`

Ativa o suporte ao LDAP no `/etc/nsswitch.conf`, permitindo a seu sistema recuperar as informações sobre os usuários (UIDs, diretórios home, shells, etc.) de um diretório LDAP. Para usar esta opção, você deve instalar o pacote `nss_ldap`. Você também deve especificar um servidor e uma base DN com o `--ldapserver=` e `--ldapbasedn=`.

`--enableldapauth`

Usa o LDAP como um método de autenticação. Isto habilita o módulo `pam_ldap` para autenticação e alteração de senhas, usando um diretório LDAP. Para usar esta opção, você deve ter o pacote `nss_ldap` instalado. Você também deve especificar um servidor e uma base DN com o `--ldapserver=` e `--ldapbasedn=`.

`--ldapserver=`

Se você especificou `--enableldap` ou `--enableldapauth`, use esta opção para especificar o nome do servidor LDAP a usar. Esta opção é definida no arquivo `/etc/ldap.conf`.

`--ldapbasedn=`

Se você especificou `--enableldap` ou `--enableldapauth`, use esta opção para especificar o DN (distinguished name) na árvore de seu diretório LDAP sob a qual as informações dos usuários são armazenadas. Esta opção é definida no arquivo `/etc/ldap.conf`.

`--enableldaptls`

Use as procuras TLS (Transport Layer Security). Esta opção permite que o LDAP envie nomes de usuários e senhas criptografados para um servidor LDAP antes da autenticação.

`--enablekrb5`

Use o Kerberos 5 para autenticar usuários. O Kerberos em si não sabe sobre diretórios home, UIDs ou shells. Portanto, se você habilitar o Kerberos, terá que assegurar que as contas de usuários são conhecidas por esta estação de trabalho, habilitando o LDAP, NIS ou Hesiod, ou então usando o comando `/usr/sbin/useradd` para tornar suas contas conhecidas por esta estação de trabalho. Se você usar esta opção, deve ter o pacote `pam_krb5` instalado.

`--krb5realm=`

O reino do Kerberos 5, ao qual sua estação de trabalho pertence.

`--krb5kdc=`

O KDC (ou KDCs) que servem pedidos para o reino. Se você tem KDCs múltiplos em seu reino, separe seus nomes por vírgulas (,).

`--krb5adminserver=`

O KDC em seu reino que também roda o kadmind. Este servidor lida com alteração de senhas e outros pedidos administrativos. O servidor deve rodar em um KDC mestre se você tiver mais de um KDC.

`--enablehesiod`

Habilite o suporte ao Hesiod para que procure por diretórios home, UIDs e shells dos usuários. Você pode encontrar mais informações sobre a configuração e uso do Hesiod em sua rede no `/usr/share/doc/glibc-2.x.x/README.hesiod`, incluso no pacote `glibc`. O Hesiod é uma extensão do DNS que usa os registros do DNS para armazenar informações sobre usuários, grupos e vários outros itens.

`--hesiodlhs`

A opção Hesiod LHS ("left-hand side"), configurada no `/etc/hesiod.conf`. Esta opção é usada pela biblioteca do Hesiod para determinar o nome para a procura DNS quando buscar informações; similar ao uso do LDAP sobre o DN de base.

`--hesiodrhs`

A opção Hesiod RHS ("right-hand side"), configurada no `/etc/hesiod.conf`. Esta opção é usada pela biblioteca do Hesiod para determinar o nome para a procura DNS quando buscar informações; similar ao uso do LDAP sobre o DN de base.

**Dica**

Para procurar por "jim" nas informações de usuário, a biblioteca do Hesiod procura por *jim.passwd<LHS><RHS>*, o que deve resultar em um registro TXT que se parece com o que sua senha se pareceria (`jim:*:501:501:Jungle Jim:/home/jim:/bin/bash`). Para grupos, a situação é idêntica, exceto que *jim.group<LHS><RHS>* será usado.

A procura de usuários e grupos por número é feita tornando "501.uid" um CNAME para "jim.senha", e "501.gid" um CNAME para "jim.grupo". Note que LHS e RHS não têm pontos [.] à frente deles quando a biblioteca determina o nome pelo qual procurar, portanto LHS e RHS geralmente começam por pontos.

`--enablesmbauth`

Habilita a autenticação de usuários em um servidor SMB (tipicamente, um servidor Samba ou Windows). O suporte da autenticação SMB não sabe sobre diretórios home, UIDs e shells de usuários. Portanto, se você habilitá-lo, deve tornar as contas de usuários conhecidas pela estação de trabalho, habilitando o LDAP, NIS ou Hesiod, ou então usando o comando `/usr/sbin/useradd` para tornar suas contas conhecidas pela estação de trabalho. Para usar esta opção, você deve ter o pacote `pam_smb` instalado.

`--smbservers=`

O nome do(s) servidor(es) para usar na autenticação SMB. Para especificar mais de um servidor, separe seus nomes por vírgulas.

`--smbworkgroup=`

O nome do grupo de trabalho para os servidores SMB.

`--enablecache`

Habilita o serviço `nscd`. Este serviço armazena em cache as informações sobre usuários, grupos e vários outros tipos de informação. O cache é especialmente útil se você optar por distribuir as informações dos usuários e grupos ao longo de sua rede usando NIS, LDAP ou hesiod.

`bootloader` (requisitado)

Especifica o gestor de início (LILO ou GRUB) e como este deve ser instalado. Esta opção é requisitada tanto para instalações quanto para atualizações. Nas atualizações, se `--useLilo` não é especificado e LILO é o gestor de início corrente, o gestor será alterado para GRUB. Para preservar o LILO nas atualizações, use `bootloader --upgrade`.

`--append=`

Especifica os parâmetros do kernel. Para especificar parâmetros múltiplos, separe-os por espaços. Por exemplo:

```
bootloader --location=mbr --append="hdd=ide-scsi ide=nodma"
```

`--driveorder`

Especifica qual é o primeiro disco na ordem de inicialização do BIOS. Por exemplo:

```
bootloader --driveorder=sda,hda
```

`--location=`

Especifica onde o registro de inicialização (boot) é gravado. Os valores válidos são os seguintes: `mbr` (o default), `partition` (instala o gestor de início no primeiro setor da partição contendo o kernel), ou `nenhum` (não instala o gestor de início).

`--password=`

Se usar o GRUB, esta define a senha do gestor de início GRUB para aquela indicada com esta opção. Deve ser usada para restringir o acesso à shell do GRUB, onde as opções arbitrárias do kernel podem ser passadas.

`--md5pass=`

Se usar o GRUB, esta é similar à `--password=`, exceto pela senha que já deve estar criptografada.

`--useLilo`

Usa o LILO como gestor de início, ao invés do GRUB.

`--linear`

Se usar o LILO, use a opção `linear`; esta é somente para compatibilidade reversa (linear agora é usada por default).

`--nolinear`

Se usar o LILO, use a opção `nolinear`. Linear é o default.

`--lba32`

Se usar o LILO, force o uso do modo lba32 ao invés da auto-detecção.

`--upgrade`

Atualize a configuração existente do gestor de início, preservando as entradas antigas. Esta opção está disponível somente para atualizações (upgrades).

`clearpart` (opcional)

Remove partições do sistema antes da criação de novas partições. Por default, nenhuma partição é removida.

**Nota**

Se o comando `clearpart` for usado, então o comando `--onpart` não pode ser usado em uma partição lógica.

`--all`

Apaga todas as partições do sistema.

`--drives=`

Especifica quais discos terão suas partições limpas. Por exemplo: o seguinte limpa as partições nos primeiros dois drives do controlador IDE primário.

```
clearpart --drives hda,hdb
```

`--initlabel`

Inicializa a etiqueta de disco para o defult de sua arquitetura (ex.: `msdos` para x86 e `gpt` para Itanium). É útil pois assim o programa de instalação não questiona se deve inicializar a etiqueta de disco caso instale em um disco rígido novo.

`--linux`

Apaga todas as partições Linux.

`--none` (default)

Não remove nenhuma partição.

`cmdline` (opcional)

Executa a instalação em um modo de comando de linha completamente não-interativo. Quaisquer prompts para interação interromperão a instalação. Este modo é útil para sistemas S/390 com o console x3270.

`device` (opcional)

Na maioria dos PCS, o programa de instalação irá auto-detectar as placas Ethernet e SCSI apropriadamente. Em sistemas mais antigos e em alguns PCs, no entanto, o kickstart precisa de uma dica para encontrar os dispositivos corretos. O comando `device`, que diz ao programa de instalação para instalar módulos extras, tem este formato:

`device <type> <moduleName> --opts=<options>`

*<type>*

Substitua por `scsi` ou `eth`

*<moduleName>*

Substitua pelo nome do módulo do kernel que deve ser instalado.

`--opts=`

As opções a serem passadas para o módulo do kernel. Note que opções múltiplas podem ser passadas se forem colocadas entre aspas. Por exemplo:
`--opts="aic152x=0x340 io=11"`

`driverdisk` (opcional)

Disquetes de driver podem ser usados durante instalações kickstart. Você precisa copiar o conteúdo do disquete de driver para o diretório root de uma partição do disco rígido do sistema. E então deve usar o comando `driverdisk` para dizer ao programa de instalação onde procurar o disco de driver.
`driverdisk <partition> [--type=<fstype>]`

Alternativamente, você pode especificar uma localidade na rede para o disquete de driver:
```
driverdisk --source=ftp://path/to/dd.img
driverdisk --source=http://path/to/dd.img
driverdisk --source=nfs:host:/path/to/img
```

*<partition>*

A partição contendo o disco de driver.

`--type=`

Tipo de sistema de arquivo (ex.: vfat ou ext2).

`firewall` (opcional)

Esta opção corresponde à tela de **Configuração do Firewall** no programa de instalação:
`firewall --enabled|--disabled [--trust=] <device> [--port=]`

`--enabled`

Rejeita conexões de entrada que não são em resposta a pedidos para fora, como respostas DNS ou pedidos DHCP. Se for necessário acesso aos serviços rodando nesta máquina, você pode optar por permitir serviços específicos através do firewall.

`--disabled`

Não configurar nenhuma regra do iptables.

`--trust=`

Listar um dispositivo aqui, como eth0, permite que todo o tráfego proveniente deste dispositivo passe pelo firewall. Para listar mais de um dispositivo, use `--trust eth0 --trust eth1`. NÃO use um formato separado por vírgulas, como `--trust eth0, eth1`.

*<incoming>*

Substitua por nenhum ou mais dos seguintes para permitir a passagem dos serviços especificados pelo firewall.

- `--ssh`
- `--telnet`

- `--smtp`
- `--http`
- `--ftp`

`--port=`

Você pode especificar que estas portas sejam permitidas pelo firewall usando o fortmato porta:protocolo. Por exemplo: para permitir o acesso ao IMAP através do firewall, especifique `imap:tcp`. Portas numéricas também pode ser especificadas explicitamente. Ex.: para permitir pacotes UDP através da porta 1234, especifique `1234:udp`. Para especificar diversas portas, separe-as por vírgulas.

`firstboot` (opcional)

Determine se o **Agente de Configuração** inicia na primeira vez que o sistema é inicializado. Se habilitado, o pacote `firstboot` deve ser instalado. Se não for especificada, esta opção é desabilitada por default.

`--enable`

O **Agente de Configuração** é iniciado na primeira vez que o sistema inicializar.

`--disable`

O **Agente de Configuração** não é iniciado na primeira vez que o sistema inicializar.

`--reconfig`

Habilite o **Agente de Configuração** para iniciar no momento da inicialização no modo de reconfiguração. Este modo habilita as opções de idioma, mouse, teclado, senha root, nível de segurança, fuso horário e configuração da rede, além das opções default.

`install` (opcional)

Diz para instalar um novo sistema ao invés de atualizar um sistema existente. Este é o modo default. Para a instalação, você deve especificar o tipo de instalação - `cdrom`, `harddrive`, `nfs` ou `url` (para instalações ftp ou http). O comando `install` e o comando do método de instalação devem estar em linhas separadas.

`cdrom`

Instalar pelo primeiro drive de CD-ROM do sistema.

`harddrive`

Instalar por uma árvore de instalação da Red Hat em um disco local, que deve ser vfat ou ext2.

- `--partition=`

  Partição pela qual instalar (ex.: sdb2).

- `--dir=`

  Diretório contendo o diretório `RedHat` da árvore de instalação.

Por exemplo:

```
harddrive --partition=hdb2 --dir=/tmp/install-tree
```

`nfs`

Instalar pelo servidor NFS especificado.

- `--server=`

  Servidor a partir do qual instalar (endereço ou IP da máquina).

- `--dir=`

  Diretório contendo o diretório `RedHat` da árvore de instalação.

Por exemplo:

```
nfs --server=nfsserver.example.com --dir=/tmp/install-tree
```

`url`

Instalar a partir de uma árvore de instalação em um servidor remoto via FTP ou HTTP.

Por exemplo:

```
url --url http://<server>/<dir>
```

ou:

```
url --url ftp://<username>:<password>@<server>/<dir>
```

`interactive` (opcional)

Usa as informações providas no arquivo kickstart durante a instalação, mas permite a revisão e modificação dos valores dados. Você verá cada tela do programa de instalação com os valores do arquivo kickstart. Aceite os valores clicando em **Próximo** ou altere-os e clique em **Próximo** para continuar. Veja também o `autostep`.

`keyboard` (requisitado)

Define o tipo de teclado do sistema. Aqui está a lista de teclados disponíveis nas máquinas i386, Itanium e Alpha:

```
be-latin1, bg, br-abnt2, cf, cz-lat2, cz-us-qwertz, de,
de-latin1, de-latin1-nodeadkeys, dk, dk-latin1, dvorak, es, et,
fi, fi-latin1, fr, fr-latin0, fr-latin1, fr-pc, fr_CH, fr_CH-latin1,
gr, hu, hu101, is-latin1, it, it-ibm, it2, jp106, la-latin1, mk-utf,
no, no-latin1, pl, pt-latin1, ro_win, ru, ru-cp1251, ru-ms, ru1, ru2,
ru_win, se-latin1, sg, sg-latin1, sk-qwerty, slovene, speakup,
speakup-lt, sv-latin1, sg, sg-latin1, sk-querty, slovene, trq, ua,
uk, us, us-acentos
```

O arquivo `/usr/lib/python2.2/site-packages/rhpl/keyboard_models.py` também contém esta lista e é parte do pacote `rhpl`.

`lang` (requisitado)

Define o idioma a ser usado na instalação. Por exemplo: para definir o idioma para Inglês, o arquivo kicckstart deve conter a seguinte linha:

```
lang en_US
```

O arquivo `/usr/share/redhat-config-language/locale-list` oferece uma lista de códigos de idiomas válidos na primeira coluna de cada linha e é parte do pacote `redhat-config-languages`.

`langsupport` (requisitado)

Define o(s) idioma(s) a instalar no sistema. Os mesmos códigos dos idiomas usados com o `lang` podem ser usados com `langsupport`.

Para instalar um idioma, especifique-o. Por exemplo: para instalar e usar o idioma Francês `fr_FR`:

```
langsupport fr_FR
```

`--default=`

Se especificar suporte para mais de um idioma, deve identificar um idioma default.

Por exemplo: para instalar Inglês e Francês no sistema e usar Inglês como o idioma default:

```
langsupport --default=en_US fr_FR
```

Se você usar `--default` com somente um idioma, todos os idiomas serão instalados com o idioma especificado definido como default.

`logvol` (opcional)

Crie um volume lógico para o LVM (Logical Volume Management) com a seguinte sintaxe:

```
logvol <mntpoint> --vgname=<name> --size=<size> --name=<name> <options>
```

As opções são as seguintes:

--noformat

Usa um volume lógico existente e não o formata.

--useexisting

Usa um volume lógico existente e o reformata.

Crie a partição primeiro, depois crie o grupo de volume lógico e então o volume lógico. Por exemplo:

```
part pv.01 --size 3000
volgroup myvg pv.01
logvol / --vgname=myvg --size=2000 --name=rootvol
```

`mouse` (requisitado)

Configura o mouse do sistema, nos modos GUI e texto. As opções são:

`--device=`

O dispositivo no qual está o mouse (como `--device=ttyS0`).

`--emulthree`

Se estiver presente, clicar os botões esquerdo e direto do mouse simultaneamente será reconhecido pelo Sistema X Window como o botão do meio. Esta opção deve ser usada se você tiver um mouse de dois botões.

Após as opções, o tipo do mouse deve ser especificado como um dos seguintes:

```
alpsps/2, ascii, asciips/2, atibm, generic, generic3, genericps/2,
generic3ps/2, genericwheelps/2, genericusb, generic3usb, genericwheelusb,
geniusnm, geniusnmps/2, geniusprops/2, geniusscrollps/2, geniusscrollps/2+,
thinking, thinkingps/2, logitech, logitechcc, logibm, logimman,
logimmanps/2, logimman+, logimman+ps/2, logimmusb, microsoft, msnew,
msintelli, msintellips/2, msintelliusb, msbm, mousesystems, mmseries,
mmhittab, sun, none
```

Esta lista também pode ser encontrada no arquivo `/usr/lib/python2.2/site-packages/rhpl/mouse.py`, que é parte do pacote `rhpl`.

Se o comando do mouse for submetido sem nenhum argumento, ou for omitido, o programa de instalação tentará auto-detectar o mouse. Este procedimento funciona para mouses modernos.

`network` (opcional)

Configura as informações de rede no sistema. Se a instalação kickstart não requer rede (ou seja, não é instalado através do NFS, HTTP ou FTP), a rede não é configurada no sistema. Se a instalação requer rede e as informações da rede não são providas no arquivo kickstart, o programa de instalação assume que a instalação deve ser feita pela eth0 através de um endereço IP dinâmico (BOOTP/DHCP), e configura o sistema instalado final para determinar seu endereço IP dinamicamente. A opção `network` configura as informações de rede para instalações kickstart através de uma rede assim como para o sistema instalado.

`--bootproto=`

Um destes: `dhcp`, `bootp` ou `static`.

Seu default para `dhcp`. `bootp` e `dhcp` são tratados da mesma maneira.

O método DHCP usa um sistema de servidor DHCP para obter sua configuração de rede. Como você pode supor, o método BOOTP é similar, requisitando um servidor BOOTP para prover a configuração de rede. Para direcionar um sistema a usar DHCP:

```
network --bootproto=dhcp
```

Para direcionar uma máquina a usar BOOTP para obter sua configuração de rede, use a seguinte linha no arquivo kickstart:

```
network --bootproto=bootp
```

O método estático requer que você indique todas as informações de rede necessárias no arquivo kickstart. Como o nome implica, as informações são estáticas e serão usadas durante e depois da instalação. A linha da rede estática é mais complexa, já que você deve incluir todas as informações de configuração da rede em uma linha. Você deve especificar o endereço IP, máscara de rede (netmask), porta de comunicação (gateway) e nome do servidor. Por exemplo: (\ indica que está tudo em uma linha):

```
network --bootproto=static --ip=10.0.2.15 --netmask=255.255.255.0 \
--gateway=10.0.2.254 --nameserver=10.0.2.1
```

Se você usar o método estático, esteja ciente das duas restrições a seguir:

- Todas as informações de configuração de rede devem ser especificadas em *uma* linha; você não pode separar linhas com uma barra invertida. Por exemplo:
- Você pode especificar apenas um nome de servidor (nameserver) aqui. No entanto, você pode fazer com que a seção `%post` do arquivo kickstart (descrita na Seção 9.7) adicione mais nomes de servidores, se necessário:

`--device=`

Usado para selecionar um dispositivo Ethernet específico para a instalação. Note que o uso do `--device=` não será efetivo a não ser que o arquivo kickstart seja um arquivo local (como `ks=floppy`), já que o programa de instalação configurará a rede para encontrar o arquivo kickstart.Exemplo:

```
network --bootproto=dhcp --device=eth0
```

`--ip=`

Endereço IP para a máquina a ser instalada.

`--gateway=`

Porta de comunicação default como um endereço IP.

`--nameserver=`

Nome do servidor primário, como um endereço IP.

`--nodns`

Não configurar nenhum servidor DNS.

`--netmask=`

Máscara de rede para o sistema instalado.

`--hostname=`

Nome da máquina para o sistema instalado.

`part` ou `partition` (requisitado para instalações; ignorado para atualizações)

Cria uma partição no sistema.

Se houver mais de uma instalação do Red Hat Enterprise Linux em diferentes partições do sistema, o programa de instalação questiona qual instalação o usuário pretende atualizar.

**Atenção**

Todas as partições criadas serão formatadas como parte do processo de instalação, a não ser que `--noformat` and `--onpart` seja usados.

*<mntpoint>*

O *<mntpoint>* é onde a partição será montada e deve ter uma das seguintes formas:

- `/`*<path>*

  Por exemplo: `/`, `/usr`, `/home`

- `swap`

  A partição será usada como espaço virtual (swap).

  Para determinar o tamanho da partição swap automaticamente, use a opção `--recommended`:
  `swap --recommended`

  O tamanho da partição swap gerada automaticamente será igual ou maior à quantidade de RAM no sistema e, no máximo, o dobro da quantidade de RAM no sistema.

- `raid.`*<id>*

  A partição será usada para o RAID de software (consulte o `raid`).

- `pv.`*<id>*

  A partição será usada para o LVM (consulte o `logvol`).

`--size=`

O tamanho mínimo da partição em megabytes. Especifique aqui um valor inteiro, como 500. Não acrescente 'MB' ao número.

`--grow`

Diz à partição para aumentar até preencher todo o espaço disponível, ou até a definição de tamanho máximo.

`--maxsize=`

O tamanho máximo da partição em megabytes quando a partição é definida para aumentar. Especifique aqui um valor inteiro e não acrescente 'MB' ao número.

`--noformat`

Diz ao programa de instalação para não formatar a partição, no uso com o comando `--onpart`.

`--onpart=` ou `--usepart=`

Insere a partição no dispositivo *já existente*. Por exemplo:
`partition /home --onpart=hda1`

colocará `/home` no `/dev/hda1`, que já existe.

`--ondisk=` ou `--ondrive=`

Força a criação da partição em um disco específico. Por exemplo: `--ondisk=sdb` colocará a partição no segundo disco SCSI do sistema.

`--asprimary`

Força a alocação automática da partição como uma partição primária ou a partição falhará.

`--type=` (substituído por `fstype`)

Esta opção não está mais disponível. Use `fstype`.

`--fstype=`

Define o tipo de sistema de arquivo da partição. Os valores válidos são `ext2`, `ext3`, `swap` e `vfat`.

`--start=`

Especifica o cilindro inicial da partição. Requer a especificação de um disco com `--ondisk=` ou `ondrive=`. Também requer que o cilindro final seja especificado com `--end=` ou que o tamanho da partição seja especificado com `--size=`.

`--end=`

Especifica o cilindro final da partição. Requer que o cilindro inicial seja especificado com `--start=`.

**Nota**

Se a partição falhar por alguma razão, aparecerão mensagens de diagnóstico no console virtual 3.

`raid` (opcional)

Monta um dispositivo RAID de software. Este comando tem a forma:
`raid <mntpoint> --level=<level> --device=<mddevice> <partitions*>`

*<mntpoint>*

Localidade onde o sistema de arquivo RAID é montado. Se for /, o nível do RAID deve ser 1 a não ser que uma partição boot (/boot) esteja presente. Se estiver, a partição /boot deve ter nível 1 e a partição root (/) pode ter qualquer um dos tipos disponíveis. As *<partitions*>* (o que denota que diversas partições podem ser listadas) lista os identificadores RAID a serem adicionados ao conjunto RAID.

--level=

Nível do RAID a usar (0, 1 ou 5).

--device=

Nome do dispositivo RAID a usar (como md0 ou md1). Os dispositivos RAID variam de md0 a md7, e cada um pode ser usado somente uma vez.

--spares=

Especifica o número de discos avulsos alocados para o conjunto RAID. Os discos avulsos são usados para reconstruir o conjunto no caso de falha no disco.

--fstype=

Determina o tipo de sistema de arquivo do conjunto RAID. Os valores válidos são ext2, ext3, swap e vfat.

--noformat

Usa um dispositivo RAID existente e não formata o conjunto RAID.

--useexisting

Usa um dispositivo RAID existente e o reformata.

O exemplo seguinte mostra como criar uma partição RAID de nível 1 para /, e uma de nível 5 para /usr, assumindo que há três discos SCSI no sistema. Também cria três partições swap, uma em cada disco.

```
part raid.01 --size=60 --ondisk=sda
part raid.02 --size=60 --ondisk=sdb
part raid.03 --size=60 --ondisk=sdc
part swap --size=128 --ondisk=sda
part swap --size=128 --ondisk=sdb
part swap --size=128 --ondisk=sdc
part raid.11 --size=1 --grow --ondisk=sda
part raid.12 --size=1 --grow --ondisk=sdb
part raid.13 --size=1 --grow --ondisk=sdc
raid / --level=1 --device=md0 raid.01 raid.02 raid.03
raid /usr --level=5 --device=md1 raid.11 raid.12 raid.13
```

reboot (opcional)

Reinicialize a máquina após completar a instalação. Normalmente, o kickstart exibe uma mensagem e espera que o usuário pressione uma tecla antes de reinicializar.

rootpw (requisitado)

Define a senha root do sistema como o argumento *<password>*.

```
rootpw [--iscrypted] <password>
```

`--iscrypted`

Se isto estiver presente, assume-se que o argumento da senha já esteja criptografado.

`skipx` (opcional)

Se estiver presente, o X não está configurado no sistema instalado.

`text` (opcional)

Executa a instalação kickstart no modo texto. As instalações kickstart são executadas no modo gráfico por default.

`timezone` (requisitado)

Define o fuso horário do sistema como <*timezone*>, que pode ser qualquer um dos fusos horários listados pelo `timeconfig`.

`timezone [--utc]` <*timezone*>

`--utc`

Se estiver presente, o sistema assume que o relógio do hardware está definido para usar UTC (Horário de Greenwich).

`upgrade` (opcional)

Diz para atualizar um sistema existente ao invés de instalar um novo sistema. Você deve especificar um destes: cdrom, disco rígido (harddrive), nfs ou url (para ftp e http) como a localidade da árvore de instalação. Consulte o `install` para detalhes.

`xconfig` (opcional)

Configura o Sistema X Window. Se esta opção não for dada, o usuário precisará configurar o X manualmente durante a instalação, caso o X esteja instalado. Esta opção não deve ser usada se o X não está instalado no sistema final.

`--noprobe`

Não detectar o monitor.

`--card=`

Usa uma placa especificada. O nome desta placa deve estar na lista de placas do `/usr/share/hwdata/Cards` no pacote `hwdata`. A lista de placas também pode ser encontrada na tela **Configuração do X** da **Configurador do Kickstart**. Se este argumento não for provido, o programa de instalação detectará o canal PCI da placa. Como o AGP é parte do canal PCI, as placas AGP serão detectadas caso sejam suportadas. A ordem de detecção é determinada pela ordem do scan PCI da placa-mãe.

`--videoram=`

Especifique a quantidade de RAM da placa de vídeo.

`--monitor=`

Usa um monitor especificado. O nome do monitor deve constar da lista de monitores no `/usr/share/hwdata/MonitorsDB` do pacote `hwdata`. A lista de monitores também pode ser encontrada na tela **Configuração do X** da **Configurador do Kickstart**. Isto é

ignorado se a `--hsync` ou a `--vsync` for provida. Se não for provida nenhuma informação do monitor, o programa de instalação tenta detectá-lo automaticamente.

`--hsync=`

Especifica a frequência da sincronia horizontal do monitor.

`--vsync=`

Especifica a frequência da sincronia vertical do monitor.

`--defaultdesktop=`

Especifica GNOME ou KDE como sua área de trabalho (desktop) default, assumindo que ambos ou um dos ambientes foram instalados através do `%packages`.

`--startxonboot`

Usa autenticação (login) gráfica no sistema instalado.

`--resolution=`

Especifica a resolução default para o Sistema X Window do sistema instalado. Os valores válidos são: 640x480, 800x600, 1024x768, 1152x864, 1280x1024, 1400x1050 e 1600x1200. Assegure que a resolução seja compatível com a placa de vídeo e monitor.

`--depth=`

Especifica a definição de cores para o Sistema X Window do sistema instalado. Os valores válidos são: 8, 16, 24 e 32. Assegure que a definição de cores seja compatível com a placa de vídeo e monitor.

`volgroup` (opcional)

Use para criar um grupo LVM (Logical Volume Management) com a sintaxe:

```
volgroup <name> <partition> <options>
```

As opções são as seguintes:

--noformat

Usa um grupo de volume existente e não o formata.

--useexisting

Usa um grupo de volume existente e o reformata.

Crie a partição primeiro, depois crie o grupo de volume lógico e então o volume lógico. Por exemplo:

```
part pv.01 --size 3000
volgroup myvg pv.01
logvol / --vgname=myvg --size=2000 --name=rootvol
```

`zerombr` (opcional)

Se `zerombr` é especificado e `yes` é seu único argumento, quaisquer tabelas de partição inválidas encontradas nos discos são inicializadas. Isto destruirá todo o conteúdo dos discos com tabelas de partição inválidas. Este comando deve ter o seguinte formato:

```
zerombr yes
```

Nenhum outro formato é efetivo.

`%include`

Use o comando `%include` *`/path/to/file`* para incluir o conteúdo de outro arquivo no arquivo kickstart, como se o conteúdo estivesse na localidade do comando `%include` no arquivo kickstart.

## 9.5. Seleção de Pacotes

Use o comando `%packages` para começar uma seção do arquivo kickstart listando os pacotes que você quer instalar (válido apenas para instalações, já que a seleção de pacotes não é suportada em atualizações).

Os pacotes podem ser especificados pelo grupo ou pelo nome do pacote. O programa de instalação define vários grupos que contêm pacotes relacionados. Consulte o arquivo `RedHat/base/comps.xml` no primeiro CD-ROM do Red Hat Enterprise Linux para obter uma lista dos grupos. Cada grupo tem um id, valor de visibilidade do usuário, nome, descrição e lista de pacotes. Na lista, os pacotes marcados como obrigatórios são sempre instalados se o grupo for selecionado; os pacotes marcados como default são selecionados por default se o grupo for selecionado; e pacotes marcados como opcionais devem ser especificamente selecionados mesmo que o grupo esteja selecionado para ser instalado.

Na maioria dos casos, é necessário listar somente os grupos desejados e não os pacotes individualmente. Note que os grupos `Core` e `Base` são sempre selecionados por default, portanto não é necessário especificá-los na seção `%packages`.

Veja um exemplo da seleção de `%packages`:

```
%packages
@ X Window System
@ GNOME Desktop Environment
@ Graphical Internet
@ Sound and Video
dhcp
```

Como pode-se observar, os grupos são especificados, um em cada linha, começando pelo símbolo `@`, um espaço e então o nome completo do grupo conforme designado no arquivo `comps.xml`. Os grupos também podem ser especificados através de seus ids, como `gnome-desktop`. Especifique os pacotes individualmente sem caracteres adicionais (a linha `dhcp` do exemplo acima é um pacote individual).

Você também pode especificar quais pacotes não deseja instalar na lista de pacotes default:

```
-autofs
```

As opções seguintes estão disponíveis para a opção `%packages`:

`--resolvedeps`

Instale os pacotes listados e resolva as dependências de pacotes automaticamente. Se esta opção não está especificada e houver dependências de pacotes, a instalação automatizada terá uma pausa e questionará o usuário. Por exemplo:

```
%packages --resolvedeps
```

`--ignoredeps`

Ignore as dependências não resolvidas e instale os pacotes listados sem as dependências. Exemplo:

```
%packages --ignoredeps
```

`--ignoremissing`

Ignore os pacotes e grupos faltando ao invés de interromper a instalação para questionar se esta deve ser abortada ou continuada. Por exemplo:

```
%packages --ignoremissing
```

## 9.6. Script de Pré-Instalação

Você pode adicionar comandos para rodar no sistema logo após o `ks.cfg` ser examinado. Esta seção deve estar no fim do arquivo kickstart (depois dos comandos) e deve começar com o comando `%pre`. Você pode acessar a rede na seção `%pre`; no entanto, o *serviço de nome* ainda não foi configurado neste ponto, portanto somente o endereço IP funcionará.

**Nota**

Note que o script de pré-instalação não é executado no ambiente change root.

`--interpreter /usr/bin/python`

Permite que você especifique uma linguagem diferente de script, como Python. Substitua `/usr/bin/python` pela sua linguagem de script preferida.

### 9.6.1. Exemplo

Veja um exemplo da seção `%pre`:

```
%pre

#!/bin/sh

hds=""
mymedia=""

for file in /proc/ide/h*
do
  mymedia=`cat $file/media`
  if [ $mymedia == "disk" ] ; then
      hds="$hds `basename $file`"
  fi
done

set $hds
numhd=`echo $#`

drive1=`echo $hds | cut -d' ' -f1`
drive2=`echo $hds | cut -d' ' -f2`

#Write out partition scheme based on whether there are 1 or 2 hard drives

if [ $numhd == "2" ] ; then
  #2 drives
  echo "#partitioning scheme generated in %pre for 2 drives" > /tmp/part-include
  echo "clearpart --all" >> /tmp/part-include
  echo "part /boot --fstype ext3 --size 75 --ondisk hda" >> /tmp/part-include
  echo "part / --fstype ext3 --size 1 --grow --ondisk hda" >> /tmp/part-include
```

```
  echo "part swap --recommended --ondisk $drive1" >> /tmp/part-include
  echo "part /home --fstype ext3 --size 1 --grow --ondisk hdb" >> /tmp/part-include
else
  #1 drive
  echo "#partitioning scheme generated in %pre for 1 drive" > /tmp/part-include
  echo "clearpart --all" >> /tmp/part-include
  echo "part /boot --fstype ext3 --size 75" >> /tmp/part-includ
  echo "part swap --recommended" >> /tmp/part-include
  echo "part / --fstype ext3 --size 2048" >> /tmp/part-include
  echo "part /home --fstype ext3 --size 2048 --grow" >> /tmp/part-include
fi
```

Esse script determina o número de discos rígidos do sistema e grava um arquivo texto com um esquema de particionamento diferente dependendo do número de discos (um ou dois). Ao invés de ter um conjunto de comandos de particionamento no arquivo kickstart, inclua a linha:

```
%include /tmp/part-include
```

Os comandos de particionamento selecionados no script serão usados.

## 9.7. Script de Pós-Instalação

Você tem a opção de adicionar comandos para rodar no sistema logo após completar a instalação. Esta seção deve estar no fim do arquivo kickstart e deve começar com o comando `%post`. Esta seção é útil para funções como a instalação de software adicionais e a configuração de um servidor de nome (nameserver) adicional.

**Nota**

Se você configurou a rede com informações de IP estático, incluindo um servidor de nome, pode acessar a rede e resolver endereços IP na seção `%post`. Se configurou a rede para o DHCP, o arquivo `/etc/resolv.conf` não foi completado quando a instalação executou a seção `%post`. Você pode acessar a rede, mas não pode resolver endereços IP. Portanto, se usar o DHCP, você deve especificar os endereços IP na seção `%post`.

**Nota**

O script de pós-instalação é executado em um ambiente chroot; consequentemente, tarefas como copiar scripts ou RPMs pela mídia de instalação não funcionarão.

`--nochroot`

Permite que você especifique comandos que queira rodar fora do ambiente chroot.

O exemplo a seguir copia o arquivo `/etc/resolv.conf` para o sistema que acaba de ser instalado.

```
%post --nochroot
cp /etc/resolv.conf /mnt/sysimage/etc/resolv.conf
```

`--interpreter /usr/bin/python`

Permite que você especifique uma linguagem diferente de script, como Python. Substitua `/usr/bin/python` pela sua linguagem de script preferida.

### 9.7.1. Exemplos

Ligar e desligar os serviços:

```
/sbin/chkconfig --level 345 telnet off
/sbin/chkconfig --level 345 finger off
/sbin/chkconfig --level 345 lpd off
/sbin/chkconfig --level 345 httpd on
```

Executar um script chamado `runme` em uma partilha NFS:

```
mkdir /mnt/temp
mount 10.10.0.2:/usr/new-machines /mnt/temp
open -s -w -- /mnt/temp/runme
umount /mnt/temp
```

Adicionar um usuário ao sistema:

```
/usr/sbin/useradd bob
/usr/bin/chfn -f "Bob Smith" bob
/usr/sbin/usermod -p 'kjdf$04930FTH/ ' bob
```

## 9.8. Disponibilizando um Arquivo Kickstart

Um arquivo kickstart deve ser alocado em uma das localidades seguintes:

- Em um disquete boot
- Em um CD-ROM boot
- Em uma rede

Normalmente, um arquivo kickstart é copiado para o disquete boot ou disponibilizado na rede. A rede é o método mais usado, pois a maioria das instalações kickstart tende a ser executada nos computadores em rede.

Vamos dar uma olhada mais detalhada onde o arquivo kickstart pode ser alocado.

### 9.8.1. Criando um Disquete Boot com Kickstart

Para executar uma instalação kickstart baseada no disquete, o arquivo kickstart deve ser nomeado `ks.cfg` e deve estar localizado no diretório raiz do disquete. Consulte a seção *Criando um Disquete Boot de Instalação* do *Guia de Instalação do Red Hat Enterprise Linux* para obter instruções sobre a criação do disquete boot. Como o disquete boot tem formato MS-DOS, é fácil copiar o arquivo kickstart sob o Linux usando o comando `mcopy`.

```
mcopy ks.cfg a:
```

Alternativamente, você pode usar o Windows para copiar o arquivo. Pode também montar o disquete boot MS-DOS no Red Hat Enterprise Linux com o tipo de sistema de arquivo vfat e usar o comando `cp` para copiar o arquivo no disquete.

### 9.8.2. Criando um CD-ROM Boot com o Kickstart

Para executar uma instalação kickstart baseada no CD-ROM, o arquivo kickstart deve ser nomeado `ks.cfg` e deve estar localizado no diretório raiz do CD-ROM. Como um CD-ROM é somente-leitura, o arquivo deve ser adicionado ao diretório usado para criar a imagem gravada no CD-ROM. Consulte a seção *Criando um CD-ROM Boot de Instalação* do *Guia de Instalação do Red Hat Enterprise Linux* para obter instruções sobre a criação de um CD-ROM boot, mas, antes de criar o arquivo de imagem `file.iso`, copie o arquivo kickstart `ks.cfg` no diretório `isolinux/`.

### 9.8.3. Disponibilizando o Arquivo Kickstart na Rede

Instalações de rede usando kickstart são bastante comuns, porque os administradores de sistemas podem facilmente automatizar a instalação para muitos computadores em rede de forma rápida. Geralmente, a maneira mais usada é o administrador ter ambos, um servidor BOOTP/DHCP e um servidor NFS na rede local. O servidor BOOTP/DHCP é usado para dar ao sistema cliente sua configuração de rede, enquanto os arquivos usados durante a instalação são servidos pelo servidor NFS. Muitas vezes, estes dois servidores rodam na mesma máquina, mas isto não é necessário.

Para executar uma instalação kickstart baseada na rede, você precisa ter um servidor BOOTP/DHCP na sua rede e deve incluir as informações de configuração da máquina na qual está instalando o Red Hat Enterprise Linux. O servidor BOOTP/DHCP proverá suas informações de rede e a localidade do arquivo kisckstart ao cliente.

Se um arquivo kickstart é especificado pelo servidor BOOTP/DHCP, o sistema cliente tentará uma montagem NFS da localidade do arquivo e o copiará no cliente, usando-o como um arquivo kickstart. As configurações exatas variam dependendo do servidor BOOTP/DHCP que você usar.

Veja um exemplo de uma linha do arquivo `dhcpd.conf` do servidor DHCP:

```
filename "/usr/new-machine/kickstart/";
next-server blarg.redhat.com;
```

Note que você deve substituir o valor após `filename` pelo nome do arquivo kickstart (ou pelo diretório no qual o arquivo kickstart reside), e o valor após `next-server` pelo nome do servidor NFS.

Se o nome do arquivo retornado pelo servidor BOOTP/DHCP termina com uma barra ("/"), então é interpretado somente como a localidade. Neste caso, o sistema cliente monta esta localidade usando NFS e procura por um arquivo específico. O nome do arquivo pelo qual o cliente procura é:

```
<ip-addr>-kickstart
```

A seção `<ip-addr>` do nome do arquivo deve ser substituída pelo endereço IP do cliente com representação decimal pontuada. Por exemplo: o nome do arquivo de um computador com endereço IP 10.10.0.1 seria `10.10.0.1-kickstart`.

Note que se você não especificar um nome de servidor, o sistema cliente tentará usar o servidor que respondeu ao pedido BOOTP/DHCP como se fosse seu servidor NFS. Se você não especificar uma localidade ou nome de arquivo, o sistema cliente tentará montar o `/kickstart` pelo servidor BOOTP/DHCP e tentará encontrar o arquivo kickstart usando o mesmo nome de arquivo `<ip-addr>-kickstart`, conforme descrito acima.

## 9.9. Disponibilizando a Árvore de Instalação

A instalação kickstart precisa acessar uma *árvore de instalação*. Uma árvore de instalação é uma cópia dos CD-ROMs binários do Red Hat Enterprise Linux com a mesma estrutura de diretórios.

Se você está executando uma instalação baseada em CD, insira o CD-ROM 1 do Red Hat Enterprise Linux no computador antes de começar a instalação kickstart.

Se você está executando uma instalação baseada no disco rígido, assegure que as imagens ISO dos CD-ROMs binários do Red Hat Enterprise Linux estejam no disco rígido do computador.

Se você está executando uma instalação baseada na rede (NFS, FTP ou HTTP), deve disponibilizar a árvore de instalação na rede. Consulte a seção *Preparando uma Instalação de Rede* no *Guia de Instalação do Red Hat Enterprise Linux* para mais detalhes.

## 9.10. Iniciando uma Instalação Kickstart

Para começar uma instalação kickstart, você deve inicializar o sistema através de um disquete boot do Red Hat Enterprise Linux, CD-ROM boot ou pelo CD-ROM 1 do Red Hat Enterprise Linux e indicar um comando boot especial no prompt de início. O programa de instalação procura pelo arquivo kickstart se o argumento da linha de comando `ks` for passado ao kernel.

Disquete Boot

Se o arquivo kickstart estiver em um disquete boot conforme descrito na Seção 9.8.1, inicialize o sistema com o disquete no drive, e indique o seguinte comando no prompt `boot:`:

```
linux ks=floppy
```

CD-ROM 1 e Disquete

O comando **`linux ks=floppy`** também funciona se o arquivo `ks.cfg` está localizado em um sistema de arquivo vfat ou ext2 de um disquete e você inicializa pelo CD-ROM 1 do Red Hat Enterprise Linux.

Um comando boot alternativo é inicializar pelo CD-ROM 1 do Red Hat Enterprise Linux e ter o arquivo kickstart em um sistema de arquivo vfat ou ext2 de um disquete. Para fazer isso, indique o seguinte comando no prompt `boot:`:

```
linux ks=hd:fd0:/ks.cfg
```

Com Disco de Driver

Se você precisa usar um disco de driver com kickstart, especifique também a opção **`dd`**. Por exemplo: para inicializar por um disquete boot e usar um disco de driver, indique o seguinte comando no prompt `boot:`:

```
linux ks=floppy dd
```

CD-ROM Boot

Se o arquivo kickstart está em um CD-ROM boot, conforme descrito na Seção 9.8.2, insira o CD-ROM no sistema, inicialize o sistema e indique o seguinte comando no prompt `boot:` (onde `ks.cfg` é o nome do arquivo kickstart):

```
linux ks=cdrom:/ks.cfg
```

Há outras opções para iniciar uma instalação kickstart:

`ks=nfs:`*<server>*`:/`*<path>*

O programa de instalação procurará pelo arquivo kickstart no servidor NFS *<server>*, como o arquivo *<path>*. O programa de instalação usará o DHCP para configurar a placa Ethernet. Por exemplo: se o seu servidor NFS é servidor.exemplo.com e o arquivo kickstart está na partilha NFS `/mydir/ks.cfg`, o comando boot correto seria `ks=nfs:server.example.com:/mydir/ks.cfg`.

`ks=http://<server>/<path>`

O programa de instalação procurará pelo arquivo kickstart no servidor HTTP *<server>*, como o arquivo *<path>*. O programa de instalação usará o DHCP para configurar a placa Ethernet. Por exemplo: se o seu servidor HTTP é servidor.exemplo.com e o arquivo kickstart está no diretório HTTP `/mydir/ks.cfg`, o comando boot correto seria `ks=http://server.example.com/mydir/ks.cfg`.

`ks=floppy`

O programa de instalação procura o arquivo `ks.cfg` em um sistema de arquivo vfat ou ext2 do disquete em `/dev/fd0`.

`ks=floppy:/<path>`

O programa de instalação procurará o arquivo kickstart no disquete em `/dev/fd0`, como o arquivo *<path>*.

`ks=hd:<device>:/<file>`

O programa de instalação montará o sistema de arquivo no *<device>* (que deve ser vfat ou ext2), e procurará o arquivo de configuração kickstart como *<file>* naquele sistema de arquivo (ex.: `ks=hd:sda3:/mydir/ks.cfg`).

`ks=file:/<file>`

O programa de instalação tentará acessar o arquivo *<file>* pelo sistema de arquivo; nenhuma montagem será feita. Isto é usado normalmente se o arquivo kickstart já está na imagem `initrd`

`ks=cdrom:/<path>`

O programa de instalação procurará o arquivo kickstart no CD-ROM, como o arquivo *<path>*.

`ks`

Se `ks` é usado sozinho, o programa de instalação configurará a placa Ethernet para usar o DHCP. O arquivo kickstart é lido no "bootServer" pela resposta DHCP como se fosse um servidor NFS compartilhando o arquivo kickstart. Por default, o bootServer é o mesmo que o servidor DHCP. O nome do arquivo kickstart é um dos seguintes:

- Se o DHCP é especificado e o arquivo boot começa com uma `/`, o arquivo boot provido pelo DHCP é procurado no servidor NFS.
- Se o DHCP é especificado e o arquivo boot começa com algo diferente de `/`, o arquivo boot provido pelo DHCP é procurado no diretório `/kickstart` do servidor NFS.
- Se o DHCP não especificar um arquivo boot, então o programa de instalação tenta acessar o arquivo `/kickstart/1.2.3.4-kickstart`, onde *1.2.3.4* é o endereço IP numérico da máquina sendo instalada.

`ksdevice=<device>`

O programa de instalação usará este dispositivo de rede para conectar à rede. Por exemplo: para inciar uma instalação kickstart com o arquivo kickstart em um servidor NFS conectado ao sistema através do dispositivo eth1, use o comando `ks=nfs:<server>:/<path> ksdevice=eth1` no prompt `boot:`.

# Capítulo 10.

# Configurador do Kickstart

A **Configurador do Kickstart** permite criar ou modificar um arquivo kickstart usando uma interface gráfica de usuário para que você não precise lembrar a sintaxe correta do arquivo.

Para usar a **Configurador do Kickstart**, você precisar estar no Sistema X Window. Para iniciar a **Configurador do Kickstart**, selecione **Botão do Menu Principal** (no Painel) => **Ferramentas do Sistema => Kickstart**, ou digite o comando `/usr/sbin/redhat-config-kickstart`.

Enquanto você cria um arquivo kickstart, pode selecionar **Arquivo => Pré-visualização** a qualquer momento para rever suas seleções correntes.

Para iniciar com um arquivo kickstart existente, selecione **Arquivo => Abrir** e selecione o arquivo.

## 10.1. Configuração Básica

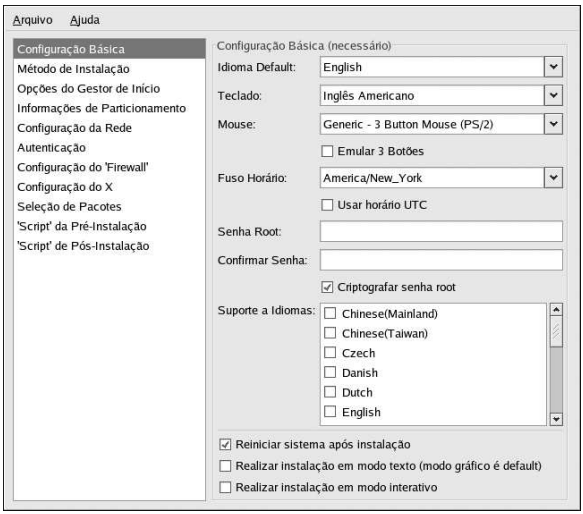


**Figura 10-1. Configuração Básica**

Selecione o idioma a usar durante a instalação e como idioma default após a instalação a partir do menu **Idioma Default**.

Selecione o tipo de teclado do sistema no menu **Teclado**.

Selecione o mouse do sistema no menu **Mouse**. Se a opção **Sem Mouse** está selecionada, nenhum mouse será configurado. Se **Detectar Mouse** está selecionada, o programa de instalação tenta detectar o mouse automaticamente. A detecção funciona para a maioria dos mouses modernos.

Se o sistema tem um mouse de dois botões, é possível emular um mouse de três botões, selecionando **Emular 3 Botões**. Se esta opção está selecionada, quando você clicar os dois botões do mouse simultaneamente, será reconhecido como um clique do botão do meio de um mouse de três botões.

No menu **Fuso Horário**, selecione o fuso horário a utilizar para o sistema. Para configurar o sistema a usar UTC, selecione **Usar relógio UTC**.

Indique a senha root desejada para o sistema na caixa de texto **Senha Root**. Digite a mesma senha na caixa de texto **Confirmar Senha**. O segundo campo garante que você não tenha digitado errado a senha e depois perceba que não sabe o que foi digitado após completar a instalação. Para salvar a senha como criptografada no arquivo, selecione **Criptografar senha root**. Se a opção de criptografia está selecionada, ao salvar o arquivo, a senha somente-texto que você digitou será criptografada e gravada no arquivo kickstart. Não digite uma senha já criptografada e escolha criptografá-la. Como um arquivo kickstart é somente-texto e fácil de ser acessado, é recomendado usar uma senha criptografada.

Para instalar idiomas além daquele selecionado no menu suspenso **Idioma Default**, selecione-os na lista **Suporte ao Idioma**. O idioma selecionado no menu suspenso **Idioma Default** é usado por default após a instalação; no entanto, pode ser alterado com a **Ferramenta de Configuração do Idioma** (`redhat-config-language`) após a instalação.

Selecionando **Reinicializar sistema após instalação** reinicializará seu sistema automaticamente após completar a instalação.

Instalações kickstart são executadas no modo gráfico por default. Para sobrescrever este default e usar o modo texto, selecione a opção **Executar instalação em modo texto**.

Você pode executar uma instalação kickstart no modo interativo, Isto significa que o programa de instalação usa todas as opções pré-configuradas no arquivo kickstart, mas permite que você veja as opções em cada tela antes de continuar para a próxima tela. Para continuar à próxima tela, clique no botão **Próximo** após aprovar as configurações ou alterá-las antes de continuar a instalação. Para selecionar este tipo de instalação, escolha a opção **Executar instalação no modo interativo**.

## 10.2. Método de Instalação

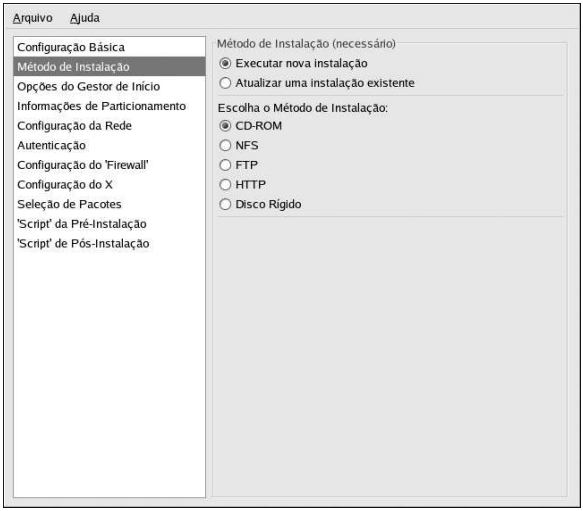


**Figura 10-2. Método de Instalação**

A tela **Método de Instalação** permite escolher entre executar uma nova instalação ou uma atualização (upgrade). Se você escolher atualizar, as opções **Informações da Partição** e **Seleção de Pacotes** serão

desabilitadas. Estas não são suportadas para atualizações kickstart.

Também escolha o tipo da tela da instalação ou atualização kickstart dentre as seguintes opções:

- **CD-ROM** — Selecione esta opção para instalar ou atualizar a partir dos CD-ROMs do Red Hat Enterprise Linux.
- **NFS** — Selecione esta opção para instalar ou atualizar a partir de um diretório NFS compartilhado. No campo de texto do servidor NFS, indique um nome de domínio ou endereço IP qualificado. No caso do diretório NFS, indique o diretório NFS que contém o diretório `RedHat` da árvore de instalação. Por exemplo: se o servidor NFS contém o diretório `/mirrors/redhat/i386/RedHat/`, indique `/mirrors/redhat/i386/` para o diretório NFS.
- **FTP** — Selecione esta opção para instalar ou atualizar a partir de um servidor FTP. No campo de texto do servidor FTP, indique um nome de domínio ou endereço IP qualificado. No o diretório FTP, indique o diretório FTP que contém o diretório `RedHat` directory. Por exemplo: se o servidor FTP contém o diretório `/mirrors/redhat/i386/RedHat/`, indique `/mirrors/redhat/i386/` para o diretório FTP. Se o servidor FTP requer um nome de usuário e senha, especifique-os também.
- **HTTP** — Selecione esta opção para instalar ou atualizar a partir de um servidor HTTP. No campo de texto do servidor HTTP, indique um nome de domínio ou endereço IP qualificado. No diretório HTTP, indique o nome do diretório HTTP que contém o diretório `RedHat`. Por exemplo: se o servidor HTTP contém o diretório `/mirrors/redhat/i386/RedHat/`, indique `/mirrors/redhat/i386/` para o diretório HTTP.
- **Disco Rígido** — Selecione esta opção para instalar ou atualizar a partir de um disco rígido. Instalações pelo disco rígido requerem o uso de imagens ISO (ou de CD-ROM). Certifique-se de verificar se as imagens ISO estão intactas antes de começar a instalação. Para verificá-las, use um programa `md5sum` assim como a opção boot `linux mediacheck` abordada no *Guia de Instalação do Red Hat Enterprise Linux*. Indique a partição do disco rígido que contém as imgens ISO (ex.: `/dev/hda1`) na caixa de texto **Partição do Disco Rígido**. Indique o diretório que contém as imagens ISO na caixa de texto **Diretório do Disco Rígido**.

## 10.3. Opções de Gestor de Início

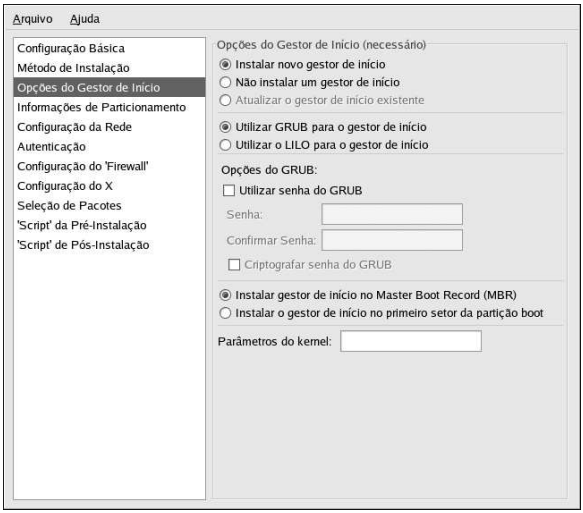


**Figura 10-3. Opções de Gestor de Início**

Você tem a opção de instalar o GRUB ou o LILO como o gestor de início. Se você não deseja instalar um gestor de início, selecione **Não instalar gestor de início**. Se você assim optar, certifique-se de criar um disquete boot ou de ter uma outra maneira de inicializar (como um gestor de início de terceiros) seu sistema.

Se você optar por instalar um gestor de início, também deve escolher qual deles instalar (GRUB ou LILO) e onde instalá-lo (no Master Boot Record ou no primeiro setor da partição `/boot`). Instale o gestor de início no MBR se você planeja usá-lo como seu gestor de início. Se você usar um gestor de início diferente, instale o LILO ou o GRUB no primeiro setor da partição `/boot` e configure o outro gestor para inicializar o Red Hat Enterprise Linux.

Para passar quaisquer requerimentos especiais ao kernel utilizado na inicialização do sistema, indique-os no campo de texto **Parâmetros do kernel**. Por exemplo: se você tem um Gravador de CD-ROM IDE, pode dizer ao kernel usar o driver de emulação SCSI que deve ser carregado antes de usar o `cdrecord`. Basta configurar **`hdd=ide-scsi`** como um parâmetro do kernel (onde **`hdd`** é o dispositivo do CVD-ROM).

Se você escolher o GRUB como gestor de início, pode protegê-lo com uma senha. Selecione **Usar senha do GRUB**, e indique a senha no campo **Senha**. Digite a mesma senha no campo **Confirmar Senha**. Para salvar a senha criptografada no arquivo , selecione **Criptografar senha do GRUB**. Se a opção de criptografia está selecionada, ao salvar o arquivo, a senha somente-texto que você digitou será criptografada e salva no arquivo kickstart. Não digite uma senha já criptografada e selecione criptografá-la.

Se você optar pelo LILO como o gestor de início, escolha se deseja usar o modo linear e se deseja forçar o uso de um modo lba32.

Se a opção **Atualizar uma instalação existente** está selecionada na página **Método de Instalação**, selecione **Atualizar gestor de início existente** para atualizar a configuração, enquanto preserva entradas antigas.

## 10.4. Informações da Partição

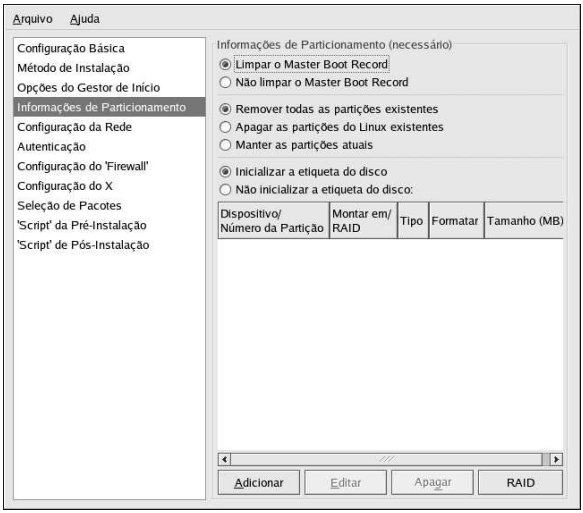


**Figura 10-4. Informações da Partição**

Selecione limpar ou não o Master Boot Record (MBR). Escolha entre remover todas as partições existentes, remover todas as partições Linux ou preservar as partições existentes.

Para inicializar a etiqueta do disco como default para a arquitetura do sistema (por exemplo: `msdos` para x86 e `gpt` para Itanium), selecione **Inicializar a etiqueta de disco** se você está instalando em um disco rígido novo.

### 10.4.1. Criando Partições

Para criar uma partição, clique no botão **Adicionar**. Aparece a janela **Opções da Partição**, conforme mostra aFigura 10-5. Escolha o ponto de montagem, tipo de sistema de arquivo e tamanho da nova partição. Opcionalmente, você também pode escolher a partir do seguinte:

- Na seção **Opções Adicionais de Tamanho**, escolha ter a partição de tamanho fixo, até um tamanho escolhido ou preencher o espaço remanescente no disco rígido. Se você selecionou o tipo de partição swap, pode optar para que programa de instalação crie a partição swap com o tamanho recomendado ao invés de especificá-lo.
- Forçar para que a partição seja criada como primária.
- Crie a partição em um disco rígido específico. Por exemplo: para criar a partição noprimeiro disco rígido IDE (`/dev/hda`), indique **`hda`** como o disco rígido. Não inclua `/dev` no nome do disco.
- Use uma partição existente. Por exemplo: para criar a partição na primeira partição doprimeiro disco rígido IDE (`/dev/hda1`), indique **`hda1`** como a partição. Não inclua `/dev` no nome da partição.
- Formate a partição como o tipo de sistema de arquivo escolhido.

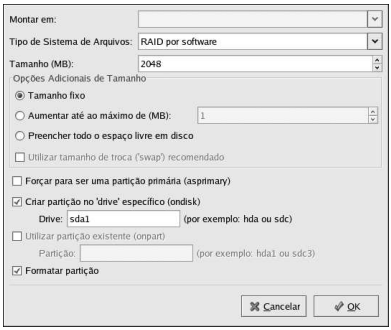


**Figura 10-5. Criando Partições**

Para editar uma partição existente, selecione-a na lista e clique no botão **Editar**. Aparece a mesma janela **Opções da Partição** quando você adiciona uma partição, conforme a Figura 10-5, exceto pelo fato de que esta reflete os valores da partição selecionada. Modifique as opções da partição e clique em **OK**.

Para apagar uma partição existente, selecione-a na lista e clique no botão **Apagar**.

#### 10.4.1.1. Criando Partições RAID de Software

Consulte o Capítulo 3 para aprender mais sobre o RAID e seus diferentes níveis. Os RAIDs 0, 1 e 5 podem ser configurados.

Para criar uma partição RAID de software, siga os seguintes passos:

1. Clique no botão **RAID**.
2. Selecione **Criar uma partição RAID de software**.
3. Configure as partições conforme descrito anteriormente, mas desta vez selecione **RAID de Software** como o tipo de sistema de arquivo. Também é necessário especificar um disco rígido no qual criar a partição ou uma partição existente para usar.

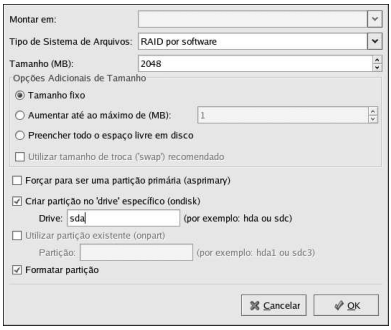


**Figura 10-6. Criando uma Partição RAID de Software**

Repita estes passos para criar quantas partições forem necessárias para a configuração de seu RAID. Não é necessário que todas as partições sejam RAID.

Após criar todas as partições necesárias para formar um dispositivo RAID, siga estes passos:

1. Clique no botão **RAID**.
2. Selecione **Criiar um dispositivo RAID**.
3. Escolha um ponto de montagem, tipo de sistema de arquivo, nome do dispositivo RAID, nível do RAID, membros do RAID, número de avulsas para o dispositivo RAID de software e se deseja formatar o dispositivo RAID.

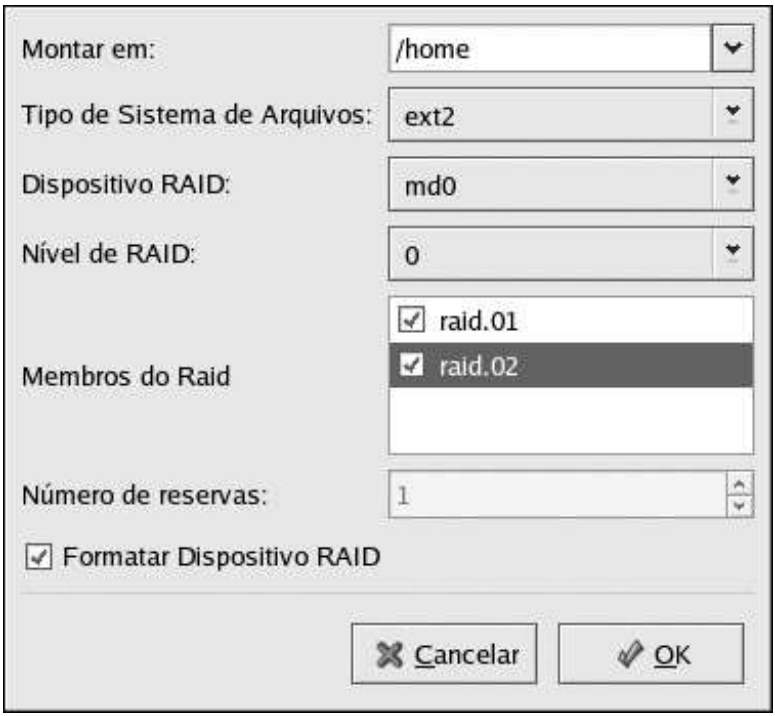


**Figura 10-7. Criando um Dispositivo RAID de Software**

4. Clique em **OK** para adicionar o dispositivo à lista.

## 10.5. Configuração de Rede

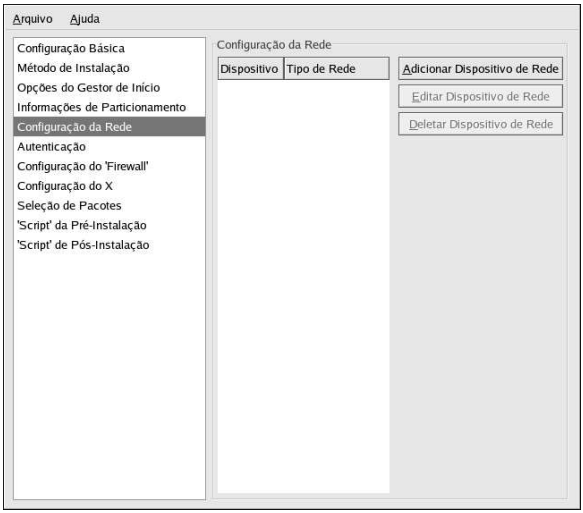


**Figura 10-8. Configuração de Rede**

Se o sistema a ser instalado via kickstart não tem uma placa Ethernet, não configure-a na página **Configuração de Rede**.

A rede é necessária somente se você escolher um método de instalação baseado na rede (NFS, FTP ou HTTP). A rede pode sempre ser configurada após a instalação com a **Ferramenta de Administração de Rede** (`redhat-config-network`). Consulte o Capítulo 19 para mais detalhes.

Para cada placa Ethernet no sistema, clique em **Adicionar Dispositivo de Rede** e selecione o tipo de rede e dispositivo de rede. Selecione **eth0** para configurar a primeira placa Ethernet, **eth1** para a segunda placa Ethernet e assim por diante.

## 10.6. Autenticação

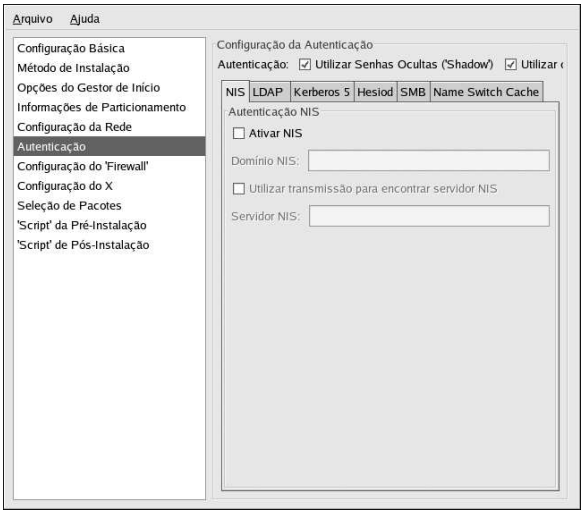


**Figura 10-9. Autenticação**

Na seção **Autenticação**, selecione se deseja usar senhas shadow e criptografia MD5 para senhas de usuário. Estas opções são altamente recomendadas e selecionadas por default.

As opções da **Configuração da Autenticação** permitem configurar os seguintes métodos de autenticação:

- NIS
- LDAP
- Kerberos 5
- Hesiod
- SMB
- Name Switch Cache

Estes métodos não são habilitados por default. Para habilitar um ou mais deles, clique na aba apropriada e depois selecione a caixa de verificação próxima de **Habilitar**, e indique as informações necessárias para o método de autenticação. Consulte o Capítulo 29 para mais informações sobre estas opções.

## 10.7. Configuração do Firewall

A janela de **Configuração do Firewall** é similar à tela do programa de instalação e à **Ferramenta de Configuração do Nível de Segurança**.

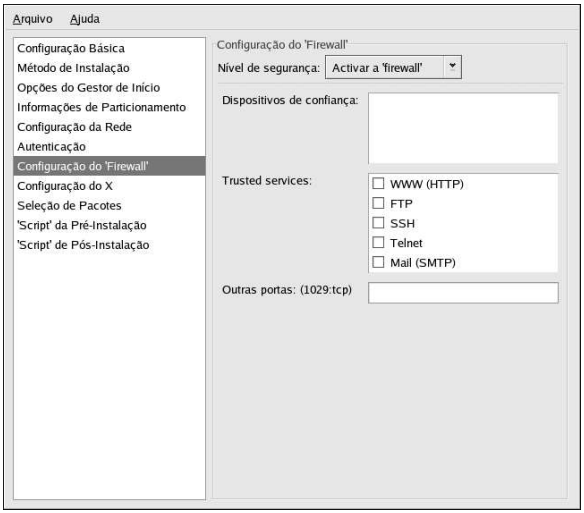


**Figura 10-10. Configuração do Firewall**

Se **Desabilitar firewall** é selecionada, o sistema permite acesso completo a todos os serviços e portas ativos. Nenhuma conexão ao sistema é recusada ou proibida.

Selecionar **Habilitar firewall** configura o sistema para rejeitar conexões de entrada que não vem como respostas a pedidos para fora, como respostas DNS ou pedidos DHCP. Se for necessário o acesso a serviços rodando nesta máquina, você pode optar por permitir determinados serviços através do firewall.

Somente os dispositivos configurados na seção**Configuração de Rede** são listados como **Dispositivos confiáveis** disponíveis. As conexões de qualquer dispositivo da lista são aceitas pelo sistema. Por exemplo: se **eth1** recebe conexões somente do sistema interno, você provavelmente desejará permitir as conexões dela.

Se um serviço é selecionado da lista **Dispositivos confiáveis**, as conexões para o serviço são aceitas e processadas pelo sistema.

Liste as portas adicionais que devem ser abertas para acesso remoto no campo **Outras portas**. Use o seguinte formato: **`porta:protocolo`**. Por exemplo: para permitir acesso ao IMAP através do firewall, especifique **`imap:tcp`**. Portas numéricas também podem ser especificadas. Para permitir pacotes UDP na porta 1234 através do firewall, indique **`1234:udp`**.

## 10.8. Configuração do X

Se você está instalando o Sistema X Window, pode configurá-lo durante a instalação do kickstart, selecionando a opção **Configurar o Sistema X Window** na janela **Configuração do X**, conforme a Figura 10-11. Se esta opção não estiver selecionada, as opções de configuração do X serão desabilitadas e a opção `skipx` será gravada no arquivo kickstart.

### 10.8.1. Geral

O primeiro passo na configuração do X é selecionar a resolução e a definição de cores default. Selecione-as em seus respectivos menus suspensos. Certifique-se de especificar uma resolução e definição de cores compatíveis com a placa de vídeo e com o monitor do sistema.

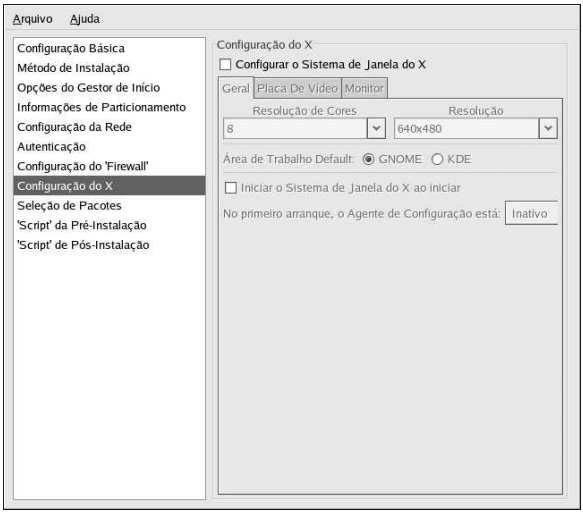


**Figura 10-11. Configuração do X - Geral**

Se você está instalando ambas áreas de trabalho, GNOME e KDE, deve selecionar qual delas será a default. Se for instalar apenas uma, certifique-se de selecioná-la. Após o sistema ser instalado, os usuários podem escolher qual área de trabalho querem que seja a default.

Em seguida, selecione se deseja que o Sistema X Window inicie no momento da inicialização da máquina. Esta opção inicializará o sistema no nível de execução 5 com a tela de autenticação gráfica. Após instalar o sistema, isto pode ser modificado alterando o arquivo de configuração `/etc/inittab`.

Selecione também se deseja iniciar o **Agente de Configuração** na primeira vez em que o sistema é reinicializado. O agente é desabilitado por default, mas a configuração pode ser alterada para habilitado ou habilitado no modo de reconfiguração. O modo de reconfiguração habilita o idioma, mouse, teclado, senha root, nível de segurança, fuso horário e as opções de configuração da rede, além das opções default.

### 10.8.2. Placa de Vídeo

A opção **Detectar placa de vídeo** é selecionada por default. Aceite-a para que o programa de instalação detecte a placa de vídeo durante a instalação. A detecção funciona para a maioria das placas de vídeo modernas. Se esta opção está selecionada e o programa de instalação não puder detectar a placa de vídeo, o programa de instalação parará na tela de configuração da placa de vídeo. Para continuar o processo de instalação, selecione sua placa de vídeo na lista e clique em **Próximo**.

Alternativamente, é possível selecionar a placa de vídeo na lista da aba **Placa de Vídeo**, conforme mostra a Figura 10-12. Especifique a quantidade de RAM de vídeo da placa selecionada no menu suspenso **RAM da Placa de Vídeo**. Estes valores são usados pelo programa de instalação para configurar o Sistema X Window.

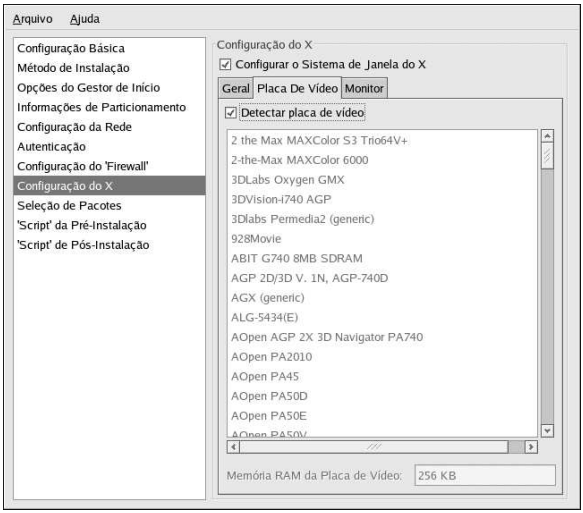


**Figura 10-12. Configuração do X - Placa de Vídeo**

### 10.8.3. Monitor

Após configurar a placa de vídeo, clique na aba **Monitor**, conforme a Figura 10-13.

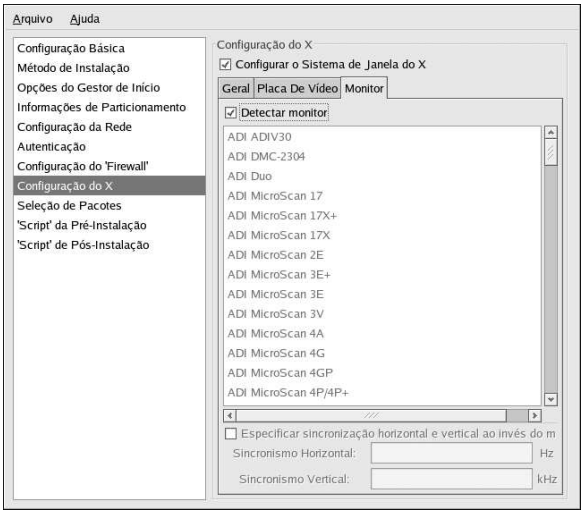


**Figura 10-13. Configuração do X - Monitor**

A opção **Detectar monitor** é selecionada por default. Aceite-a para que o programa de instalação detecte o monitor durante a instalação. A detecção funciona para a maioria dos monitores modernos. Se esta opção está selecionada e o programa de instalação não puder detectar o monitor, o programa de instalação parará na tela de configuração do monitor. Para continuar o processo de instalação, selecione seu monitor da lista e clique em **Próximo**.

Alternativamente, é possível selecionar o monitor da lista. Você também pode especificar as taxas de sincronia horizontal e vertical ao invés de selecionar um monitor específico, selecionando a opção **Especificar hysnc e vsync ao invés do monitor**. Esta opção é útil caso o monitor do sistema não esteja listado. Note que quando esta opção é habilitada, a lista de monitores é desabilitada.

## 10.9. Seleção de Pacotes

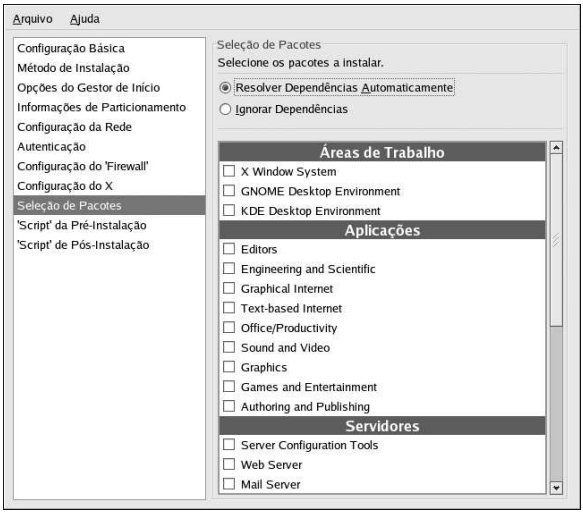


**Figura 10-14. Seleção de Pacotes**

A janela **Seleção de Pacotes** permite escolher quais grupos de pacotes instalar.

Também há opções disponíveis para resolver e ignorar as dependências de pacotes automaticamente.

Atualmente, a **Configurador do Kickstart** não permite selecionar pacotes individuais. Para instalar pacotes individuais, modifique a seção `%packages` do arquivo kickstart após salvá-lo. Consulte a Seção 9.5 para mais detalhes.

## 10.10. Script de Pré-Instalação

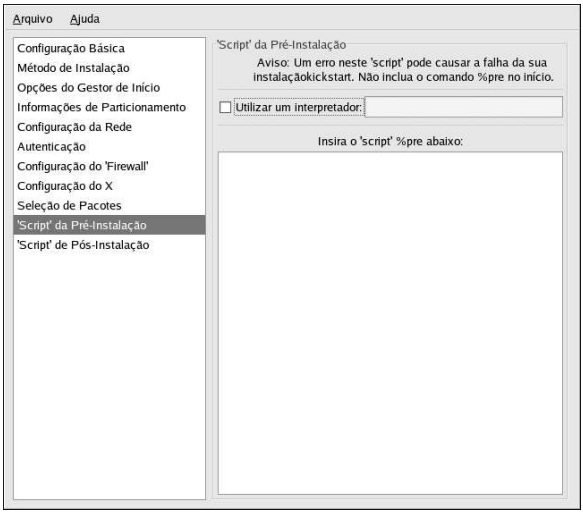


**Figura 10-15. Script de Pré-Instalação**

Você pode adicionar comandos para rodarem no sistema logo após o arquivo kickstart ser examinado e antes da instalação começar. Se você configurou a rede no arquivo kickstart, ela estará habilitada antes desta seção ser processada. Para incluir um script de pré-instalação, digite-o na área de texto.

Para especificar uma linguagem de script a ser usada na execução do script, selecione a opção **Usar um intérprete** e indique o intérprete na caixa de texto ao seu lado. Por exemplo: **`/usr/bin/python2.2`** pode ser especificado para um script Python. Esta opção corresponde a usar `%pre --interpreter` *`/usr/bin/python2.2`* em seu arquivo kickstart.

**Atenção**

Não inclua o comando `%pre`, pois será adicionado para você.

## 10.11. Script de Pós-Instalação

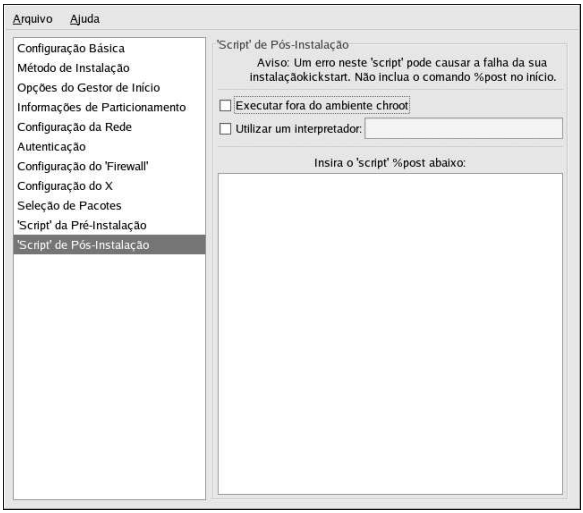


**Figura 10-16. Script de Pós-Instalação**

Você também pode adicionar comandos para executar no sistema após a conclusão da instalação. Se a rede estiver configurada corretamente no arquivo kickstart, é habilitada e o script pode incluir comandos para acessar recursos na rede. Para incluir um script de pós-instalação, digite-o na área de texto.


**Atenção**

Não inclua o comando `%post`, pois será adicionado para você.

Por exemplo: para alterar a mensagem do dia no sistema recém-instalado, adicione o seguinte comando à seção `%post`:

```
echo "Hackers will be punished!" > /etc/motd
```


**Dica**

Outros exemplos podem ser encontrados na Seção 9.7.1.

### 10.11.1. Ambiente Chroot

Para rodar o script de pós-instalação fora do ambiente chroot, clique na caixa de verificação próxima a esta opção no alto da janela **Pós-Instalação**. Isto equivale a usar a opção `--nochroot` na seção `%post`.

Para modificar o sistema de arquivo recém-instalado na seção pós-instalação fora do ambiente chroot, você deve preceder o nome do diretório com `/mnt/sysimage/`.

Por exemplo: se você selecionar **Rodar fora do ambiente chroot**, o exemplo anterior precisa ser alterado para o seguinte:

```
echo "Hackers will be punished!" > /mnt/sysimage/etc/motd
```

### 10.11.2. Usar um Intérprete

Para especificar uma linguagem de script a ser usada na execução do script, selecione a opção **Usar um intérprete** e indique o intérprete na caixa de texto ao seu lado. Por exemplo: **`/usr/bin/python2.2`** pode ser especificado para um script Python. Esta opção corresponde a usar `%post --interpreter` *`/usr/bin/python2.2`* em seu arquivo kickstart.

## 10.12. Salvando o Arquivo

Para rever o conteúdo do arquivo kickstart após conluir a escolha de suas opções, selecione **Arquivo => Pré-visualização** no menu suspenso.

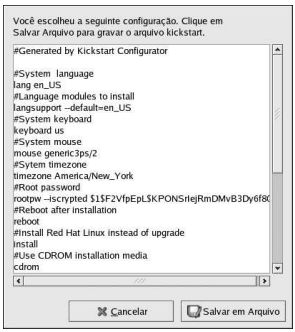


**Figura 10-17. Pré-visualização**

Para salvar o arquivo kickstart, clique no botão **Salvar no Arquivo** na janela de pré-visualização. Para salvar o arquivo sem visualizá-lo, selecione **Arquivo => Salvar Arquivo** ou pressione [Ctrl]-[S]. Aparece uma caixa de diálogo e então selecione onde salvar o arquivo.

Após salvar o arquivo, consulte a Seção 9.10 para obter informações sobre como iniciar a instalação do kickstart.

redhat

Capítulo 11.

# Recuperação Básica do Sistema

Quando algumas coisas dão errado, há diversas maneiras de solucionar os problemas. No entanto, estes métodos requerem que você entenda bem o funcionamento do sistema. Este capítulo explica como inicializar a máquina no modo de recuperação, no modo de usuário simples e no modo de emergência, no qual você pode usar seu próprio conhecimento para consertar o sistema.

## 11.1. Problemas Comuns

Você talvez precise inicializar em um destes modos de recuperação por alguma das razões abaixo:

- Não é possível inicializar a máquina manualmente no Red Hat Enterprise Linux (nível de execução 3 ou 5).
- Ocorrem problemas de hardware ou software e você deseja remover alguns arquivos importantes de seu disco rígido.
- Você esqueceu a senha.

### 11.1.1. Não é possível Inicializar no Red Hat Enterprise Linux

Este problema é causado frequentemente pela instalação de outro sistema operacional após você ter instalado o Red Hat Enterprise Linux. Alguns sistemas operacionais assumem que você não tenha outros em seu computador. Eles sobrescrevem o Master Boot Record (MBR) que originalmente continha o gestor de início GRUB ou LILO. Se o gestor for sobrescrito desta maneira, você não poderá inicializar o Red Hat Enterprise Linux a não ser que consiga entrar no modo de recuperação e reconfigure o gestor de início.

Um outro problema comum ocorre ao usar uma ferramenta de particionamento para redimensionar ou criar uma partição no espaço livre após a instalação, e altera a ordem de suas partições. Se o número de sua partição `/` mudar, o gestor de início talvez não encontre a partição para montá-la. Para consertar este problema, inicialize a máquina em modo de recuperação e modifique `/boot/grub/grub.conf` se usar o GRUB ou `/etc/lilo.conf` para o LILO. Você também *deve* rodar o comando `/sbin/lilo` sempre que alterar o arquivo de configuração do LILO.

### 11.1.2. Problemas com Hardware/Software

Esta categoria inclui uma ampla variedade de situações diferentes. Dois exemplos são a queda de discos rígidos e a especificação de um dispositivo root ou kernel inválido no arquivo de configuração do gestor de início. Se algum destes ocorrer, é possível que você não consiga inicializar o Red Hat Enterprise Linux. No entanto, se você inicializar em um dos modos de recuperação do sistema, pode resolver o problema ou, pelo menos, obter cópias de seus arquivos mais importantes.

### 11.1.3. Senha Root

O que você pode fazer se esquecer sua senha root? Para restaurá-la para uma senha diferente, incialize no modo de recuperação ou de usuário simples e use o comando `passwd` para restaurar a senha root.

## 11.2. Inicializando no Modo de Recuperação

O modo de recuperação oferece a habilidade de inicializar um ambiente Red Hat Enterprise Linux pequeno inteiramente a partir de um disquete, CD-ROM ou algum outro método de inicialização além do disco rígido do sistema.

Como o nome implica, o modo de recuperação é oferecido para salvá-lo de algo. Durante a operação normal, seu sistema Red Hat Enterprise Linux usa arquivos localizados no disco rígido para fazer tudo — rodar programas, armazenar seus arquivos, dentre outras tarefas.

Entretanto, às vezes você não consegue fazer o Red Hat Enterprise Linux rodar suficientemente para acessar os arquivos no disco rígido de seu sistema. Usando o modo de recuperação, você pode acessar os arquivos de seu disco rígido mesmo que não seja possível rodar o Red Hat Enterprise Linux neste disco rígido.

Para inicializar no modo de recuperação, você deve inicializar o sistema usando um dos métodos a seguir:

- Inicializando o sistema através de um disquete boot de instalação. [1]
- Inicializando o sistema através de um CD-ROM boot de instalação.[1]
- Inicializando o sistema através do CD-ROM 1 do Red Hat Enterprise Linux.

Após inicializar o sistema usando um dos métodos descritos, adicione a palavra-chave **`rescue`** como um parâmetro do kernel. Por exemplo: para um sistema x86, digite o seguinte comando no prompt de início da instalação:

```
linux rescue
```

Você terá que responder algumas questões básicas, incluindo qual idioma usar. Também deverá selecionar a localização de uma imagem de recuperação válida. Selecione **CD-ROM local**, **Disco Rígido**, **Imagem NFS**, **FTP** ou **HTTP**. A localização selecionada deve conter uma árvore de instalação válida, e esta deve ser para a mesma versão do Red Hat Enterprise Linux que o CD-ROM 1 com o qual você inicializou a máquina. Se você usou um disquete ou CD-ROM boot para iniciar o modo de recuperação, a árvore de instalação deve ser da mesma árvore a partir da qual a mídia foi criada. Para mais informações sobre a configuração de uma árvore de instalação no disco rígido, servidor NFS, servidor FTP ou servidor HTTP, consulte o *Guia de Instalação do Red Hat Enterprise Linux*.

Se você selecionar uma imagem de recuperação que não requer uma conexão de rede, você será questionado se deseja ou não estabelecer uma. A conexão de rede é útil se você quiser fazer backup de arquivos em um outro computador ou instalar alguns pacotes RPM de uma localização de rede compartilhada, por exemplo.

Você também verá a seguinte mensagem:

```
The rescue environment will now attempt to find your Red Hat
Linux installation and mount it under the directory
/mnt/sysimage.  You can then make any changes required to your
system.  If you want to proceed with this step choose
'Continue'. You can also choose to mount your file systems
read-only instead of read-write by choosing 'Read-only'.
If for some reason this process fails you can choose 'Skip'
and this step will be skipped and you will go directly to a
command shell.
```

Se você selecionar **Continuar**, tenta montar seu sistema de arquivo sob o diretório `/mnt/sysimage/`. Se falhar em montar a partição, você será avisado. Se você selecionar **Somente-Leitura**, tenta montar seu sistema de arquivo sob o diretório `/mnt/sysimage/`, mas no modo somente-leitura. Se você

1. Consulte o *Guia de Instalação do Red Hat Enterprise Linux* para mais detalhes.

1. Consulte o *Guia de Instalação do Red Hat Enterprise Linux* para mais detalhes.

selecionar **Pular**, seu sistema de arquivo não é montado. Escolha **Pular** se acreditar que seu sistema de arquivo esteja corrompido.

Uma vez que seu sistema está no modo de recuperação, aparece um prompt no CV 1 (console virtual) e no CV 2 (use a combinação das teclas [Ctrl]-[Alt]-[F1] para acessar o CV 1 e [Ctrl]-[Alt]-[F2] para acessar o CV 2):

```
sh-2.05b#
```

Se você selecionou **Continuar** para montar suas partições automaticamente e estas foram montadas com sucesso, você está no modo de usuário simples.

Mesmo que seu sistema de arquivo seja montado, a partição root default é temporária enquanto estiver no modo de recuperação; não é a partição root do sistema de arquivo usada durante o modo normal de usuário (níveis de execução 3 ou 5). Se você escolheu montar seu sistema de arquivo e o fez com sucesso, pode alterar a partição root do ambiente do modo de recuperação para a partição root de seu sistema de arquivo, executando o seguinte comando:

```
chroot /mnt/sysimage
```

Isto é útil se você precisa rodar comandos como `rpm`, que requerem que sua partição root seja montada como `/`. Para sair do ambiente chroot, digite `exit` e você retornará ao prompt.

Se você selecionou **Pular**, ainda pode tentar montar uma partição manualmente dentro do modo de recuperação criando um diretório como */foo*, e digitando o comando a seguir:

```
mount -t ext3 /dev/hda5 /foo
```

No comando acima, */foo* é um diretório que você criou e */dev/hda5* é a partição que você deseja montar. Se a partição for do tipo `ext2`, substitua `ext3` por `ext2`.

Se você não sabe os nomes de suas partições, use o seguinte comando para listá-las:

```
fdisk -l
```

A partir do prompt é possível executar diversos comandos úteis, como

- `list-harddrives` para listar os discos rígidos do sistema
- `ssh`, `scp` e `ping` se a rede for iniciada
- `dump` e `restore` para usuários com drives de fita
- `parted` e `fdisk` para administrar as partições
- `rpm` para instalar ou atualizar (upgrade) software
- `joe` para editar os arquivos de configuração (se você tentar iniciar outros editores populares como o `emacs`, `pico` ou o `vi`, o editor `joe` será iniciado.)

## 11.3. Inicializando no Modo de Usuário Simples

Uma das vantagens do modo de usuário simples é que você não precisa de um disquete ou CD-ROM boot; no entanto, não oferece a opção de montar os sistemas de arquivo como somente-leitura ou de não montá-los.

Se o seu sistema inicializar, mas não permitir a autenticação após completar a inicialização, tente o modo de usuário simples.

No modo de usuário simples, seu computador inicializa no nível de execução 1. Seus sistemas de arquivo locais estão montados, mas sua rede não está ativada. Você tem uma shell de manutenção do

sistema utilizável. Ao contrário do modo de recuperação, o modo de usuário simples tenta montar seu sistema de arquivo automaticamente; *não* use o modo de usuário simples se o seu sistema de arquivo não for montado com sucesso. Você não pode usar o modo de usuário simples se a configuração do nível de execução 1 do seu sistema estiver corrompida.

Em um sistema x86 usando o gestor de início GRUB, use os seguintes passos para inicializar a máquina no modo de usuário simples:

1. Se você tiver uma senha configurada para o GRUB, digite `p` e insira a senha.
2. Selecione o **Red Hat Enterprise Linux** com a versão do kernel na qual você deseja inicializar e digite `a` para adicionar a linha.
3. Vá para o final da linha e digite **`single`** como uma palavra separada (pressione a [Barra de Espaço] e então digite **`single`**). Pressione [Enter] para sair do modo de edição.
4. Voltando à tela do GRUB, digite `b` para inicializar a máquina no modo de usuário simples.

Em um sistema x86 usando o gestor de início LILO, no prompt de início do LILO (se você está usando o LILO gráfico, deve pressionar [Ctrl]-[x] para sair da tela gráfica e ir para o prompt `boot:`) digite:

```
linux single
```

Para todas as outras plataformas, indique **`single`** como um parâmetro do kernel no prompt de início.

## 11.4. Inicializando no Modo de Emergência

No modo de emergência, você inicializa a máquina no ambiente mais básico possível. O sistema de arquivo root é montado como somente-leitura e praticamente nada está configurado. A principal vantagem do modo de emergência sobre o modo de usuário simples é que os arquivos `init` não são carregados. Se `init` estiver corrompido ou não estiver funcionando, ainda é possível montar os sistemas de arquivo para recuperar dados que podem ser perdidos durante uma reinstalação.

Para inicializar a máquina no modo de emergência, use o mesmo método descrito para o modo de usuário simples na Seção 11.3 com uma exceção; substitua a palavra **`single`** por **`emergency`**.

Capítulo 12.

# Configuração do RAID do Software

Primeiramente, leia o Capítulo 3 para aprender sobre o RAID, as diferenças entre RAID de Hardware e de Software e as diferenças entre os RAIDs 0, 1 e 5.

O RAID de software pode ser configurado durante a instalação gráfica do Red Hat Enterprise Linux ou durante uma instalação kickstart. Este capítulo aborda como configurar o RAID de software durante a instalação, usando a interface do **Disco Druid**.

Antes de poder criar um dispositivo RAID, você deve primeiro criar as partições RAID usando as seguntes instruções:

1. Na tela **Configuração do Particionamento de Disco**, selecione **Particionar manualmente com o Disco Druid**.
2. No **Disco Druid**, selecione **Nova** para ciar uma nova partição.
3. Selecione **RAID de software** no menu suspenso **Tipo de Sistema de Arquivo**, conforme mostra a Figura 12-1.

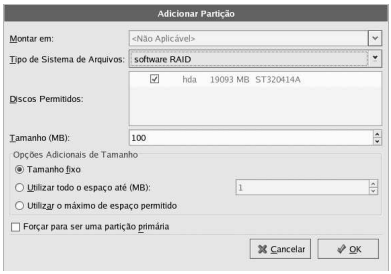


**Figura 12-1. Criando uma Nova Partição RAID**

4. Você não poderá indicar um ponto de montagem (poderá fazê-lo após criar um dispositivo RAID).
5. Uma partição RAID de software deve ser restrita a um disco (drive). Em **Discos Permissíveis**, selecione aquele no qual o RAID será criado. Se você tem discos múltiplos, todos estarão selecionados, e você deve desselecionar todos os discos menos um.
6. Indique o tamanho para a partição.
7. Selecione **Tamanho fixo** para criar a partição do tamanho especificado, selecione **Preencha todo espaço até (MB)** e indique o tamanho em MBs para dar uma escala ao tamanho da partição, ou selecione **Preencha o tamanho máximo permitido** para aumentá-la de modo a preencher todo o espaço disponível no disco rígido. Se você criar mais de uma partição crescente, elas dividirão o espaço disponível no disco.
8. Selecione **Forçar para ser uma partição primária** se você deseja que a partição seja primária.
9. Clique em **OK** para retornar à tela principal.

Repita estes passos para criar todas as partições necessárias para a configuração do seu RAID. Note que as partições não precisam ser todas RAID. Por exemplo: você pode configurar somente a partição `/home` como um dispositivo RAID de software.

Após criar todas as partições como **RAID de software**, siga estes passos:

1. Selecione o botão **RAID** na tela principal de particionamento do **Disco Druid** (veja a Figura 12-4).
2. A Figura 12-2 aparecerá. Selecione **Criar um dispositivo RAID**.

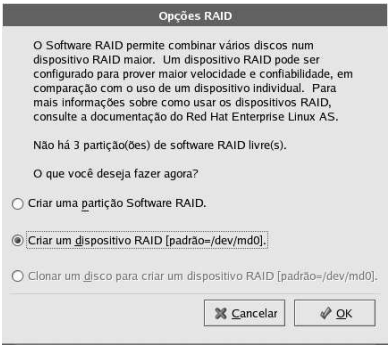


**Figura 12-2. Opções do RAID**

3. Em seguida, a Figura 12-3 aparecerá, onde você pode criar um dispositivo RAID.

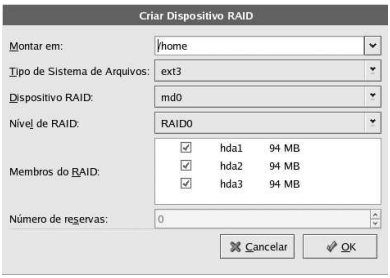


**Figura 12-3. Criando um Dispositivo RAID**

4. Indique um ponto de montagem.
5. Escolha o tipo de sistema de arquivo para a partição.
6. Selecione um nome para o dispositivo RAID como **md0**.
7. Escolha o nível do RAID. Você pode escolher entre **RAID 0**, **RAID 1** e **RAID 5**.

**Nota**

Se você criar uma partição RAID na `/boot`, deve escolher o nível 1 do RAID, e esta deve usar um dos dois primeiros discos (IDE primeiro, SCSI segundo). Se você não criar uma partição RAID na `/boot`, mas criá-la em `/`, deve ter o nível 1 do RAID e usar um dos dois primeiros discos (IDE primeiro, SCSI segundo).

8. As partições RAID recém-criadas aparecem na lista **Membros RAID**. Selecione as partições que devem ser usadas para criar o dispositivo RAID.
9. Se configurar o RAID 1 ou RAID 5, especifique o número de partições avulsas. Se uma partição RAID de software falhar, a avulsa será automaticamente usada como substituta. Para cada partição avulsa, você deve criar uma partição RAID de software adicional (além das partições para o dispositivo RAID). No passo anterior, selecione as partições para o dispositivo RAID e a(s) partição(ões) para a(s) avulsa(s).
10. Após clicar em **OK**, o dispositivo RAID aparecerá na lista **Resumo do Disco**, conforme mostra a Figura 12-4. Neste ponto, você pode continuar seu processo de instalação. Consulte o *Guia de Instalação do Red Hat Enterprise Linux* para mais instruções.


**Figura 12-4. Conjunto RAID Criado**

# Capítulo 13.

# Configuração do LVM

O LVM pode ser configurado durante o processo gráfico de instalação ou durante uma instalação do kickstart. Você pode usar os utilitários do pacote `lvm` para criar a configuração do LVM, mas estas instruções focam no uso do **Disk Druid** durante a instalação para completar esta tarefa.

Primeiramente leia o Capítulo 4 para aprender sobre o LVM. Aqui está uma visão geral dos passos necessários para configurar o LVM:

- Crie *volumes físicos* a partir dos discos rígidos.
- Crie *grupos de volume* a partir dos volumes físicos.
- Crie *volumes lógicos* a partir dos grupos de volume e atribua pontos de montagem aos volumes lógicos.

**NOta**

Você pode editar grupos de volume LVM somente no modo de instalação GUI (gráfico). No modo de instalação texto, pode-se atribuir pontos de montagem aos volumes lógicos existentes.

Para criar um grupo de volume lógico com volumes lógicos durante a instalação:

1. Na tela **Configuração do Particionamento de Disco**, selecione **Particionar manualmente com Disk Druid**.
2. Selecione **Nova**.
3. Selecione **volume físico (LVM)** no menu suspenso **Tipo de Sistema de Arquivo**, conforme mostra a Figura 13-1.

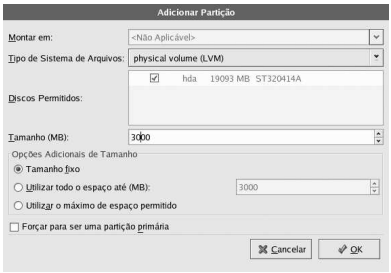


**Figura 13-1. Criando um Volume Físico**

4. Você não poderá indicar um ponto de montagem (somente poderá fazê-lo após criar um grupo de volume).
5. Um volume físico deve ser restrito a um disco. Para **Discos Permitidos**, selecione o disco no qual o volume físico será criado. Se você tem diversos discos (drives), todos eles serão selecionados, e você deve desselecionar todos exceto um.

6. Indique o tamanho desejado para o volume físico.
7. Selecione **Tamanho fixo** para dar ao volume físico o tamanho especificado; selecione **Utilizar todo espaço até (MB)** e indique o tamanho em MB do volume físico, ou selecione **Utilizar o máximo de tamanho permitido** para aumentá-lo ao tamanho total de espaço disponível no disco rígido. Caso você criar mais de um volume crescente, eles dividirão o espaço livre disponível no disco.
8. Selecione **Forçar para ser uma partição primária** se você deseja que a partição seja primária.
9. Clique em **OK** para retornar à tela principal.

Repita este passo para criar quantos volumes físicos foram necessários para a configuração do seu LVM. Por exemplo: se você deseja que o grupo de volume se extenda a mais de um disco, crie um volume fisico em cada um dos discos.

**Atenção**

A partição `/boot` não pode estar em um grupo de volume porque o gestor de início não consegue lê-lo. Se desejar ter sua partição root em um volume lógico, deverá criar uma partição `/boot` separada, que não é parte de um grupo de volume.

Após criar todos os volumes físicos, siga estes passos:

1. Clique no botão **LVM** para juntar os volumes físicos em grupos de volume. Um grupo de volume é basicamente um conjunto de volumes físicos. Você pode ter diversos grupos de volume lógico, mas um volume físico só pode estar em um grupo de volume.

**NOta**

Há espaço excedente em disco reservado no grupo de volume lógico. O somatório dos volumes físicos pode ser diferente do tamanho do grupo de volume; no entanto, o tamanho exibido para os volumes lógicos é correto.

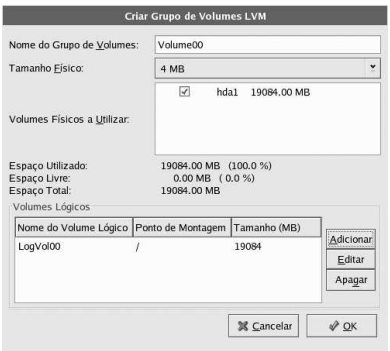


**Figura 13-2. Criando um Dispositivo LVM**

2. Altere o **Nome do Grupo de Volume** se desejar.

3. Todos os volumes lógicos de um grupo de volume devem ser alocados em unidades de *extensão física*. Por default, a extensão física é definida para 4MB, portanto os tamanhos dos volumes lógicos devem ser divisíveis por 4MB. Se você indicar um tamanho que não seja múltiplo de 4MB, o programa de instalação detecta automaticamente o tamanho múltiplo de 4MB mais próximo. Não é recomendado alterar esta configuração.
4. Selecione quais volumes físicos usar para o grupo de volume.
5. Crie volumes lógicos com pontos de montagem como `/home`. Lembre-se que `/boot` não pode ser um volume lógico. Para adicionar um volume lógico, clique no botão **Adicionar** na seção **Volumes Lógicos**. Aparecerá uma janela de diálogo conforme a Figura 13-3 .


**Figura 13-3. Criando um Volume Lógico**

Repita estes passos para cada grupo de volume que deseja criar.

**Dica**

Talvez você queira deixar algum espaço livre no grupo de volume lógico para que possa expandir os volumes lógicos posteriormente.


**Figura 13-4. Volumes Lógicos Criados**

# Capítulo 14.

# Instalações de Rede PXE

O Red Hat Enterprise Linux permite instalações através de uma rede usando os protocolos NFS, FTP ou HTTP. Uma instalação de rede pode ser iniciada a partir de um disquete boot, um CD-ROM boot de rede ou usando a opção boot `askmethod` com o CD 1 do Red Hat Enterprise Linux. Alternativamente, se o sistema a ser instalado contém uma placa de interface de rede (network interface card, NIC) com suporte ao Ambiente de Pré-Execução (Pre-Execution Environment, PXE), pode ser configurdo para inicializar a partir de arquivos em outro sistema da rede, ao invés de um disquete ou CD-ROM.

Para uma instalação de rede PXE, a NIC do cliente com suporte ao PXE envia um pedido de transmissão (broadcast) por informações do DHCP. O servidor DHCP oferece um endereço IP ao cliente, outras informações de rede como servidor de nomes, o endereço IP ou nome da máquina do servidor `tftp` (que oferece os arquivos necessários para iniciar o programa de instalação), e a localidade dos arquivos no servidor `tftp`. Isto é possível por causa do PXELINUX, que é parte do pacote `syslinux`.

Os passos seguintes devem ser executados para preparar uma instalação PXE:

1. Configurar o servidor de rede (NFS, FTP, HTTP) para exportar a árvore de instalação.
2. Configurar os arquivos no servidor `tftp` necessários para a inicialização PXE.
3. Configurar quais máquinas podem inicializar pela configuração PXE.
4. Iniciar o serviço `tftp`.
5. Configurar o DHCP.
6. Inicializar a máquina cliente e começar a instalação.

## 14.1. Configurando o Servidor de Rede

Primeiro, configure um servidor NFS, FTP ou HTTP para exportar a árvore de instalação inteira para a versão e variante do Red Hat Enterprise Linux a ser instalado. Consulte a seção *Preparando para uma Instalação de Rede* do *Guia de Instalação do Red Hat Enterprise Linux* para instruções detalhadas.

## 14.2. Configuração de Inicialização (boot) PXE

O próximo passo é copiar os arquivos necessários para iniciar a instalação para o diretório `tftp` para que possam ser encontrados quando o cliente solicitá-los. O servidor `tftp` é geralmente o mesmo que o servidor de rede exportando a árvore de instalação.

Para copiar estes arquivos, execute a **Ferramenta de Inicialização da Rede** no servidor NFS, FTP ou HTTP. Um servidor PXE separado não é necessário.

Para visualizar estas instruções na versão de linha de comando, consulte a Seção 14.2.1.

Para usar a versão gráfica da **Ferramenta de Inicialização da Rede**, você deve rodar o Sistema X Window, ter privilégios root e ter o pacote RPM `redhat-config-netboot` instalado. Para iniciar a **Ferramenta de Inicialização da Rede** pela área de trabalho, vá para o **Botão do Menu Principal** (no Painel) => **Configurações do Sistema** => **Configurações do Servidor** => **Serviço de Inicialização da Rede**. Ou digite o comando `redhat-config-netboot` em uma janela de comandos (ex.: num **XTerm** ou **Terminal GNOME**).

Se iniciar a **Ferramenta de Inicialização da Rede** pela primeira vez, selecione **Instalação de Rede** no **Primeira vez do Druid**. Caso contrário, selecione **Configurar** => **Instalação de Rede** no menu suspenso e então clique em **Adicionar**. Aparece o diálogo exibido na Figura 14-1.

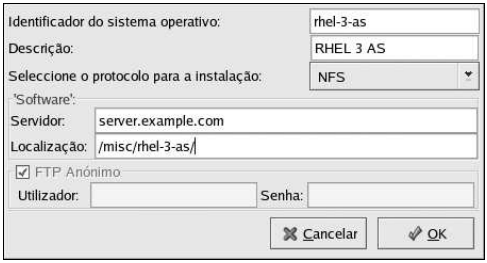


**Figura 14-1. Configuração da Instalação de Rede**

Forneça as seguintes informações:

- **Identificador do sistema operacional** — Indique um nome único usando uma palavra para identificar a versão e variante do Red Hat Enterprise Linux. É usado como o nome do diretório no diretório `/tftpboot/linux-install/`.
- **Descrição** — Indique uma breve descrição da versão e variante do Red Hat Enterprise Linux.
- **Selecionar protocolo para instalação** — Selecione NFS, FTP ou HTTP como o tipo de instalação de rede dependendo de qual foi configurado anteriormente. Se o FTP é selecionado e o FTP anônimo não é usado, desselecione **FTP Anônimo** e indique um nome de usuário e senha válidos.
- **Servidor** — Indique o endereço IP ou nome de domínio do servidor NFS, FTP ou HTTP.
- **Localidade** — Indique o diretório compartilhado pelo servidor de rede. Se selecionou FTP ou HTTP, o diretório deve ser relativo ao diretório default do servidor FTP ou ao documento root do servidor HTTP. Para todas as instalações de rede, o diretório provido deve conter o diretório `RedHat/` da árvore de instalação.

Após clicar em **OK**, os arquivos `initrd.img` e `vmlinuz`, necessários para iniciar o programa de instalação, são transferidos de `images/pxeboot/` na árvore de instalação provida para `/tftpboot/linux-install/<os-identifier>/` no servidor `tftp` (aquele no qual você está rodando a **Ferramenta de Inicialização da Rede**).

### 14.2.1. Configuração pela Linha de Comando

Se o servidor de rede não está rodando o X, o utilitário de linha de comando `pxeos`, parte do pacote `redhat-config-netboot`, pode ser usado para configurar os arquivos do servidor `tftp`, conforme descrito na Seção 14.4:

```
pxeos -a -i "<description>" -p <NFS|HTTP|FTP> -D 0 -s client.example.com \
-L <net-location> <os-identifer>
```

A lista a seguir explica as opções:

- `-a` — Especifica que uma instância do SO está sendo adicionada à configuração do PXE.
- `-i "<description>"` — Substitua "<description>" pela descrição da instância do SO. Isto corresponde ao campo **Descrição** na Figura 14-1.
- `-p <NFS|HTTP|FTP>` — Especifica quais dos protocolos, NFS, FTP ou HTTP usar para a instalação. Somente um deve ser especificado. Isto corresponde ao menu **Selecionar protocolo para a instalação** na Figura 14-1.
- `-D 0` — Indica que não se trata de uma configuração sem disco, já que o `pxeos` pode ser usado para configurar o ambiente sem disco também.

- `-s client.example.com` — Indique o nome do servidor NFS, FTP ou HTTP após a opção `-s`. Isto corresponde ao campo **Servidor** na Figura 14-1.
- `-L <net-location>` — Indique a localidade da árvore de instalação neste servidor após a opção `-L`. Isto corresponde ao campo **Localidade** na Figura 14-1.
- `<os-identifer>` — Especifique o identificador do SO, que é usado como o nome do diretório no diretório `/tftpboot/linux-install/`. Isto corresponde ao campo **Identificador do Sistema Operacional** na Figura 14-1.

Se o FTP é selecionado como o protocolo de instalação e a autenticação anônima não está disponível, especifique um nome de usuário e senha para autenticação, com as seguintes opções antes do `<os-identifer>` no comando anterior:

```
-A 0 -u <username> -p <password>
```

## 14.3. Adicionando Máquinas PXE

Após configurar o servidor de rede, aparece a interface conforme a Figura 14-2.

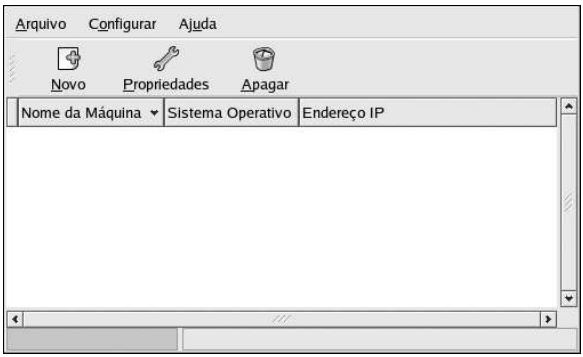


**Figura 14-2. Adicionar Máquinas**

O próximo passo é configurar quais máquinas têm permissão para conectar ao servidor de inicialização PXE. Para a versão de linha de comando deste passo, consulte a Seção 14.3.1.

Para adicionar máquinas, clique no botão **Nova**.

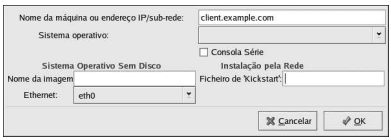


**Figura 14-3. Adicionar uma Máquina**

Indique as seguintes informações:

- **Nome da máquina ou endereço IP/sub-rede** — Indique o endereço IP, o nome completo da máquina ou uma sub-rede de sistemas que devem ter permissão para conectar-se ao servidor PXE para instalações.
- **Sistema Operacional** — Selecione o identificador do sistema operacional a instalar neste cliente. A lista está repleta de instâncias de instalação de rede criadas no **Diálogo de Instalação de Rede**.
- **Console Serial** — Selecione esta opção para usar um console serial.
- **Arquivo Kickstart** — Especifque a localidade de um arquivo kickstart a usar, tal como **`http://server.example.com/kickstart/ks.cfg`**. Este arquivo pode ser criado com a **Configurador do Kickstart**. Consulte o Capítulo 10 para mais detalhes.

Ignore as opções **Nome instantâneo** (Snapshot name) e **Ethernet**. Estas são usadas somente em ambientes em disco.

### 14.3.1. Configuração pela Linha de Comando

Se o servidor de rede não está rodando o X, o utilitário `pxeboot`, parte do pacote `redhat-config-netboot`, pode ser usado para adicionar máquinas com permissão para conectar ao servidor PXE.

```
pxeboot -a -O <os-identifier> -r <value> <host>
```

A lista seguinte descreve as opções:

- `-a` — Especifica que uma máquina deve ser adicionada.
- `-O` <*`os-identifier`*> — Substitua <*`os-identifier`*> pelo identificador do sistema operacional, conforme definido na Seção 14.2.
- `-r` <*`value`*> — Substitua <*`value`*> pelo tamanho do disco ram.
- <*`host`*> — Substitua <*`host`*> pelo endereço IP ou pelo nome da máquina a adicionar.

## 14.4. Iniciando o Servidor `tftp`

No servidor DHCP, verifique se o pacote `tftp-server` está instalado com o comando `rpm -q tftp-server`. Se não está instalado, instale-o através da Red Hat Network ou pelos CDs do Red Hat Enterprise Linux. >>>>>> 1.1.2.4 Para mais informações sobre a instalação dos pacotes RPM, consulte a Parte III.

O `tftp` é um serviço baseado no xinetd; inicie-o com os seguintes comandos:

```
/sbin/chkconfig --level 345 xinetd on
/sbin/chkconfig --level 345 tftp on
```

Este comando configura os serviços `tftp` e `xinetd` para ligarem imediatamente e para iniciarem no momento da inicialização nos níveis de execução (runlevels) 3, 4 e 5.

## 14.5. Configurando o Servidor DHCP

Se um servidor DHCP ainda não existe na rede, configure um. Consulte o Capítulo 25 para mais detalhes. Certifique-se de que o arquivo de configuração contenha o seguinte, para que a inicialização através do PXE seja habilitada para sistemas que o suportam:

```
allow booting;
allow bootp;
class "pxeclients" {
```

```
   match if substring(option vendor-class-identifier, 0, 9) = "PXEClient";
   next-server <server-ip>;
   filename "linux-install/pxelinux.0";
}
```

O endereço IP após a opção `next-server` deve ser o endereço IP do servidor `tftp`.

## 14.6. Adicionando uma Mensagem de Inicialização Personalizada

Opcionalmente, modifique `/tftpboot/linux-install/msgs/boot.msg` para usar uma mensagem de inicialização personalizada.

## 14.7. Executando a Instalação PXE

Para instruções sobre a configuração da placa de interface de rede com suporte ao PXE para inicializar pela rede, consulte a documentação da placa. O processo varia ligeiramente de acordo com a placa.

Após o sistema iniciar o programa de instalação, consulte o *Guia de Instalação do Red Hat Enterprise Linux*.

# Capítulo 15.

# Ambientes Sem Disco

Algumas redes requerem vários sistemas com a mesma configuração. Também é necessário que estes sistemas sejam fáceis de reinicializar, atualizar e administrar. Uma solução é usar um *ambiente sem disco*, no qual a maior parte do sistema operacional (que pode ser somente-leitura) é compartilhada de um servidor central entre os clientes, e os clientes individuais têm seus próprios diretórios no servidor central para o resto do sistema operacional (que deve ser leitura e gravação). Cada vez que o cliente inicializar, monta a maior parte do sistema operacional a partir do servidor NFS como somente-leitura (read-only) e um outro diretório como leitura e gravação (read-write). Cada cliente tem seu próprio diretório leitura e gravação, pois assim um cliente não afeta os outros.

Os passos a seguir são necessários para configurar o Red Hat Enterprise Linux para rodar em um cliente sem disco:

1. Instale o Red Hat Enterprise Linux em um sistema para que os arquivos possam ser copiados no servidor NFS. (Consulte o *Guia de Instalação do Red Hat Enterprise Linux* para mais detalhes.) Todos os software a serem utilizados nos clientes devem ser instalados neste sistema, e o pacote `busybox-anaconda` também deve ser instalado.
2. Crie um diretório no servidor NFS para conter o ambiente sem disco, como `/diskless/i386/RHEL3-AS/`. Por exemplo:
   ```
   mkdir -p /diskless/i386/RHEL3-AS/
   ```
   O diretório é referido como o `diretório sem disco`.
3. Neste diretório, crie um sub-diretório chamado `root/`:
   ```
   mkdir -p /diskless/i386/RHEL3-AS/root/
   ```
4. Copie o Red Hat Enterprise Linux do sistema cliente ao servidor usando o `rsync`. Por exemplo:
   ```
   rsync -a -e ssh installed-system.example.com:/ /diskless/i386/RHEL3-AS/root/
   ```
   A duração desta operação depende da velocidade da conexão de rede, assim como do tamanho do sistema de arquivo no sistema instalado. Pode levar um bom tempo.
5. Inicie o servidor `tftp`, conforme descrito na Seção 15.1.
6. Configure o servidor DHCP, conforme descrito na Seção 15.2.
7. Finalize a criação do ambiente sem disco, conforme descrito na Seção 15.4.
8. Configure os clientes sem disco, conforme descrito na Seção 15.5.
9. Configure cada cliente sem disco para inicializar através do PXE e então inicialize-os.

## 15.1. Inicie o Servidor `tftp`

No servidor DHCP, verifique se o pacote `tftp-server` está instalado com o comando `rpm -q tftp-server`. Se não está instalado, instale-o através da Red Hat Network ou pelos CDs do Red Hat Enterprise Linux. >>>>>> 1.1.2.4 Para mais informações sobre a instalação dos pacotes RPM, consulte a Parte III.

O `tftp` é um serviço baseado no xinetd; inicie-o com os seguintes comandos:

```
/sbin/chkconfig --level 345 xinetd on
/sbin/chkconfig --level 345 tftp on
```

Este comando configura os serviços `tftp` e `xinetd` para ligarem imediatamente e para iniciarem no momento da inicialização nos níveis de execução (runlevels) 3, 4 e 5.

## 15.2. Configurando o Servidor DHCP

Se um servidor DHCP ainda não existe na rede, configure um. Consulte o Capítulo 25 para mais detalhes. Certifique-se de que o arquivo de configuração contenha o seguinte, para que a inicialização através do PXE seja habilitada para sistemas que o suportam:

```
allow booting;
allow bootp;
class "pxeclients" {
   match if substring(option vendor-class-identifier, 0, 9) = "PXEClient";
   next-server <server-ip>;
   filename "linux-install/pxelinux.0";
}
```

O endereço IP após a opção `next-server` deve ser o endereço IP do servidor `tftp`.

## 15.3. Configurando o Servidor NFS

A parte somente-leitura do sistema operacional é compartilhada através do NFS.

Configure o NFS para exportar os diretórios `root/` e `snapshot/`, adicionando-os ao `/etc/exports`. Por exemplo:

```
/diskless/i386/RHEL3-AS/root/     *(ro,sync,no_root_squash)
/diskless/i386/RHEL3-AS/snapshot/ *(rw,sync,no_root_squash)
```

Substitua o `*` por um dos formatos de nome de máquina abordados na Seção 23.3.2. Torne a declaração do nome da máquina o mais específica possível, para que sistemas não quistos não possam acessar a montagem do NFS.

Se o serviço NFS não está rodando, inicie-o:

```
service nfs start
```

Se o serviço NFS já está rodando, recarregue o arquivo de configuração:

```
service nfs reload
```

## 15.4. Finalize a Configuração do Ambiente Sem Disco

Para usar a versão gráfica da **Ferramenta de Inicialização da Rede**, você deve rodar o Sistema X Window, ter privilégios root e ter o pacote RPM `redhat-config-netboot` instalado. Para iniciar a **Ferramenta de Inicialização da Rede** pela área de trabalho, vá para o **Botão do Menu Principal** (no Painel) => **Configurações do Sistema** => **Configurações do Servidor** => **Serviço de Inicialização da Rede**. Ou digite o comando `redhat-config-netboot` em uma janela de comandos (por exemplo, num **XTerm** ou num **terminal GNOME**).

Se for iniciar a **Ferramenta de Inicialização da Rede** pela primeira vez, selecione **Sem disco** em **Primeira vez do Druid**. Caso contrário, selecione **Configurar** => **Sem disco** no menu suspenso e então clique em **Adicionar**.

Aparece um assistente para guiá-lo através do processo:

1. Clique em **Próximo** na primeira página.
2. Na página **Identificador sem disco**, indique um **Nome** e **Descrição** para o ambiente sem disco. Clique em **Próximo**.

3. Indique o endereço IP ou nome do domínio do servidor NFS configurado na Seção 15.3 assim como o diretório exportado como ambiente sem disco. Clique em **Próximo**.
4. As versões do kernel instalado no ambiente sem disco estão listadas. Selecione a versão do kernel para inicializar no sistema sem disco.
5. Clique em **Aplicar** para finalizar a configuração.

Após clicar em **Aplicar**, o kernel sem disco e o arquivo da imagem são criados baseados no kernel selecionado. Estes são copiados no diretório boot do PXE `/tftpboot/linux-install/<os-identifier>/`. O diretório `snapshot/` é criado no mesmo diretório que `root/` (ex.: `/diskless/i386/RHEL3-AS/snapshot/`) com um arquivo chamado `files` dentro dele. Este arquivo contém uma lista de arquivos e diretórios que devem ser leitura e gravação (read/write) para cada sistema sem disco. Não modifique este arquivo. Se precisar adicionar novas entradas à lista, crie um arquivo `files.custom` no mesmo diretório que o arquivo `files` e adicione cada arquivo ou diretório em uma linha separada.

## 15.5. Adicionando Máquinas

Cada cliente sem disco deve ter seu próprio diretório *instantâneo* no servidor NFS que é usado como seu sistema de arquivo leitura e gravação (read/write). A **Ferramenta de Inicialização da Rede** pode ser usada para criar estes diretórios instantâneo.

Após completar estes passos da Seção 15.4, aparece uma janela que permite adicionar máquinas ao ambiente sem disco. Clique no botão **Nova**. No diálogo exibido na Figura 15-1, indique as seguintes informações:

- **Nome da máquina ou Endereço/Sub-rede IP** — Especifique o nome da máquina ou endereço IP de um sistema para adicioná-lo como uma máquina para o ambiente sem disco. Indique uma sub-rede para especificar um grupo de sistemas.
- **Sistema Operacional** — Selecione o ambiente sem disco para a máquina ou sub-rede de máquinas.
- **Console Serial** — Selecione esta caixa para executar uma instalação serial.
- **Nome instantâneo** — Indique o nome de um sub-diretório a ser usado para armazenar todo o conteúdo leitura e gravação (read/write) da máquina.
- **Ethernet** — Selecione o dispositivo Ethernet na máquina a ser usada para montar o ambiente sem disco. Se a máquina tem apenas uma placa Ethernet, selecione **eth0**.

Ignore a opção **Arquivo Kickstart**. É usado somente para instalações PXE.

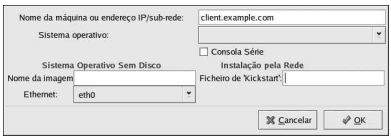


**Figura 15-1. Adicionar Máquina Sem Disco**

No diretório `snapshot/` existente no diretório sem disco, é criado um sub-diretório com o **Nome instantâneo** especificado como o nome do arquivo. Então, todos os arquivos listados no `snapshot/files` e no `snapshot/files.custom` são copiados do diretório `root/` para este novo diretório.

## 15.6. Inicializando as Máquinas

Consulte a documentação da sua placa PXE para configurar a máquina a inicializar através do PXE.

Quando o cliente sem disco inicializar, monta o diretório `root/` no diretório sem disco como somente-leitura (read-only). Também monta seu diretório instantâneo individual como leitura e gravação (read/write). Então, monta todos os arquivos e diretórios nos arquivos `files` e `files.custom` usando o `mount -o bind` sobre o diretório sem disco somente-leitura, para permitir que aplicações gravem no diretório root do ambiente sem disco, caso for preciso.

# III. Administração de Pacotes

Todos softwares de um sistema Red Hat Enterprise Linux estão divididos em pacotes RPM, que podem ser instalados, atualizados (upgrade) ou removidos. Esta parte descreve como administrar os pacotes RPM de um sistema Red Hat Enterprise Linux usando ferramentas gráficas e de linha de comandos.

## Índice

redhat

Capítulo 16.

# Gerenciamento de Pacotes com RPM

O Gestor de Pacotes RPM (RPM) é um sistema de empacotamento aberto, disponível para uso de todos, que roda no Red Hat Enterprise Linux assim como em outros sistemas Linux e UNIX. A Red Hat, Inc. incentiva outros fabricantes a usarem o RPM em seus produtos. O RPM pode ser distribuído sob os termos da GPL.

O RPM facilita as atualizações do sistema para o usuário final. Tarefas como instalar, desinstalar e atualizar os pacotes RPM, podem ser feitas com comandos curtos. O RPM mantém um banco de dados de pacotes instalados e seus arquivos, para que você possa efetuar buscas e verificações poderosas em seu sistema. Se você prefere uma interface gráfica, pode usar a **Ferramenta de Administração de Pacotes** para executar muitos comandos RPM. Consulte o Capítulo 17 para mais detalhes.

Durante as atualizações, o RPM lida cuidadosamente com os arquivos de configuração, para que você nunca perca a personalização — algo impossível de ser feito com arquivos `.tar.gz` normais.

Para o desenvolvedor, o RPM permite levar o código fonte do sotfware e empacotá-lo em uma fonte e pacotes binários para usuários finais. Este processo é bem simples e é iniciado a partir de um arquivo simples e consertos opcionais que você cria. Esta diferenciação clara entre recursos *originais* e seus consertos, junto a instruções para criação (build), facilita a manutenção do pacote conforme o lançamento de novas versões do software.

**Nota**

Como o RPM efetua alterações no seu sistema, você deve estar como root para instalar, remover ou atualizar um pacote RPM.

## 16.1. Objetivos de Desenvolvimento do RPM

Para entender o uso do RPM, pode ser útil entender seus objetivos de desenvolvimento:

Capacidade de Atualização (Upgradability)

Usando o RPM, você pode atualizar componentes individuais de seu sistema sem precisar reinstalá-los completamente. Quando você obtém uma nova versão de um sistema operacional baseado em RPMs (como o Red Hat Enterprise Linux), não precisa reinstalá-lo em sua máquina (como é o caso de sistemas operacionais baseados em outros sistemas de empacotamento). O RPM permite atualizações inteligentes, totalmente automatizadas e certeiras de seu sistema. Os arquivos de configuração dos pacotes são preservados ao longo das atualizações, para que você não perca sua personalização. Não há arquivos especiais necessários para a atualização de um pacote porque o mesmo arquivo RPM é usado para instalar e atualizar o pacote no seu sistema.

Busca (querying) Poderosa

O RPM é desenvolvido para prover opções poderosas de busca. Você pode procurar determinados pacotes ou arquivos no seu banco de dados inteiro. Você também pode descobrir a qual pacote um arquivo pertence e de onde o pacote veio. Os arquivos que o pacote RPM contém estão em um arquivo comprimido, com um cabeçalho binário personalizado contendo informações úteis sobre o pacote e seu conteúdo, permitindo que você procure pacotes individuais fácil e rapidamente.

Verificação do Sistema

Uma outra funcionalidade imporante é a verificação de pacotes. Se você não sabe se apagou algum arquivo importante de algum pacote, verifique-o. Você será notificado de quaisquer anomalias. Neste ponto, você pode reinstalar o pacote se necessário. Todos os arquivos de configuração que você modificou são preservados durante a reinstalação.

Recursos Originais

Um dos objetivos cruciais do desenvolvimento é permitir o uso de recursos "originais" de software, como distribuídos pelos autores originiais do software. Com o RPM, você tem os recursos originais junto a todos os consertos que foram usados, mais as instruções de criação (build). Esta é uma vantagem importante por diversas razões. Por exemplo: se uma nova versão do programa é lançada, você não precisa necessariamente começar do zero para compilá-la. Você pode verificar no conserto o que *deve* fazer. Todos os defaults que fazem parte da compilação e todas as alterações efetuadas para que o software fosse criado apropriadamente são facilmente visíveis através desta técnica.

O objetivo de manter os recursos originais talvez seja importante apenas para desenvolvedores, mas resulta em software de melhor qualidade para usuários finais também. Nós gostaríamos de agradecer aos amigos da distribuição BOGUS por dar origem ao conceito do recurso original.

## 16.2. Usando o RPM

O RPM tem cinco modos de operação básicos (sem contar a compilação de pacotes): instalar, desinstalar, atualizar, buscar e verificar. Esta seção contém uma visão geral de cada modo. Para ver os detalhes e opções completas, invoque `rpm --help`, ou vá para a Seção 16.5 para obter mais informações sobre o RPM.

### 16.2.1. Encontrando Pacotes RPM

Antes de usar um RPM, você deve saber onde encontrá-los. Uma busca na Internet retorna muitos repositórios de RPM, mas se você procura por pacotes RPM compilados pela Red Hat, estes podem ser encontrados nas seguintes localidades:

- Nos CDs do Red Hat Enterprise Linux
- Na Página de Erratas da Red Hat, http://www.redhat.com/apps/support/errata/
- No Site Espelho FTP da Red Hat, na url: http://www.redhat.com/download/mirror.html
- Red Hat Network — Consulte o Capítulo 18 para mais detalhes sobre a Red Hat Network

### 16.2.2. Instalando

Os pacotes RPM geralmente têm nomes de arquivos como `foo-1.0-1.i386.rpm`. O nome do arquivo inclui o nome do pacote (`foo`), versão (`1.0`), sub-versão (`1`) e arquitetura (`i386`). Instalar um pacote é tão simples quanto se autenticar como root e digitar o seguinte em uma janela de comandos:

```
rpm -Uvh foo-1.0-1.i386.rpm
```

Se a instalação for bem-sucedida, o seguinte output é apresentado:

```
Preparing...                ########################################### [100%]
   1:foo                    ########################################### [100%]
```

Como você pode observar, O RPM traz o nome do pacote e então uma sucessão de hífens como medida do progresso, conforme o pacote é instalado.

Iniciando com a versão 4.1 do RPM, a assinatura de um pacote é verificada automaticamente ao instalar ou atualizar um pacote. Se a verificação da assinatura falhar, é apresentada uma mensagem de erro parecida com a seguinte:

```
error: V3 DSA signature: BAD, key ID 0352860f
```

Se a assinatura é nova, somente com cabeçalho, aparece uma mensagem de erro parecida com a seguinte:

```
error: Header V3 DSA signature: BAD, key ID 0352860f
```

Se você não tem a chave apropriada instalada para verificar a assinatura, a mensagem contém a palavra `NOKEY`, tal como:

```
warning: V3 DSA signature: NOKEY, key ID 0352860f
```

Consulte a Seção 16.3 para mais informações sobre a verificação da assinatura de pacotes.

**Nota**

Se você está instalando um pacote do kernel, deve usar o comando `rpm -ivh`. Consulte o Capítulo 39 para mais detalhes.

A instalação de pacotes foi concebida para ser simples, mas você pode encontrar erros em algumas vezes.

#### 16.2.2.1. Pacote Já Instalado

Se o pacote da mesma versão já está instalado, o seguinte é apresentado:

```
Preparing...                ########################################### [100%]
package foo-1.0-1 is already installed
```

Se você deseja instalar o pacote de qualquer maneira e a mesma versão já está instalada, você pode usar a opção `--replacepkgs`, que pede ao RPM para ignorar o erro:

```
rpm -ivh --replacepkgs foo-1.0-1.i386.rpm
```

Esta opção é útil se os arquivos instalados pelo RPM foram apagados ou se você deseja instalar os arquivos originais de configuração pelo RPM.

#### 16.2.2.2. Arquivos Conflitantes

Se você tentar instalar um pacote que contém um arquivo que foi instalado por outro pacote ou por uma versão mais antiga do mesmo pacote, aparece o seguinte:

```
Preparing...                ########################################### [100%]
file /usr/bin/foo from install of foo-1.0-1 conflicts with file from package bar-2.0.20
```

Para fazer com que o RPM ignore este erro, use a opção `--replacefiles`:

```
rpm -ivh --replacefiles foo-1.0-1.i386.rpm
```

#### 16.2.2.3. Dependência Não-resolvida

Os pacotes ROM podem "depender" de outros pacotes, o que significa que eles requerem a instalação de outros pacotes para rodarem apropriadamente. Se você tentar instalar um pacote que tem uma dependência não-resolvida, aparece um output similar ao seguinte:

```
Preparing...                ########################################### [100%]
error: Failed dependencies:
        bar.so.2 is needed by foo-1.0-1
    Suggested resolutions:
        bar-2.0.20-3.i386.rpm
```

Se você instalar um pacote pelos CDs do Red Hat Enterprise Linux, geralmente sugere-se que resolva a dependência do(s) pacote(s). Encontre este pacote nos CDs do Red Hat Enterprise Linux ou pelo site (ou espelho) FTP da Red Hat e adicione-o ao comando:

```
rpm -ivh foo-1.0-1.i386.rpm bar-2.0.20-3.i386.rpm
```

Se a instalação dos dois pacotes for bem-sucedida, aparece um output similar ao seguinte:

```
Preparing...                ########################################### [100%]
   1:foo                    ########################################### [ 50%]
   2:bar                    ########################################### [100%]
```

Se não sugere um pacote para resolver a dependência, você pode tentar a opção `--redhatprovides` para determinar qual pacote contém o arquivo necessário. Você precisa ter o pacote `rpmdb-redhat` instalado para usar estas opções.

```
rpm -q --redhatprovides bar.so.2
```

Se o pacote que contém o `bar.so.2` está no banco de dados instalado pelo pacote `rpmdb-redhat`, o nome do pacote é apresentado:

```
bar-2.0.20-3.i386.rpm
```

Para forçar a instalação de qualquer maneira (uma má idéia já que o pacote provavelmente não rodará corretamente), use a opção `--nodeps`.

### 16.2.3. Desinstalando

Desinstalar um pacote é tão simples quanto instalar um. Digite o seguinte em uma janela de comandos:

```
rpm -e foo
```

**Nota**

Note que usamos o *nome* do pacote `foo` e não o nome do *arquivo* do pacote original `foo-1.0-1.i386.rpm`. Para desinstalar um pacote, substitua `foo` pelo nome verdadeiro do pacote original.

Você pode encontrar um erro de dependência ao desinstalar um pacote, caso um outro pacote instalado dependa daquele que tenta remover. Por exemplo:

```
Preparing...                ########################################### [100%]
error: removing these packages would break dependencies:
        foo is needed by  bar-2.0.20-3.i386.rpm
```

Para fazer com que o RPM ignore este erro e desinstale o pacote de qualquer maneira (o que também é uma má idéia já que o pacote que depende deste provavelmente não funcionará corretamente), use a opção `--nodeps`.

### 16.2.4. Atualizando (upgrade)

Atualizar um pacote é similar a instalar um. Digite o seguinte em uma janela de comandos:

```
rpm -Uvh foo-2.0-1.i386.rpm
```

O que você não vê acima é que o RPM automaticamente desinstalou todas as versões antigas do pacote `foo`. Se quiser, você pode sempre usar `-U` para instalar pacotes, já que funciona mesmo quando não há versões anteriores do pacote instalado.

Como o RPM executa a atualização inteligente de pacotes com arquivos de configuração, você talvez veja uma mensagem como esta:

```
saving /etc/foo.conf as /etc/foo.conf.rpmsave
```

Esta mensagem significa que suas alterações ao arquivo de configuração talvez não sejam "compatíveis"com o novo arquivo de configuração no pacote, portanto o RPM salvou o arquivo original e instalou um novo. Você deve verificar as diferenças entre os dois arquivos de configuração e resolvê-las o quanto antes para garantir o bom funcionamento do seu sistema.

Na realidade, atualizar é uma combinação entre instalar e desinstalar, portanto, durante uma atualização do RPM, você pode encontrar erros de instalação e desinstalação, mais um. Se o RPM acha que você está tentando atualizar para um pacote com uma versão *mais antiga*, o ouput é similar ao seguinte:

```
package foo-2.0-1 (which is newer than foo-1.0-1) is already installed
```

Para fazer com que o RPM "atualize" de qualquer maneira, use a opção `--oldpackage`:

```
rpm -Uvh --oldpackage foo-1.0-1.i386.rpm
```

### 16.2.5. Recarregando

Recarregar um pacote é similar a atualizar um. Digite o seguinte em uma janela de comandos:

```
rpm -Fvh foo-1.2-1.i386.rpm
```

A opção de recarregamento (freshen) do RPM verifica as versões dos pacotes especificados na linha de comando com as versões dos pacotes que já foram instalados no seu sistema. Quando uma versão mais recente de um pacote já instalado é processada pela opção de recarregamento do RPM, é atualizada para a versão mais nova. Entretanto, a opção de recarregamento do RPM não instala um pacote se não houver um outro previamente instalado com o mesmo nome. Isto difere da opção de atualização do RPM, já que a atualização *instala* os pacotes, independente do fato de haver uma versão mais antiga do pacote ou não.

A opção de recarregamento do RPM para pacotes simples ou um grupo de pacotes. Se você fez o download de um grande número de pacotes diferentes e só deseja atualizar os pacotes que já estão instalados no sistema, o recarregamento é a melhor opção. Se usar o recarregamento, não é necessário apagar pacotes não quistos do grupo baixado (download) antes de usar o RPM.

Neste caso, invoque o seguinte comando:

```
rpm -Fvh *.rpm
```

O RPM atualiza automaticamente somente aqueles pacotes que já estão instalados.

### 16.2.6. Busca

Use o comando `rpm -q` para efetuar buscas no banco de dados de pacotes instalados. O comando `rpm -q foo` exibe o nome, versão e sub-versão do pacote instalado foo:

```
foo-2.0-1
```

**Nota**

Note que usamos *nome* do pacote `foo`. Para buscar um pacote, é necessário substituir `foo` pelo nome verdadeiro do pacote.

Ao invés de especificar o nome do pacote, você pode usar as seguintes opções com `-q` para especificar o(s) pacote(s) que deseja buscar. Estas são chamadas *Opções de Especificação de Pacotes*.

- `-a` busca em todos os pacotes atualmente instalados.
- `-f` <*`file`*> busca pelo pacote que detém o <*`file`*>. Ao especificar um arquivo, é necessário indicar a localidade completa do mesmo (ex.: `/usr/bin/ls`).
- `-p` <*`packagefile`*> busca pelo pacote <*`packagefile`*>.

Há diversas maneiras de especificar quais informações devem ser apresentadas sobre os pacotes encontrados. As opções a seguir são usadas para selecionar o tipo de informação pela qual você procura. Estas são chamadas de *Opções de Seleção das Informações*.

- `-i` apresenta as informações do pacote incluindo nome, descrição, versão, tamanho, data de criação, data de instalação, fabricante e outras informações diversas.
- `-l` apresenta a lista dos arquivos contidos no pacote.
- `-s` apresenta o estado de todos os arquivos do pacote.
- `-d` apresenta uma lista dos arquivos marcados como documentação (páginas man, páginas info, READMEs, etc.).
- `-c` apresenta uma lista dos arquivos marcados como arquivos de configuração. Estes são os arquivos que você altera após a instalação para adaptar o pacote ao seu sistema (ex.: `sendmail.cf`, `passwd`, `inittab`, etc.).

Para as opções que apresentam listas de arquivos, você pode adicionar `-v` ao comando para apresentar as listas num formato `ls -l` familiar.

### 16.2.7. Verificando

Verificar um pacote compara as informações sobre os arquivos instalados de um pacote às mesmas informações do pacote original. Dentre outras coisas, a verificação compara o tamanho, soma MD5, permissões, tipo, proprietário (owner) e o grupo de cada arquivo.

O comando `rpm -V` verifica um pacote. Você pode usar qualquer uma das *Opções de Seleção de Pacotes* listadas para a procura, para especificar os pacotes que deseja verificar. Um uso simples da verificação é `rpm -V foo`, que verifica se todos os arquivos do pacote foo estão como estavam quando foram originalmente instalados. Por exemplo:

- Para verificar um pacote contendo um determinado arquivo:
  `rpm -Vf /bin/vi`
- Para verificar TODOS os pacotes instalados:
  `rpm -Va`
- Para verificar um pacote instalado sobre um arquivo do pacote RPM:
  `rpm -Vp foo-1.0-1.i386.rpm`

  Este comando pode ser útil se você suspeitar que seus bancos de dados RPM estejam corrompidos.

Se tudo for verificado apropriadamente, não haverá output. Se houver discrepâncias, estas serão apresentadas. O formato do output é um conjunto de oito caracteres (um `c` denota um arquivo de configuração) e então o nome do arquivo. Cada um dos oito caracteres denota o resultado de uma comparação de um atributo do arquivo ao valor deste mesmo atributo registrado no banco de dados RPM. Um único `.` (ponto) significa que o teste foi aprovado. Os seguintes caracteres denotam a falha de determinados testes:

- `5` — verificação de consistência MD5
- `S` — tamanho do arquivo (size)
- `L` — ligação simbólica
- `T` — hora da modificação do arquivo (time)
- `D` — dispositivo
- `U` — usuário
- `G` — grupo
- `M` — modo (inclui permissões e tipo do arquivo)
- `?` — arquivo ilegível

Se você ver algum output, use seu bom senso para determinar se deve remover ou reinstalar o pacote, ou então consertar o problema de outra maneira.

## 16.3. Verificando a Assinatura de um Pacote

Se você deseja verificar se um pacote foi corrompido ou modificado, examine somente a soma md5 digitando o seguinte comando em uma janela de comandos (<*rpm-file*> pelo nome do arquivo do pacote RPM):

```
rpm -K --nogpg <rpm-file>
```

A mensagem <*rpm-file*>: `md5 OK` á apresentada. Esta breve mensagem significa que o arquivo não foi corrompido pelo download. Para visualizar uma mensagem mais verbalizada, substitua `-K` por `-Kvv` no comando.

Por outro lado, o quão confiável é o desenvolvedor que criou o pacote? Se o pacote é *assinado* com a *chave* GnuPG do desenvolvedor, você sabe que o desenvolvedor é realmente quem ele clama ser.

Um pacote RPM pode ser assinado usando o Gnu Privacy Guard (ou GnuPG), para que você tenha certeza de fazer o download de um pacote confiável.

O GnuPG é uma ferramenta para comunicação segura; é um substituto completo e gratuito da tecnologia de criptografia do PGP, um programa de privacidade eletrônica. Com o GnuPG, você pode autenticar a validade de documentos e criptografar/descriptografar dados de e para outros destinos. O GnuPG também é capaz de descriptografar e verificar arquivos PGP 5.*x*.

Durante a instalação, o GnuPG é instalado por default. Desta maneira, você pode começar a usar o GnuPG imediatamente para verificar todos os pacotes que receber da Red Hat. Primeiro, você precisa importar a chave pública da Red Hat.

### 16.3.1. Importando Chaves

Para verificar os pacotes da Red Hat, você deve importar a chave GPG da Red Hat. Para fazê-lo, execute o seguinte em uma janela de comandos:

```
rpm --import /usr/share/rhn/RPM-GPG-KEY
```

Para exibir uma lista de todas as chaves instaladas para a verificação do RPM, execute o comando:

```
rpm -qa gpg-pubkey*
```

Para a chave da Red Hat, o output inclui:

```
gpg-pubkey-db42a60e-37ea5438
```

Para exibir detalhes sobre uma chave específica, use `rpm -qi` seguido pelo output do comando anterior:

```
rpm -qi gpg-pubkey-db42a60e-37ea5438
```

### 16.3.2. Verificando a Assinatura de Pacotes

Para verificar a assinatura GnuPG de um arquivo RPM após importar a chave GnuPG do criador, use o seguinte comando (substitua <*rpm-file*> pelo nome do arquivo do pacote RPM):

```
rpm -K <rpm-file>
```

Se tudo correr bem, é exibida a seguinte mensagem: `md5 gpg OK`. Isto significa que a assinatura do pacote foi verificada e não está corrompida.

## 16.4. Impressionando Seus Amigos com o RPM

O RPM é útil para administrar seu sistema e para diagnosticar e consertar problemas. A melhor maneira de entender todas as suas opções é dar uma olhada em alguns exemplos.

- Talvez você tenha apagado alguns arquivos por acidente, mas não sabe ao certo o que foi apagado. Para verificar seu sistema inteiro e saber o que pode estar faltando, você pode tentar o seguinte comando:
  `rpm -Va`

Se alguns arquivos estão faltando ou parecem estar corrompidos, você provavelmente deve reinstalar, ou desinstalar o pacote e então reinstalá-lo.

- Em algum ponto, você deve ver um arquivo que não reconhece. Para descobrir a qual pacote pertence, insira o seguinte:
  ```
  rpm -qf /usr/X11R6/bin/ghostview
  ```
  O output será parecido com o seguinte:
  ```
  gv-3.5.8-22
  ```
- Nós podemos combinar os dois exemplos acima no seguinte cenário. Digamos que você tem problemas com `/usr/bin/paste`. Você deseja verificar o pacote que detém este programa, mas não sabe qual pacote detém o `paste`. Simplesmente insira o seguinte comando:
  ```
  rpm -Vf /usr/bin/paste
  ```
  e o pacote apropriado é verificado.
- Você deseja descobrir mais informações sobre um determinado programa? Você pode tentar o seguinte comando para localizar a documentação que acompanha o pacote que detém programa:
  ```
  rpm -qdf /usr/bin/free
  ```
  O output será parecido com o seguinte:
  ```
  /usr/share/doc/procps-2.0.11/BUGS
  /usr/share/doc/procps-2.0.11/NEWS
  /usr/share/doc/procps-2.0.11/TODO
  /usr/share/man/man1/free.1.gz
  /usr/share/man/man1/oldps.1.gz
  /usr/share/man/man1/pgrep.1.gz
  /usr/share/man/man1/pkill.1.gz
  /usr/share/man/man1/ps.1.gz
  /usr/share/man/man1/skill.1.gz
  /usr/share/man/man1/snice.1.gz
  /usr/share/man/man1/tload.1.gz
  /usr/share/man/man1/top.1.gz
  /usr/share/man/man1/uptime.1.gz
  /usr/share/man/man1/w.1.gz
  /usr/share/man/man1/watch.1.gz
  /usr/share/man/man5/sysctl.conf.5.gz
  /usr/share/man/man8/sysctl.8.gz
  /usr/share/man/man8/vmstat.8.gz
  ```
- Você pode encontrar um RPM novo, mas não sabe o que este faz. Para encontrar informações a respeito, use o seguinte comando:
  ```
  rpm -qip crontabs-1.10-5.noarch.rpm
  ```
  O output será parecido com o seguinte:
  ```
  Name        : crontabs                      Relocations: (not relocateable)
  Version     : 1.10                               Vendor: Red Hat, Inc.
  Release     : 5                             Build Date: Fri 07 Feb 2003 04:07:32 PM EST
  Install date: (not installed)               Build Host: porky.devel.redhat.com
  Group       : System Environment/Base       Source RPM: crontabs-1.10-5.src.rpm
  Size        : 1004                             License: Public Domain
  Signature   : DSA/SHA1, Tue 11 Feb 2003 01:46:46 PM EST, Key ID fd372689897da07a
  Packager    : Red Hat, Inc. <http://bugzilla.redhat.com/bugzilla>
  Summary     : Root crontab files used to schedule the execution of programs.
  Description :
  The crontabs package contains root crontab files. Crontab is the
  program used to install, uninstall, or list the tables used to drive the
  cron daemon. The cron daemon checks the crontab files to see when
  particular commands are scheduled to be executed. If commands are
  scheduled, then it executes them.
  ```
- Talvez você queira visualizar quais arquivos o RPM `crontabs` instala. Você deve indicar o seguinte:

```
rpm -qlp crontabs-1.10-5.noarch.rpm
```

O output é similar ao seguinte:

```
Name        : crontabs                     Relocations: (not relocateable)
Version     : 1.10                              Vendor: Red Hat, Inc.
Release     : 5                             Build Date: Fri 07 Feb 2003 04:07:32 PM EST
Install date: (not installed)               Build Host: porky.devel.redhat.com
Group       : System Environment/Base       Source RPM: crontabs-1.10-5.src.rpm
Size        : 1004                             License: Public Domain
Signature   : DSA/SHA1, Tue 11 Feb 2003 01:46:46 PM EST, Key ID fd372689897da07a
Packager    : Red Hat, Inc. <http://bugzilla.redhat.com/bugzilla>
Summary     : Root crontab files used to schedule the execution of programs.
Description :
The crontabs package contains root crontab files. Crontab is the
program used to install, uninstall, or list the tables used to drive the
cron daemon. The cron daemon checks the crontab files to see when
particular commands are scheduled to be executed. If commands are
scheduled, then it executes them.
```

Estes são apenas alguns exemplos. Conforme usá-lo, você descobrirá muitos outros usos para o RPM.

## 16.5. Recursos Adicionais

O RPM é um utilitário extremamente complexo com muitas opções e métodos de busca, instalação, atualização e remoção de pacotes. Consulte os seguintes recursos para aprender mais sobre o RPM.

### 16.5.1. Documentação Instalada

- `rpm --help` — Este comando exibe uma referência rápida dos parâmetros do RPM.
- `man rpm` — A página man do RPM traz mais detalhes sobre seus parâmetros do que o comando `rpm --help`.

### 16.5.2. Sites Úteis

- http://www.rpm.org/ — O site do RPM.
- http://www.redhat.com/mailman/listinfo/rpm-list/ — A lista de discussão do RPM é arquivada aqui. Para assiná-la, envie um e-mail para <`rpm-list-request@redhat.com`> com a palavra `subscribe` no assunto.

### 16.5.3. Livros Relacionados

- *Guia do RPM da Red Hat* por Eric Foster-Johnson; Wiley, John & Sons, Incorporated — Este livro é um guia detalhado do RPM, trazendo informações de instalação de pacotes a compilação de RPMs.

Capítulo 17.

# Ferramenta de Administração de Pacotes

Durante a instalação, um conjunto default de pacotes de software é instalado. Como as pessoas usam seus computadores de diversas maneiras, os usuários talvez queiram remover ou instalar outros pacotes após a instalação. A **Ferramenta de Administração de Pacotes** permite que usuários executem estas ações.

O Sistema X Window é necessário para rodar a **Ferramenta de Administração de Pacotes**. Para iniciar esta aplicação, clique no **Botão do Menu Principal** (no Painel) => **Configurações do Sistema => Adicionar/Remover Aplicações**, ou digite o comando `redhat-config-packages` em uma janela de comandos.

A mesma interface aparece se você inserir o CD 1 do Red Hat Enterprise Linux no seu computador.

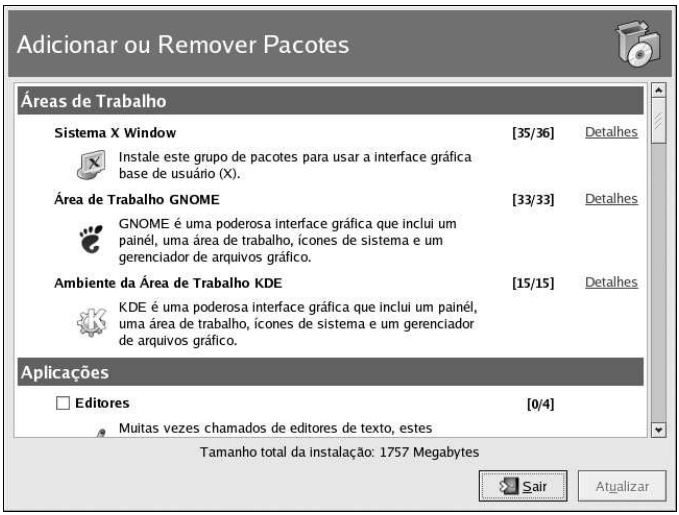


**Figura 17-1. Ferramenta de Administração de Pacotes**

A interface desta aplicação é similar àquela usada para a seleção de pacotes individuais durante a instalação. Os pacotes são divididos em grupos, que contêm uma lista de *pacotes padrão* e *pacotes extras* que compartilham funcionalidades em comum. Por exemplo: o grupo **Internet Grafica** contém um navegador Web, cliente de e-mail e outros programas gráficos usados para conectar à Internet. Os pacotes padrão não podem ser selecionados para remoção, a não ser que o grupo interiro seja removido. Os pacotes extras são opcionais e podem ser instalados ou removidos, desde que o grupo de pacotes seja selecionado.

A janela principal mostra uma lista de grupos de pacotes. Se o grupo de pacotes tiver uma marquinha na caixa de verificação ao seu lado, os pacotes deste grupo estão instalados no momento. Para visualizar a lista de pacotes de um grupo, clique no botão **Detalhes** ao seu lado. Os pacotes com uma marquinha ao seu lado estão instalados no momento.

## 17.1. Instalando Pacotes

Para instalar os pacotes padrão de um grupo não instalado no momento, selecione a caixa de verificação ao seu lado. Para personalizar os pacotes a serem instalados dentro de um grupo, clique no botão **Detalhes** ao seu lado. A lista de pacotes padrão e extras é exibida, conforme a Figura 17-2. Clicar no nome do pacote exibe o espaço necessário em disco para instalá-lo na parte inferior da janela. Ao selecionar a caixa de verificação ao lado do nome do pacote, marca-o para a instalação.

Você também pode selecionar pacotes de grupos já instalados, clicando no botão **Detalhes** e selecionando os pacotes extras que ainda não estão instalados.

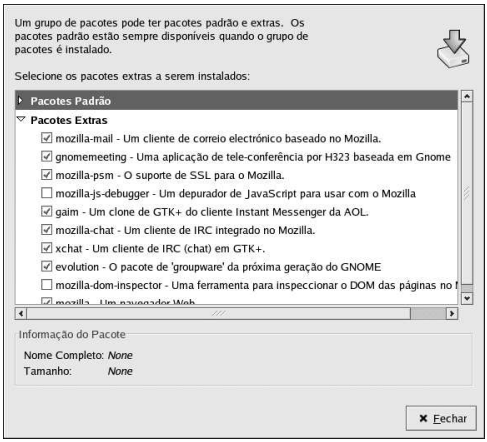


**Figura 17-2. Seleção de Pacotes Individuais**

Após selecionar os grupos de pacotes e pacotes individuais a instalar, clique no botão **Atualizar** na janela principal. O número de pacotes a ser instalado e a quantidade de espaço em disco requerida para instalar os pacotes, assim como quaisquer dependências de pacotes são apresentados em uma janela de sumário. Se houver dependências, estas serão automaticamente adicionadas à lista de pacotes a instalar. Clique no botão **Detalhes** para visualizar a lista completa de pacotes a instalar.

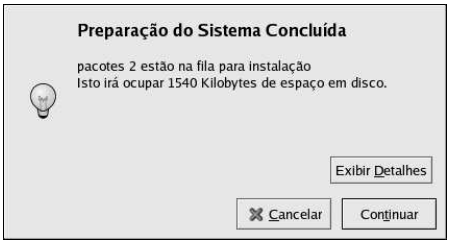


**Figura 17-3. Sumário da Instalação de Pacotes**

Clique em **Continuar** para iniciar o processo de instalação. Ao terminar, aparecerá uma mensagem **Atualização Concluída**.

**Dica**

Se você usar o **Nautilus** para navegar pelos arquivos e diretórios de seu computador, também pode usá-lo para instalar os pacotes. No **Nautilus**, vá para o diretório que contém um pacote RPM (geralmente terminam em `.rpm`) e duplo-clique no ícone RPM.

## 17.2. Removendo Pacotes

Para remover todos os pacotes instalados de um grupo, desselecione a caixa de verificação ao seu lado. Para remover pacotes individuais, clique no botão **Detalhes** ao lado do grupo de pacotes e desselecione os pacotes individualmente.

Quando terminar de selecionar os pacotes a remover, clique no botão **Atualizar** na janela principal. A aplicação computa a quantidade de espaço em disco que será liberada, assim como as dependências de pacote de software. Se outros pacotes dependem dos pacotes que você selecionou para remover, estes serão automaticamente adicionados à lista de pacotes a serem removidos. Clique no botão **Detalhes** para visualizar a lista de pacotes a remover.

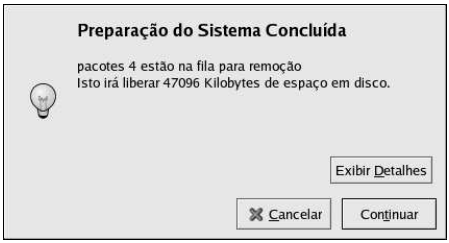


**Figura 17-4. Sumário da Remoção de Pacotes**

Clique em **Continuar** para iniciar o processo de remoção. Quando terminar, aparecerá uma mensagem **Atualização Concluída**.

**Dica**

Você pode combinar a instalação e remoção de pacotes selecionando os pacotes/grupos de pacotes a serem instalados/removidos, e então clicando em **Atualizar**. A janela **Preparação do Sistema Completo** exibirá o número de pacotes a serem instalados e removidos.

# Capítulo 18.

# Red Hat Network

A Red Hat Network é uma solução Internet para administrar um ou mais sistemas Red Hat Enterprise Linux. Todos os Alertas de Segurança, Alertas de Conserto de Erros e Alertas de Melhoria (conhecidos coletivamente como Alertas de Erratas) podem ser baixados (download) diretamente da Red Hat usando a aplicação **Agente de Atualizações Red Hat** ou através do site da RHN, https://rhn.redhat.com/.


**Figura 18-1. Sua RHN**

A Red Hat Network poupa tempo dos usuários porque eles recebem e-mail quando pacotes atualizados são lançados. Os usuários não precisam procurar na Web por pacotes ou alertas de segurança atualizados. Por default, a Red Hat Network instala os pacotes também. Os usuários não precisam aprender a usar o RPM ou se preocupar com a resolução de dependências de pacotes; a RHN faz tudo.

As funcionalidades da Red Hat Network incluem:

- Alertas de Erratas — aprenda quando os Alertas de Segurança, Alertas de Conserto de Erro e Alertas de Melhoria são atribuídos para todos os sistemas da sua rede


**Figura 18-2. Erratas Relevantes**

- Notificações automáticas por e-mail — receba uma notificação por e-mail quando um Alerta de Erratas é atribuído ao seu sistema.
- Atualizações de Erratas Agendadas — entrega agendada de Atualizações de Errata
- Instalação de pacotes — Agende a instalação de pacotes em um ou mais sistemas com o clique de um botão
- **Agente de Atualizações Red Hat** — use a **Agente de Atualizações Red Hat** para baixar (download) os pacotes de software mais recentes para seu sistema (com instalação de pacotes opcionais)
- Site da Red Hat Network — administre sistemas múltiplos, pacotes indiciduais baixados e programe ações como Atualizações de Erratas através de um conexão Web segura de qualquer computador

**Atenção**

Você deve ativar seu produto Red Hat Enterprise Linux antes de registrar seu sistema na Red Hat Network para garantir que usufrua dos serviços corretos. Para ativar seu produto, visite:

```
http://www.redhat.com/apps/activate/
```

Após ativar seu produto, registre-o na Red Hat Network para receber as Atualizações de Erratas. O processo de registro coleta informações sobre o sistema que você deseja receber notificações de atualizações. Por exemplo: uma lista de pacotes instalados no sistema é compilada, de modo que você é notificado apenas das atualizações relevantes para seu sistema.

Na primeira vez que o sistema é inicializado, o **Agente de Configuração** pede que você registre. Se você não registrou neste momento, selecione **Botão do Menu Principal => Ferramentas do Sistema**

=> **Red Hat Network** em sua área de trabalho para iniciar o processo de registro. Alternativamente, execute o comando `up2date` em uma janela de comandos.

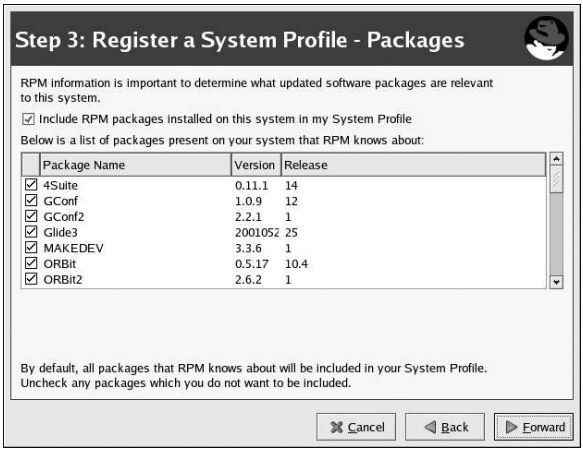


**Figura 18-3. Registrando na RHN**

Após registrar, use um dos métodos a seguir para começar a receber atualizações:

- Selecione **Botão do Menu Principal => Ferramentas do Sistema => Red Hat Network** em sua área de trabalho.
- Execute o comando `up2date` em uma janela de comandos.
- Use o site da RHN: https://rhn.redhat.com/.

Para instruções mais detalhadas, consulte a documentação disponível em:

```
http://www.redhat.com/docs/manuals/RHNetwork/
```

**Dica**

O Red Hat Enterprise Linux inclui a **Ferramenta de Notificação de Alerta da Red Hat Network**, um ícone conveniente do painel que exibe alertas visíveis quando há uma atualização para seu sistema Red Hat Enterprise Linux.

# IV. Configuração Relacionada à Rede

Após explicar como configurar a rede, esta parte aborda tópicos relacionados à rede, como a permissão de autenticações (logins) remotas, o compartilhamento de arquivos e diretórios através da rede, e a configuração de um servidor web.

## Índice

# Capítulo 19.

# Configuração de Rede

Para comunicar com outros computadores, é necessário ter uma conexão de rede. Isto é executado quando um sistema operacional reconhece uma placa de interface (tal como Ethernet, modem ISDN ou 'token ring') e configurando a interface para conectar à rede.

A **Ferramenta de Administração de Rede** pode ser usada para configurar os seguintes tipos de interfaces de rede:

- Ethernet
- ISDN
- modem
- xDSL
- token ring
- CIPE
- dispositivos sem-fio

Também pode ser usada para configurar conexões IPsec, administrar configurações do DNS e administrar o arquivo `/etc/hosts` usado para armazenar combinações adicionais de nomes e endereços IP de máquinas.

Para usar a **Ferramenta de Administração de Rede**, você precisa ter privilégios root. Para iniciar a aplicação, clique no **Botão do Menu Principal** (no Painel) => **Configurações do Sistema** => **Rede**, ou digite o comando `redhat-config-network` em uma janela de comandos (por exemplo: em um **XTerm** ou um **terminal GNOME**). Se você digitar o comando, a versão gráfica é exibida se o X estiver rodando; caso contrário, a versão texto é exibida. Para forçar a versão texto, use o comando `redhat-config-network-tui`.

Para usar a versão de linha de comando, execute o comando `redhat-config-network-cmd --help` como root para visualizar todas as opções.

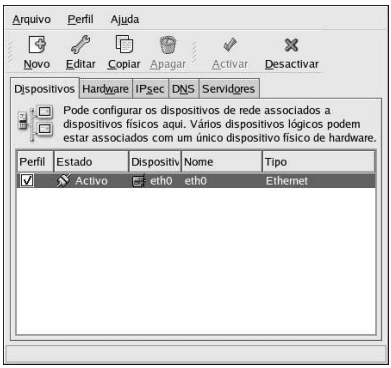


**Figura 19-1. Ferramenta de Administração de Rede**

Se você prefer modificar os arquivos de configuração diretamente, consulte o *Guia de Referência do Red Hat Enterprise Linux* para obter informações sobre suas localizações e conteúdos.

**Dica**

Visite a Lista de Compatibilidade de Hardware da Red Hat (http://hardware.redhat.com/hcl/) para determinar se o Red Hat Enterprise Linux suporta seu dispositivo de hardware.

## 19.1. Visão Geral

Para configurar uma conexão de rede com a **Ferramenta de Administração de Rede**, execute os seguintes passos:

1. Adicione um dispositivo de rede associado ao dispositivo físico de hardware.
2. Adicione o dispositivo físico de hardware à lista de hardware se ainda não existe.
3. Determine as configurações do nome da máquina e do DNS.
4. Configure todas as máquinas que não podem ser encontradas através do DNS.

Este capítulo aborda cada um destes passos para cada tipo de conexão de rede.

## 19.2. Estabelecendo uma Conexão Ehternet

Para estabelecer uma conexão Ethernet, você precisa de uma placa de interface de rede (network interface card, NIC), um cabo de rede (geralmente, um cabo CAT5) e uma rede à qual se conectar. Redes diferentes são configuradas para usar velocidades diferentes de rede; certifique-se de que sua NIC seja compatível com a rede à qual você deseja se conectar.

Para adicionar uma conexão Ethernet, siga estes passos:

1. Clique na aba **Dispositivos**.
2. Clique no botão **Nova** na barra de ferramentas.
3. Selecione **Conexão Ethernet** na lista **Tipo de Dispositivo** e clique em **Próximo**.
4. Se você já adicionou a placa de interface de rede à lista de hardware, selecione-a na lista **Placa Ethernet**. Caso contrário, selecione **Outra Placa Ethernet** para adicionar o dispositivo de hardware.

   

   **Nota**

   O programa de instalação detecta os dispositivos Ethernet suportados e pede que você os configure. Se você configurou algum dispositivo Ethernet durante a instalação, será exibido na lista de hardware, na aba **Hardware**.a

5. Se você selecionou **Outra Placa Ethernet**, aparece a janela **Selecionar Adaptador Ethernet**. Selecione o fabricante e modelo da placa Ethernet. Selecione o nome do dispositivo. Se esta é a primeira placa Ethernet do sistema, selectione **eth0** como o nmome do dispositivo; se é a segunda placa Ethernet, selecione **eth1** e assim por diante. A **Ferramenta de Administração de Rede** também permite configurar os recursos para a NIC. Clique em **Próximo** para continuar.

6. Na janela **Definir Configurações de Rede** (veja a Figura 19-2), escolha entre o DHCP e um endereço IP estático. Se o dispositivo recebe um endereço IP diferente cada vez que a rede é iniciada, não espacifique um nome de máquina. Clique em **Próximo** para continuar.
7. Clique em **Aplicar** na página **Criar Dispositivo Ethernet**.


**Figura 19-2. Configurações da Ethernet**

Após configurar o dispositivo Ethernet, este aparece na lista, conforme mostra a Figura 19-3.

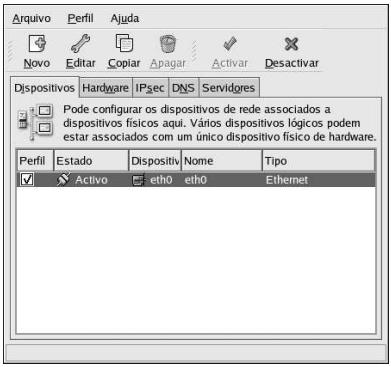


**Figura 19-3. Dispositivo Ethernet**

Certifiuqe-se de selecionar **Arquivo => Salvar** para salvar as alterações.

Após adicionar o dispositivo Ethernet, você pode editar sua configuração selecionando-o na lista de dispositivos e clicando em **Editar**. Por exemplo: quando o dispositivo é adicionado, é configurado para iniciar no momento da inicialização (boot time) por default. Para alterar esta configuração, escolha editar o dispositivo, modifique o valor **Ativar dispositivo quando o computador inicializa** e salve as alterações.

Quando o dispositivo é adicionado, não é ativado imediatamente, conforme visto pelo seu estado **Inativo**. Para ativar o dispositivo, selecione-o da lista e clique no botão **Ativar**. Se o sistema está

configurado para ativar o dispositivo quando computador é iniciailzado (o default), este passo não precisa ser executado novamente.

Se você associar mais de um dispositivo a uma placa Ethernet, os dispositivos subsequentes são *aliases de dispositivos*. Um alias de dispositivo permite configurar múltiplos dispositivos virtuais para um único dispositivo físico, consequentemente atribui mais de um endereço IP ao dispositivo físico. Por exemplo: você pode configurar um dispositivo eth1 e um dispositivo eth1:1. Para mais detalhes, conslute a Seção 19.13.

## 19.3. Estabelecendo uma Conexão ISDN

Um conexão ISDN é uma conexão à Internet, estabelecida com uma placa de modem ISDN, através de uma linha telefônica especial instalada pela companhia telefônica. As conexões ISDN são bem conhecidas na Europa.

Para adicionar uma conexão ISDN, siga estes passos:

1. Clique na aba **Dispositivos**.
2. Clique no botão **Nova** na barra de ferramentas.
3. Selecione **conexão ISDN** na lista **Tipo de Dispositivo** e clique em **Próximo**.
4. Selecione o adaptador ISDN no menu suspenso. Então, configure os recursos e o protocolo do canal D para o adaptador. Clique em **Próximo** para continuar.


**Figura 19-4. Configurações do ISDN**

5. Se o seu Provedor de Serviços de Internet (ISP) está na lista pré-configurada, selecione-o. Caso contrário, insira as informações necessárias sobre sua conta com o ISP. Se você não sabe os valores, contate seu ISP. Clique em **Próximo**.
6. Na janela **Configurações do IP**, selecione **Modo de Encapsulamento** e se deve obter um endereço IP automaticamente ou se deve determiná-lo estaticamente. Clique em **Próximo** quando terminar.
7. Na página **Criar Conexão Discada**, clique em **Aplicar**.

Após configurar o dispositivo ISDN, este aparece na lista como um dispositivo do tipo **ISDN**, conforme a Figura 19-5.

Certifiuqe-se de selecionar **Arquivo => Salvar** para salvar as alterações.

Após adicionar o dispositivo ISDN, você pode editar sua configuração, selecionando-o na lista de dispositivos e clicando em **Editar**. Por exemplo: quando o dispositivo é adicionado, é configurado para

não iniciar no momento da inicialização (boot time) por default. Edite-o para alterar esta configuração. A Compressão, opções PPP, nome de autenticação, senha e outros podem ser alterados.

Quando o dispositivo é adicionado, não é ativado imediatamente, conforme visto pelo seu estado **Inativo**. Para ativar o dispositivo, selecione-o da lista e clique no botão **Ativar**. Se o sistema está configurado para ativar o dispositivo quando computador é iniciailzado (o default), este passo não precisa ser executado novamente.

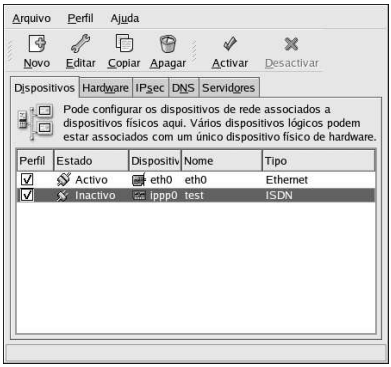


**Figura 19-5. Dispositivo ISDN**

## 19.4. Estabelecendo uma Conexão de Modem

Um modem pode ser usado para configurar uma conexão à Internet através de uma linha telefônica ativa. É necessário ter uma conta de Provedor de Serviços de Internet (ISP), também chamada de conta discada.

Para adicionar uma conexão de modem, siga estes passos:

1. Clique na aba **Dispositivos**.
2. Clique no botão **Nova** na barra de ferramentas.
3. Selecione **Conexão de modem** na lista **Tipo de Dispositivo** e clique em **Próximo**.
4. Se há um modem já configurado na lista de hardware (na aba **Hardware**), a **Ferramenta de Administração de Rede** assume que você deseja usá-lo para estabelecer uma conexão de modem. Se não há modems configurados, ela tenta detectar algum modem no sistema. Esta detecção pode levar algum tempo. Se nenhum modem for encontrado, aparece uma mensagem avisando que os valores exibidos não refletem a detecção.
5. Após a detecção, aparece uma janela igual à Figura 19-6.

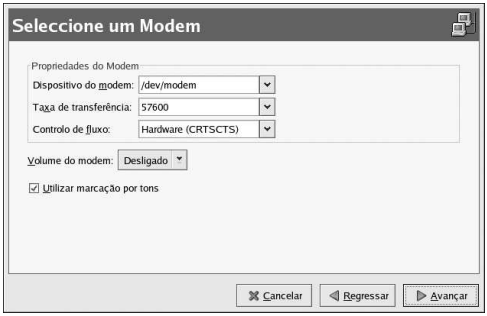


**Figura 19-6. Configurações do Modem**

6. Configure o dispositivo do modem, a taxa de transmissão (baud rate), controle de fluxo, e o volume do modem. Se você não sabe estes valores, aceite os defaults se o modem foi detectado com sucesso. Se você não tem discagem touch tone, desselecione a caixa de verificação correspondente. Clique em **Próximo**.
7. Se o seu ISP esta na lista pré-configurada, selecione-o. Caso contrário, insira as informações necessárias sobre sua conta de ISP. Se você não sabe estes valores, contate seu ISP. Clique em **Próximo**.
8. Na página **Configurações do IP**, selecione se deve obter o endereço IP automaticamente ou se deve determiná-lo estaticamente. Clique em **Próximo** quando terminar.
9. Na página **Criar Conexão Discada**, clique em **Aplicar**.

Após configurar o dispositivo do modem, este aparece na lista de dispositivos com o tipo `Modem`, conforme mostra a Figura 19-7.

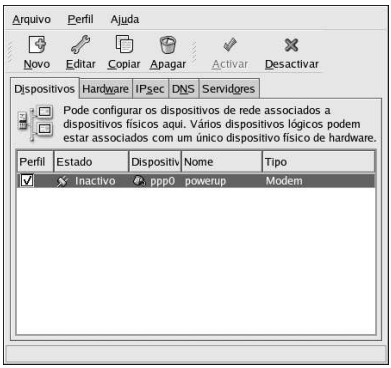


**Figura 19-7. Dispositivo do Modem**

Certifiuqe-se de selecionar **Arquivo => Salvar** para salvar as alterações.

Após adicionar o dispositivo do modem, você pode editar sua configuração selecionando-o na lista e clicando em **Editar**. Por exemplo: quando o dispositivo é adicionado, é configurado para não iniciar no momento da inicialização da máquina (boot time) por default. Edite-o para alterar esta configuração. A Compressão, opções PPP, o nome de autentgicação (login), senha e outros podem ser alterados.

Quando o dispositivo é adicionado, não é ativado imediatamente, conforme visto pelo seu estado **Inativo**. Para ativar o dispositivo, selecione-o da lista e clique no botão **Ativar**. Se o sistema está configurado para ativar o dispositivo quando computador é iniciailzado (o default), este passo não precisa ser executado novamente.

## 19.5. Estabelecendo uma Conexão xDSL

DSL significa Digital Subscriber Lines (Linhas de Assinatura Digital). Há tipos diferentes de DSL, como ADSL, IDSL, e SDSL. A **Ferramenta de Administração de Rede** usa o termo xDSL para referenciar todos os tipos de conexões DSL.

Alguns provedores de conexões DSL requerem que o sistema seja configurado para obter um endereço IP através do DHCP com uma placa Ethernet. Já outros requerem que você configure uma conexão PPPoE (Point-to-Point Protocol over Ethernet, em inglês) com uma placa Ethernet. Pergunte ao seu provedor DSL qual método você deve usar.

Se for necessário usar o DHCP, consulte a Seção 19.2 para configurar sua placa Ethernet.

Se for necessário usar o PPPoE, siga estes passos:

1. Clique na aba **Dispositivos**.
2. Clique no botão **Nova**.
3. Selecione **conexão xDSL** na lista **Tipo de Dispositivo** e clique em **Próximo**.
4. Se a sua placa Ethernet está na lista de hardware, selecione o **Dispositivo Ethernet** no menu suspenso na página exibida na Figura 19-8. Caso contrário, aparece a janela **Selecionar Adaptador Ethernet**.

**Nota**

O programa de instalação detecta os dispositivos Ethernet suportados e pede que você os configure. Se você configurou algum dispositivo Ethernet durante a instalação, será exibido na lista de hardware, na aba **Hardware**.a


**Figura 19-8. Configurações do xDSL**

5. Se aparecer a janela **Selecionar Adaptador Ethernet**, selecione o fabricante e o modelo da placa Ethernet. Selecione o nome do dispositivo. Se esta é a primeira placa Ethernet do sistema, selecione **eth0** como o nome do dispositivo; se for a segunda, selecione **eth1** e assim por diante. A **Ferramenta de Administração de Rede** também permite configurar os recursos para a NIC. Clique em **Próximo** para continuar.
6. Indique o **Nome do Provedor**, **Nome de Login** e **Senha**. Se você tem uma conta T-Online, ao invés de indicar um **Nome de Login** e **Senha** na janela default, clique no botão **Configurar Conta T-Online** e insira as informações necessárias. Clique em **Próximo** para continuar.
7. Na página **Criar Conexão DSL**, clique em **Aplicar**.

Após configurar a conexão DSL, o dispositivo aparece na lista, conforme mostra a Figura 19-7.

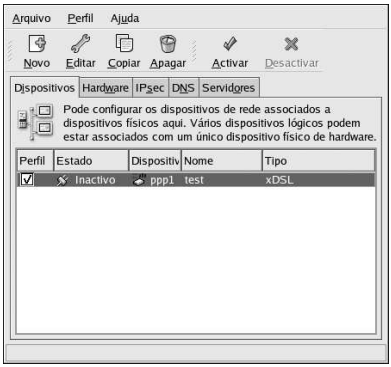


**Figura 19-9. Dispositivo xDSL**

Certifiuqe-se de selecionar **Arquivo => Salvar** para salvar as alterações.

Após adicionar a conexão xDSL, você pode editar sua configuração, seloecionando o dispositivo da lista e clicando em **Editar**. Por exemplo: quando o dispositivo é adicionado, é configurado para não iniciar no momento da inicialização, por default. Edite sua configuração para modificar isto.

Quando o dispositivo é adicionado, não é ativado imediatamente, conforme visto pelo seu estado **Inativo**. Para ativar o dispositivo, selecione-o da lista e clique no botão **Ativar**. Se o sistema está configurado para ativar o dispositivo quando computador é iniciailzado (o default), este passo não precisa ser executado novamente.

## 19.6. Estabelecendo uma Conexão Token Ring

Uma rede token ring é uma rede na qual todos os computadores são conectados num padrão circular. Um *token*, ou um pacote de rede especial, viaja ao redor do token ring e permite a computadores enviar informações uns aos outros.


**Dica**

Para mais informações sobre o uso do token ring sob o Linux, consulte o site do *Linux Token Ring Project* na URL: http://www.linuxtr.net/.

Para adicionar uma conexão token ring, siga estes passos:

1. Clique na aba **Dispositivos**.
2. Clique no botão **Nova** na barra de ferramentas.
3. Selecione **Conexão Token Ring** na lista **Tipo de Dispositivo** e clique em **Próximo**.
4. Se você já adicionou a placa token ring à lista de hardware, selecione-a na lista **Placa Token-ring**. Caso contrário, selecione **Outra Placa Tokenring** para adicionar o dispositivo.
5. Se você selecionou **Outra Placa Tokenring**, aparece a janela **Selecionar Adaptador Token Ring**, conforme a Figura 19-10. Selecione o fabricante e modelo do adaptador. Selecione o nome do dispositivo. Se esta é a primeira placa token ring do sistema, selecione **tr0**; se é a segunda placa token ring, selecione **tr1** (e assim por diante). A **Ferramenta de Administração de Rede** também permite ao usuário configurar os recursos para o adaptador. Clique em **Próximo** para continuar.


**Figura 19-10. Configuração do Token Ring**

6. Na página **Definir Configuração de Rede**, escolha entre o DHCP e o endereço IP estático. Você pode especificar um nome de máquina para o dispositivo. Se o dispositivo recebe um endereço IP dinâmico cada vez que a rede é iniciada, não especifique um nome de máquina. Clique em **Próximo** para continuar.
7. Clique em **Aplicar** na página **Criar Dispositivo Tokenring**.

Após configurar o dispositivo token ring, ele aparece na lista de dispositivos, conforme mostra a Figura 19-11.

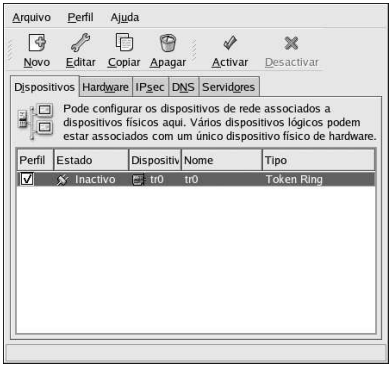


**Figura 19-11. Dispositivo Token Ring**

Certifiuqe-se de selecionar **Arquivo => Salvar** para salvar as alterações.

Após adicionar o dispositivo, você pode editar sua configuração selecionando-o na lista de dispositivos e clicando em **Editar**. Por exemplo: você pode configurar se o dispositivo é iniciado no momento da inicialização da máquina.

Quando o dispositivo é adicionado, não é ativado imediatamente, conforme visto pelo seu estado **Inativo**. Para ativar o dispositivo, selecione-o da lista e clique no botão **Ativar**. Se o sistema está configurado para ativar o dispositivo quando computador é iniciailzado (o default), este passo não precisa ser executado novamente.

## 19.7. Estabelecendo uma Conexão CIPE

CIPE significa 'Crypto IP Encapsulation'. É usado para configurar um dispositivo de transmissão de IP. Por exemplo: o CIPE pode ser usado para conceder acesso do mundo externo para uma VPN (Virtual Private Network). Se você precisa configurar um dispositivo CIPE, contate seu administrador de sistemas para obter os valores corretos.

Para configurar uma conexão CIPE, siga estes passos:

1. Clique na aba **Dispositivos**.
2. Clique no botão **Nova** na barra de ferramentas.
3. Selecione **Conexão CIPE (VPN)** na lista **Tipo de Dispositivo** e clique em **Próximo**.

   Conate seu administrador de sistemas para saber os valores a utilizar.


**Figura 19-12. Configuração do CIPE**

4. Clique em **Aplicar** na página **Criar Conexão CIPE**.

Após configurar o dispositivo CIPE, ele aparece na lista de dispositivos, conforme a Figura 19-13.

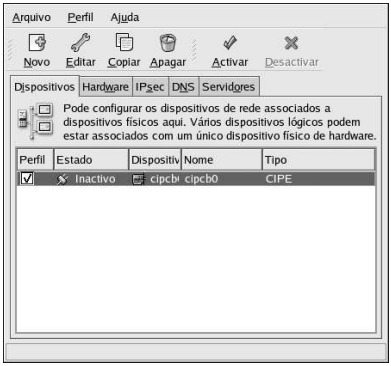


**Figura 19-13. Dispositivo CIPE**

Certifiuqe-se de selecionar **Arquivo => Salvar** para salvar as alterações.

Após adicionar o dispositivo, você pode editar sua configuração selecionando o dispositivo na lista e clicando em **Editar**. Por exemplo: você pode configurar se o dispositivo é iniciado no momento da inicialização da máquina e todas as rotas a utilizar quando o dispositivo é ativado.

Quando o dispositivo é adicionado, não é ativado imediatamente, conforme visto pelo seu estado **Inativo**. Para ativar o dispositivo, selecione-o da lista e clique no botão **Ativar**. Se o sistema está configurado para ativar o dispositivo quando computador é iniciailzado (o default), este passo não precisa ser executado novamente.

**Dica**

Para mais informações sobre o CIPE e sua configuração, consulte o *Guia de Segurança do Red Hat Enterprise Linux*.

## 19.8. Estabelecendo uma Conexão Sem-fio

Os dispositivos Ethernet sem-fio estão tornando-se cada vez mais conhecidos. A configuração é similar à da Ethernet, exceto que permite a você configurar valores como o SSID e chave para o dispositivo sem-fio.

Para adicionar uma conexão Ethernet, siga estes passos:

1. Clique na aba **Dispositivos**.
2. Clique no botão **Nova** na barra de ferramentas.
3. Selecione **Conexão sem-fio** na lista **Tipo de Dispositivo** e clique em **Próximo**.
4. Se você já adicionou a placa de interface de rede sem-fio à lista de hardware, selecione-a na lista **Placa sem-fio**. Caso contrário, selecione **Outra Placa Sem-fio** para adicionar o dispositivo de hardware.

   

   **Nota**

   O programa de instalação geralmente detecta os dispositivos Ethernet sem-fio suportados e pede que você os configure. Se você os configurou durante a instalação, estes são exibidos na lista de hardware da aba **Hardware**.

5. Se você selecionou **Outra Placa Sem-fio**, aparece a janela **Selecionar Adaptador Ethernet**. Selecione o fabricante e modelo da placa Ethernet e do dispositivo. Se esta é a primeira placa Ethernet do sistema, selecione **eth0**; se é a segunda placa Ethernet, selecione **eth1** (e assim por diante). A **Ferramenta de Administração de Rede** também permite ao usuário configurar os recursos da placa de interface de rede sem-fio. Clique em **Próximo** para continuar.
6. Na página **Configurar Conexão Sem-fio**, representada na figura Figura 19-14, configure os valores do dispositivo sem-fio.


**Figura 19-14. Configuração Sem-fio**

7. Na página **Definir Configuração de Rede**, escolha entre o DHCP e o endereço IP estático. Você pode especificar um nome de máquina para o dispositivo. Se o dispositivo recebe um endereço IP dinâmico cada vez que a rede é iniciada, não especifique um nome de máquina. Clique em **Próximo** para continuar.
8. Clique em **Aplicar** na página **Criar Dispositivo Sem-fio**.

Após configurar o dispositivo sem-fio, este aparece na lista de dispositivos, conforme mostra a Figura 19-15.

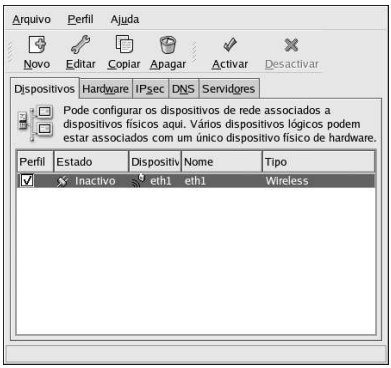


**Figura 19-15. Dispositivo Sem-fio**

Certifiuqe-se de selecionar **Arquivo => Salvar** para salvar as alterações.

Após adicionar o dispositivo sem-fio, você pode editar sua configuração selecionando-o na lista e clicando em **Editar**. Por exemplo: você pode configurar o dispositivo para ser ativado no momento da inicialização da máquina.

Quando o dispositivo é adicionado, não é ativado imediatamente, conforme visto pelo seu estado **Inativo**. Para ativar o dispositivo, selecione-o da lista e clique no botão **Ativar**. Se o sistema está

configurado para ativar o dispositivo quando computador é iniciailzado (o default), este passo não precisa ser executado novamente.

## 19.9. Administrando a Configuração do DNS

A aba **DNS** permite a você configurar o nome da máquina do sistema, domínio, servidores de nome e domínio de busca. Os nomes dos servidores são usados para procurar outras máquinas na rede.

Se os nomes dos servidores DNS são recuperados do DHCP ou PPPoE (ou recuperados do ISP), não adicione servidores DNS primários, secundários ou terciários.

Se o nome da máquina é recuperado dinamicamente do DHCP ou PPPoE (ou recuperado do ISP), não altere-o.


**Figura 19-16. Configuração do DNS**

**Nota**

Os servidores de nome não configuram o sistema para ser um servidor de nome. Ao invés disso, configuram os servidores de nome para serem usados quando resolverem endereços IP para nomes de máquina e vice-versa.

## 19.10. Administrando Máquinas

A aba **Máquinas** permite que você adicione, edite ou remova máquinas do arquivo `/etc/hosts`. Este arquivo contém os endereços IP e os nomes das máquinas correspondentes.

Quando seu sistema tenta resover um nome de máquina para um endereço IP ou determinar o nome da máquina para um endereço IP, consulta o arquivo `/etc/hosts` antes de usar os servidores de nome (se você está usando a configuração default do Red Hat Enterprise Linux). Se o endereço IP está listado no arquivo `/etc/hosts`, os servidores de nome não são usados. Se sua rede contém computadores com endereços IP não listados no DNS, é recomendado que você os adicione ao arquivo `/etc/hosts`.

Para adicionar uma entrada ao arquivo `/etc/hosts`, vá para a aba **Máquinas**, clique no botão **Nova** na barra de ferramentas, indique as informações pedidas e clique em **OK**. Selecione **Arquivo** =>

**Salvar** ou pressione [Ctrl]-[S] para salvar as alterações ao arquivo `/etc/hosts`. A rede ou serviços de rede não precisam ser reiniciados, já que a versão corrente do arquivo é referenciada cada vez que um endereço é resolvido.

**Atenção**

Não remova a entrada `localhost`. Mesmo se o sistema não tiver uma conexão de rede ou tiver uma conexão de rede rodando constantemente, alguns programas precisam conectar-se ao sistema através da interface loopback da máquina local (localhost).

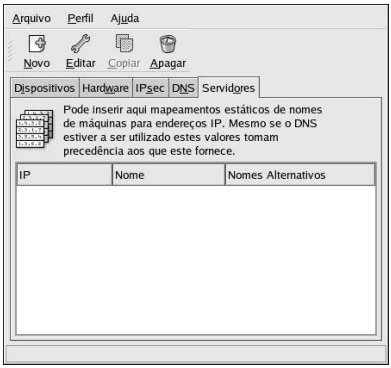


**Figura 19-17. Configuração das Máquinas**

**Dica**

Para alterar a ordem de procura, edite o arquivo `/etc/host.conf`. A linha `order hosts, bind` especifica que o `/etc/hosts` precede os servidores de nome. Alterar a linha para `order bind, hosts` configura o sistema para resolver nomes de máquinas e endereços IP usando primeiro os servidores de nome. Se o endereço IP não pode ser resolvido através dos servidores de nome, então o sistema procura pelo endereço IP no arquivo `/etc/hosts`.

## 19.11. Ativando Dispositivos

Os dispositivos de rede podem ser configurados para estarem ativos ou inativos no momento da inicialização (boot time). Por exemplo: um dispositivo de rede para uma conexão modem geralmente é configurado para ser ativado no momento da inicialização. Se o seu dispositivo de rede está configurado para não iniciar nesta hora, você pode usar o programa de **Controle de Rede Red Hat** para ativá-lo no momento da inicialização. Para tanto, selecione **Botão do Menu Principal** (no Painel) **=> Ferramentas do Sistema => Controle do Dispositivo de Rede** ou digite o comando `redhat-control-network`.

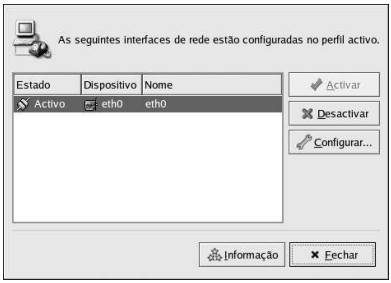


**Figura 19-18. Ativando Dispositivos**

Para ativar um dispositivo, selecione-o na lista e clique no botão **Ativar**. Para parar o dispositivo, selecione-o na lista e clique em **Desativar**.

Se mais de um perfil de rede estiver configurado, estão listados na interface e podem ser ativados. Consulte a Seção 19.12 para mais detalhes.

## 19.12. Trabalhando com Perfis

Diversos dispositivos de rede lógicos podem ser criados para cada dispositivo físico de hardware. Por exemplo: se você tem uma placa Ethernet (eth0) no seu sistema, pode criar dispositivos de rede lógicos com apelidos e opções de configuração diferentes; todos especificamente associados à eth0.

Os dispositivos de rede lógicos são diferentes dos alias dos dispositivos. Os dispositivos de rede lógicos associados ao mesmo dispositivo físico devem existir em perfis diferentes e não podem ser ativados simultaneamente. Os alias dos dispositivos também são associados ao mesmo dispositivo físico, mas podem ser ativados simultaneamente. Consulte a Seção 19.13 para mais detalhes sobre a criação de alias de dispositivos.

Os *perfis* podem ser usados para criar configurações múltiplas para redes diferentes. Uma configuração pode incluir dispositivos lógicos assim como definições de máquinas e DNS. Após configurar os perfis, você pode usar a **Ferramenta de Administração de Rede** para alternar entre eles.

Por default, existe um perfil chamado **Common**. Para criar um novo perfil, selecione **Perfil => Novo** no menu suspenso e indique um nome único para o perfil.

Agora você está modificando o prefil novo, conforme indicado pela barra de estado na parte inferior da janela principal.

Clique num dispositivo já existente na lista, e depois clique no botão **Copiar** para copiar o dispositivo existente para um dispositivo de rede lógico. Se você usar o botão **Novo**, será criado um alias de rede, o que é incorreto. Para alterar as propriedades do dispositivo lógico, selecione-o da lista e clique em **Editar**. Por exemplo: o apelido pode ser alterado para um nome mais descritivo, como **`eth0_office`**, para ser reconhecido mais facilmente.

Na lista de dispositivos, há uma coluna de caixas de verificação nomeadas **Perfil**. Para cada perfil, você pode selecionar ou desselecionar dispositivos. Somente os dispositivos selecionados são inclusos no perfil selecionado. Por exemplo: se você criar um dispositivo lógico chamado **`eth0_office`** em um perfil chamado **`Office`**, e quer ativar o dispositivo lógico se o perfil é selecionado, desselecione o dispositivo `eth0` e selecione o `eth0_office`.

Por exemplo: a Figura 19-19 exibe um perfil chamado **Office** com o dispositivo lógico **eth0_office**. Está configurado para ativar a primeira placa Ethernet usando o DHCP.

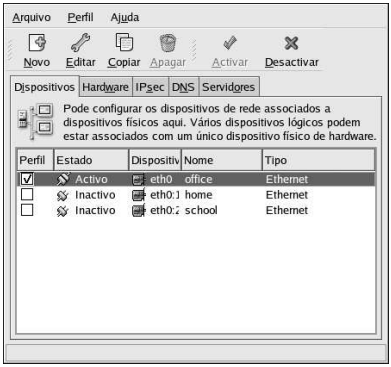


**Figura 19-19. Perfil Office**

Note que o perfil **Home** exibido na Figura 19-20 ativa o dispositivo lógico **eth0_home**, que está associado ao `eth0`.

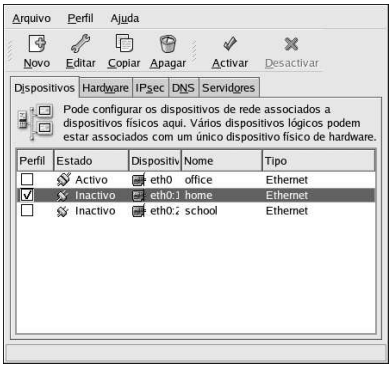


**Figura 19-20. Perfil Home**

Você também pode configurar o `eth0` para ativar no perfil **Office** somente e para ativar um dispositivo ppp (modem) somente no perfil **Home**. Um outro exemplo é ter o perfil **Common** ativar o `eth0` e um perfil **Away** ativar um dispositivo ppp para usar quando viajar.

Para ativar um perfil no momento da inicialização, modifique o arquivo da configuração do gestor de início para incluir a opção `netprofile=<`*`profilename`*`>`. Por exemplo: se o sistema usa o GRUB como gestor de início e o `/boot/grub/grub.conf` contém:

```
title Red Hat Enterprise Linux (2.4.21-1.1931.2.399.ent)
        root (hd0,0)
        kernel /vmlinuz-2.4.21-1.1931.2.399.ent ro root=LABEL=/
        initrd /initrd-2.4.21-1.1931.2.399.ent.img
```

modifque-o para o seguinte (onde <*profilename*> é o nome do perfil a ser ativado no momento da inicialização):

```
title Red Hat Enterprise Linux (2.4.21-1.1931.2.399.ent)
        root (hd0,0)
```

```
kernel /vmlinuz-2.4.21-1.1931.2.399.ent ro root=LABEL=/ netprofile=<profilename>
initrd /initrd-2.4.21-1.1931.2.399.ent.img
```

Para alternar o perfil após inicializar o sistema, vá para o **Menu Principal** (no Painel) => **Ferramentas do Sistema => Controle do Dispositivo de Rede** (ou digite o comando `redhat-control-network`) para selecionar um perfil e ativá-lo. A seção para ativar o perfil aparece somente na interface **Controle do Dispositivo de Rede**, se existir mais do que a interface default **Common**.

Alternativamente, execute o seguinte comando para habilitar um perfil (substitua <*profilename*> pelo nome do perfil):

```
redhat-config-network-cmd --profile <profilename> --activate
```

## 19.13. Alias de Dispositivos

*Alias de Dispositivos* são dispositivos virtuaIs associados ao mesmo hardware físico, mas podem ser ativados ao mesmo tempo para ter endereços IP diferentes. São comumente representados com o nome do dispositivo seguido por dois pontos e um número (ex.: eth0:1). São úteis se você quiser ter diversos endereços IP para um sistema, e o sistema tiver apenas uma placa de rede.

Após configurar o dispositivo Ethernet, como o `eth0`, para usar um endereço IP estático (o DHCP não funciona com alias), vá para a aba **Dispositivos** e clique em **Novo**. Selecione a placa Ethernet para configurar com um alias, determine um endereço IP estático para o alias e clique em **Aplicar** para criá-lo. Como o dispositivo já existe para a placa Ethernet, aquele recém-criado é o alias, como o `eth0:1`.

**Atenção**

Se você está configurando um dispositivo Ethernet para ter um alias, nem o dispositivo nem o alias podem ser configurados para usar DHCP. Você deve configurar os endereços IP manualmente.

A Figura 19-21 mostra um exemplo de um alias para o dispositivo `eth0`. Note o dispositivo `eth0:1` — o primeiro alias para `eth0`. O segundo alias para `eth0` terá o nome do dispositivo `eth0:2`, e assim por diante. Para modificar a configuração do alias do dispositivo, como ativá-lo no momento da inicialização e o número do alias, selecione-o na lista e clique no botão **Editar**.

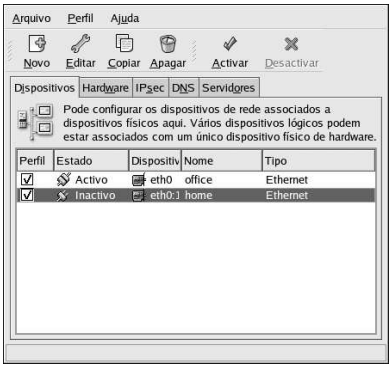


**Figura 19-21. Exemplo de Alias do Dispositivo de Rede**

Selecione o alias e clique no botão **Ativar** para ativar o alias. Se você configurou diversos perfis, selecione em quais perfis incluí-lo.

Para verificar se o alias foi ativado, use o comando `/sbin/ifconfig`. O output deve exibir o dispositivo e o alias do dispositivo com endereço IP diferente:

```
eth0      Link encap:Ethernet  HWaddr 00:A0:CC:60:B7:G4
          inet addr:192.168.100.5  Bcast:192.168.100.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:161930 errors:1 dropped:0 overruns:0 frame:0
          TX packets:244570 errors:0 dropped:0 overruns:0 carrier:0
          collisions:475 txqueuelen:100
          RX bytes:55075551 (52.5 Mb)  TX bytes:178108895 (169.8 Mb)
          Interrupt:10 Base address:0x9000

eth0:1    Link encap:Ethernet  HWaddr 00:A0:CC:60:B7:G4
          inet addr:192.168.100.42  Bcast:192.168.100.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          Interrupt:10 Base address:0x9000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:5998 errors:0 dropped:0 overruns:0 frame:0
          TX packets:5998 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1627579 (1.5 Mb)  TX bytes:1627579 (1.5 Mb)
```

## 19.14. Estabelecendo uma Conexão IPsec

*IPsec* significa *Internet Protocol Security* (Segurança do Protocolo de Internet). É uma solução de Rede Privada Virtual (Virtual Private Network) na qual estabelece-se uma conexão criptografada entre dois sistemas (*máquina-a-máquina*) ou entre duas redes (*rede-a-rede*).

**Dica**

Visite http://www.ipsec-howto.org/ para mais informações sobre a IPsec.

### 19.14.1. Conexão Máquina-a-máquina

Uma conexão IPsec máquina-a-máquina é uma conexão criptografada entre dois sistemas, ambos rodando IPsec com a mesma chave de autenticação. Com a conexão IPsec ativa, qualquer rede entre as duas máquinas é criptografada.

Para configurar uma conexão IPsec máquina-a-máquina, use os seguintes passos para cada máquina:

1. Inicie a **Ferramenta de Administração de Rede**.
2. Na aba **IPsec**, selecione **Nova**.
3. Clique em **Próximo** para começar a configurar a conexão IPsec máquina-a-máquina.
4. Indique um apelido de uma palavra, como **`ipsec0`** para a conexão e selecione se esta deve ser automaticamente ativada quando o computador inicializa. Clique em **Próximo**.
5. Selecione **Criptografia máquina a máquina** como o tipo de conexão. Clique em **Próximo**.

6. Selecione o tipo de criptografia a usar: manual ou automática.

   Se selecionar manual, deverá providenciar uma chave de criptografia posteriormente. Se selecionar automática, o daemon `racoon` é usado para administrar a chave de criptografia. Se o `racoon` é usado, o pacote `ipsec-tools` deve ser instalado.

   Clique em **Próximo** para continuar.

7. Especifique o endereço IP da outra máquina.

   Se você não sabe o endereço IP do outro sistema, execute o comando `/sbin/ifconfig <device>` no outro sistema, onde `<device>` é o dispositivo Ethernet usdao para conectar à outra máquina. Se existe apenas uma placa Ethernet no sistema, o nome do dispositivo é eth0. O endereço IP é o número seguindo a etiqueta `inet addr:`.

   Clique em **Próximo** para continuar.

8. Se a criptografia manual foi selecionada no passo 6, especifique a chave de criptografia a usar ou clique em **Gerar** para criar uma.

   Especifique uma chave de autenticação ou clique em **Gerar** para gerar uma. Pode ser qualquer combinação de números e letras.

   Clique em **Próximo** para continuar.

9. Verifique as informações na página **IPsec — Resumo** e clique em **Aplicar**.

10. Selecione **Arquivo => Salvar** para salvar a configuração.

11. Selecione a conexão IPsec na lista e clique no botão **Ativar**.

12. Repita o processo na outra máquina. É muito importante que as mesmas chaves do passo 8 sejam usadas nas outras máquinas. Caso contrário, a IPsec não fuincionará.

Após configurar a conexão IPsec, esta aparece na lista IPsec, conforme mostra a Figura 19-22.

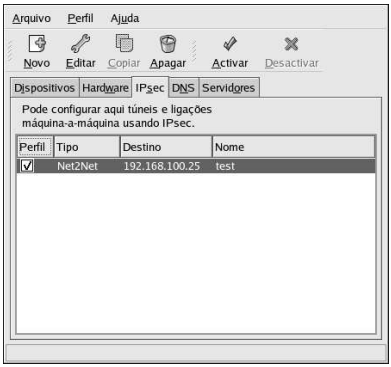


**Figura 19-22. Conexão IPsec**

São criados dois arquivos em `/etc/sysconfig/network-scripts/` — `ifcfg-<nickname>` e `keys-<nickname>`. Se a criptografia automática é selecionada, o `/etc/racoon/racoon.conf` também é criado.

Quando a interface é ativada, `<remote-ip>.conf` e `psk.txt` são criados em `/etc/racoon/`, e `racoon.conf` é modificado para incluir o `<remote-ip>.conf`.

Consulte a Seção 19.14.3 para determinar se a conexão IPsec foi estabelecida com sucesso.

### 19.14.2. Conexão Rede-a-rede (VPN)

Uma conexão IPsec rede-a-rede usa dois roteadores IPsec, um para cada rede, através dos quais o tráfego de rede é roteado para sub-redes privadas.

Por exemplo: conforme a Figura 19-23, se a rede privada 192.168.0/24 deseja enviar tráfego para a rede privada 192.168.2.0/24, os pacotes passam através da porta de comunicação0, para ipsec0; através da Internet, para ipsec1, para porta de comunicação 1 e para a sub-rede 192.168.2.0/24.

Os roteadores IPsec devem ter endereços IP publicamnete endereçáveis, assim como um outro dispositivo Ethernet conectado à sua rede privada. O tráfego passa somente se for endereçado para o outro roteador IPsec, com o qual tem uma conexão criptografada.

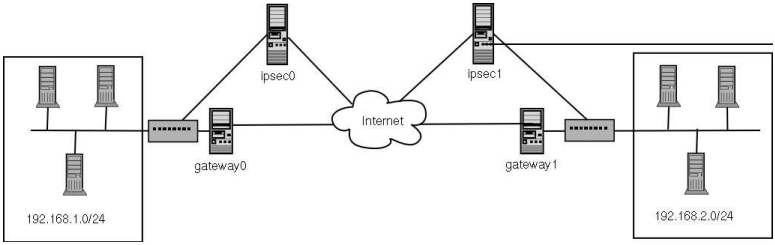


**Figura 19-23. IPsec Rede-a-rede**

Opções alternativas de configuração de rede incluem um firewall entre cada roteador IP e a Internet, e um firewall de Intranet entre cada roteador IPsec e a porta de comunicação da sub-rede. O roteador IPsec e a porta de comunicação da sub-rede podem ser um sistema com dois dispositivos Ethernet, um com um endereço IP público, que atua como o roetador IPsec; e um com um endereço IP privado, que atua como a porta de comunicação da sub-rede privada. Cada roteador IPsec pode usar a porta de comunicação de sua rede privada ou porta de comunicação pública para enviar os pacotes ao outro roteador IPsec.

Para configurar uma conexão IPsec rede-a-rede, siga os seguintes passos:

1. Inicie a **Ferramenta de Administração de Rede**.
2. Na aba **IPsec**, selecione **Nova**.
3. Clique em **Próximo** para começar a configurar a conexão IPsec rede-a-rede.
4. Indique um apelido de uma palavra, como **`ipsec0`** para a conexão e selecione se esta deve ser automaticamente ativada quando o computador inicializa. Clique em **Próximo**.
5. Selecione **Criptografia rede-a-rede (VPN)** e clique em **Próximo**.
6. Selecione o tipo de criptografia a usar: manual ou automática.

   Se você selecionar a manual, deverá providenciar uma chave de criptogafia posteriormente. Se selecionar a automática, o daemon `racoon` é usado para administrar a chave de criptografia. Se usar o `racoon`, o pacote `ipsec-tools` deve ser instalado. Clique em **Próximo** para continuar.
7. Na página **Rede Local**, indique as seguintes informações:
   - **Endereço da Rede Local** — O endereço IP do dispositivo no roteador IPsec conectado à rede privada.
   - **Máscara de Sub-rede Local** — A máscara da sub-rede do endereço IP da rede local.
   - **Porta de Comunicação da Rede Local** — A porta de comunicação da sub-rede privada.

   Clique em **Próximo** para continuar.

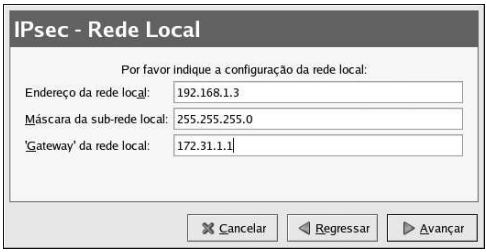


**Figura 19-24. Informações da Rede Local**

8. Na página **Rede Remota**, indique as seguintes informações:

   - **Endereço IP Remoto** — O endereço IP publicamente endereçável do roteador IPsec da *outra* rede privada. Em nosso exemplo, para o ipsec0, indique o endereço IP publicamente endereçável do ipsec1 e vice versa.
   - **Endereço da Rede Remota** — O endereço de rede da sub-rede privada por trás do *outro* roteador IPsec. Em nosso exemplo, indique **`192.168.1.0`** se configurar o ipsec1, e indique **`192.168.2.0`** se for configurar o ipsec0.
   - **Máscara da Sub-rede Remota** — A máscara da sub-rede do endereço IP remoto.
   - **Porta de Comunicação da Rede Remota** — O endereço IP da porta de comunicação do endereço da rede remota.
   - Se a criptografia manual foi selecionada no passo 6, especifique a chave de criptografia a usar ou clique em **Gerar** para criar uma.

     Especifique uma chave de autenticação ou clique em **Gerar** para gerar uma. Pode ser qualquer combinação de números e letras.

   Clique em **Próximo** para continuar.


**Figura 19-25. Informações da Rede Remota**

9. Verifique as informações na página **IPsec — Resumo** e clique em **Aplicar**.
10. Selecione **Arquivo => Salvar** para salvar a configuração.
11. Selecione a conexão IPsec na lista e clique no botão **Ativar**.
12. Como root, em uma janela de comandos, habilite o encaminhamento do IP:

    a. Edite `/etc/sysctl.conf` e defina `net.ipv4.ip_forward` para **`1`**.

    b. Execute o seguinte comando para habilitar a alteração:

```
sysctl -p /etc/sysctl.conf
```

O script de rede para ativar a conexão IPsec cria automaticamente rotas de rede para enviar pacotes através do roteador IPsec, se necessário.

Consulte a Seção 19.14.3 para determinar se a conexão IPsec foi estabelecida com sucesso.

### 19.14.3. Testando a Conexão IPsec

Use o utilitário `tcpdump` para visualizar os pacotes de rede sendo transferidos entre as máquinas (ou redes) e verifique se estão criptografados via IPsec. O pacote deve incluir um cabeçalho AH e deve ser exibido como pacotes ESP. ESP significa que está criptografado. Por exemplo:

```
17:13:20.617872 pinky.example.com > ijin.example.com: \
     AH(spi=0x0aaa749f,seq=0x335): ESP(spi=0x0ec0441e,seq=0x335) (DF)
```

### 19.14.4. Iniciando e Parando a Conexão

Se a conexão IPsec não foi configurada para ativar no momento da inicialização, inicie-a e páre-a, como root, através da linha de comandos.

Para iniciar a conexão, execute o seguinte comando, como root, em cada máquina para o IPsec máquina-a-máquina ou em cada roteador IPsec para o IPsec rede-a-rede (substitua <*ipsec-nick*> pelo apelido de uma palavra configurado anteriormente, tal como `ipsec0`):

```
/sbin/ifup <ipsec-nick>
```

Para parar a conexão, execute o seguinte comando, como root, em cada máquina para o IPsec máquina-a-máquina ou em cada roteador IPsec para o IPsec rede-a-rede (substitua <*ipsec-nick*> pelo apelido de uma palavra configurado anteriormente, tal como `ipsec0`):

```
/sbin/ifdown <ipsec-nick>
```

## 19.15. Salvando e Restaurando a Configuração de Rede

A versão de linha de comando da **Ferramenta de Administração de Rede** pode ser usada para salvar a configuração de rede do sistema em um arquivo. Este arquivo pode, então, ser usado para restaurar a configuração da rede para um sistema Red Hat Enterprise Linux.

Esta funcionalidade pode ser usada como parte de um script de backup automatizado para salvar a configuração antes de atualizar (upgrading) ou reinstalar, ou para copiar a configuração para um sistema Red Hat Enterprise Linux diferente.

Para salvar, ou *exportar*, a configuration de rede do sistema para o arquivo `/tmp/network-config`, execute o seguinte comando como root:

```
redhat-config-network-cmd -e > /tmp/network-config
```

Para restaurar, ou *importar*, a configuração de rede pelo arquivo criado no comando anterior, execute o seguinte comando como root:

```
redhat-config-network-cmd -i -c -f /tmp/network-config
```

A opção `-i` significa importar os dados; a opção `-c` pede para limpar a configuração existente antes de importar; e a opção `-f` especifica que o arquivo a importar é o que vem a seguir.

Capítulo 20.

# Configuração do Firewall Básico

Assim como uma parede de incêndio de um prédio tenta evitar que um incêndio se alastre, um firewall de computador tenta evitar que vírus se espalhem em seu computador e evita que usuários não-autorizados acessem seu computador. Um firewall reside entre seu computador e a rede. Determina quais serviços de seu computador os usuários remotos da rede podem acessar. Um firewall configurado apropriadamente pode aumentar enormemente a segurança de seu sistema. É recomendado que você configure um firewall para todos os sistemas Red Hat Enterprise Linux com uma conexão à Internet.

## 20.1. Ferramenta de Configuração do Nível de Segurança

Na tela **Configuração do Firewall** da instalação do Red Hat Enterprise Linux, você tem a opção de habilitar um firewall básico assim como permitir dispositivos específicos, entrada de serviços e portas.

Após a instalação, você pode alterar esta preferência usando a **Ferramenta de Configuração do Nível de Segurança**.

Para iniciar a aplicação, selecione **Botão do Menu Principal** (no Painel) => **Configurações do Sistema => Nível de Segurança** ou digite o comando `redhat-config-securitylevel` em uma janela de comandos (em um XTerm ou terminal do GNOME, por exemplo).


**Figura 20-1. Ferramenta de Configuração do Nível de Segurança**

**Nota**

A **Ferramenta de Configuração do Nível de Segurança** configura somente um firewall básico. Se o sistema precisa permitir ou negar acesso a portas específicas ou se precisa de regras mais complexas, consulte o *Guia de Referência do Red Hat Enterprise Linux* para detalhes sobre a configuração de regras `iptables` específicas.

Selecione uma das opções seguintes:

- **Desabilitar firewall** — Desabilitar o firewall oferece acesso completo ao seu sistema sem verificação de segurança. A verificação de segurança é a desabilitação do acesso a determinados serviços. Isto dever ser selecionado apenas se você estiver conectado a uma rede confiável (não à Internet) ou planeja configurar o firewall posteriormente.

  
  **Aviso**

  Se você tem um firewall configurado ou quaisquer regras personalizadas de firewall no arquivo `/etc/sysconfig/iptables`, o arquivo será apagado caso você selecionar **Desabilitar Firewall** e então clicar no botão **OK** para salvar as alterações.

- **Habilitar firewall** — Esta opção configura o sistema para rejeitar conexões de entrada que não venham como resposta a pedidos para fora, como respostas DNS e pedidos DHCP. Se precisar de acesso aos serviços rodando nesta máquina, você pode optar por permitir serviços específicos através do firerwall.

  Se você estiver conectando seu sistema à Internet, mas não planeja rodar um servidor, esta é a solução mais segura.

  Selecionar qualquer um dos **Dispositivos Confiáveis** permite o acesso de todo o tráfego deste dispositivo ao seu sistema, ficando excluído das regras de firewall. Por exemplo: se você rodar uma rede local, mas está conectado à Internet através de uma conexão discada PPP, pode selecionar a **eth0** e todo o tráfego proveniente de sua rede local será permitido. Selecionar a **eth0** como um meio confiável significa que todo o tráfego através da Ethernet é permitido, mas a interface ppp0 ainda está protegida pelo firewall. Para restringir o tráfego em uma interface, deixe-a desselecionada.

  Não é recomendado tornar qualquer dispositivo conectado a redes públicas, (como a Internet) num **Dispositivo Confiável**.

  Habilitar serviços da lista **Serviços Confiáveis** permite que este passe através do firewall.

  **WWW (HTTP)**

  O protocolo HTTP é usado pelo Apache (e por outros servidores web) para oferecer páginas web. Se você planeja tornar seu servidor web publicamente disponível, habilite esta opção. Esta opção não é necessária para visualizar páginas localmente ou para desenvolver páginas web. Você deve ter o pacote `httpd` instalado para oferecer páginas web.

  Habilitar o **WWW (HTTP)** não abrirá uma porta para o HTTPS, o servidor SSL de HTTP.

  **FTP**

  O protocolo FTP é usado para transferir arquivos entre máquinas em uma rede. Se você planeja tornar seu servidor FTP publicamente disponível, habilite esta opção. O pacote `vsftpd` deve estar instalado para que esta opção seja útil.

  **SSH**

  Secure Shell (SSH) é um conjunto de ferramentas para autenticação e execução de comandos em uma máquina remota. Para permitir o acesso remoto à máquina através do ssh, habilite esta opção. O pacote `openssh-server` deve ser instalado para poder acessar sua máquina remotamente usando as ferramentas SSH.

  **Telnet**

  Telnet é um protocolo para autenticação em máquinas remotas. As comunicações do Telnet não são criptografadas e não oferecem proteção contra snooping de rede. Não é recomendado permitir a entrada de serviços Telnet. Mas, se quiser fazê-lo, você deve ter o pacote `telnet-server` instalado.

**Correio (SMTP)**

Para permitir a entrada de correspondência através de seu firewall, para que máquinas remotas possam conectar-se à sua e entregar correspondência, habilite esta opção. Caso você receba sua correspondência através do servidor de seu ISP usando POP3 ou IMAP, ou se você usa uma ferramenta como o `fetchmail`, não é necessário habilitar esta opção. Perceba que um servidor SMTP mal configurado pode permitir que máquinas remotas utilizem seu servidor para enviar spam.

Clique em **OK** para salvar as alterações e para habilitar ou desabilitar o firewall. Se **Habilitar firewall** estava selecionada, as opções selecionadas são traduzidas para comandos do `iptables` e salvas no arquivo `/etc/sysconfig/iptables`. O serviço `iptables` também é iniciado para que o firewall seja ativado imediatamente após salvar as opções selecionadas. Se **Desabilitar firewall** estava selecionada, o arquivo `/etc/sysconfig/iptables` é removido e o serviço `iptables` é parado imediatamente.

As opções selecionadas também são salvas no arquivo `/etc/sysconfig/redhat-config-securitylevel` para que a configuração seja armazenada para a próxima vez que a aplicação for iniciada. Não edite este arquivo manualmente.

Apesar do firewall ser ativado imediatamente, o serviço `iptables` não está configurado para iniciar no momento da incialização da máquina. Consulte a Seção 20.2 para mais detalhes.

## 20.2. Ativando o Serviço `iptables`

As regras de firewall tornam-se ativas somente se o serviço `iptables` estiver rodando. Para iniciar o serviço manualmente, use o comando:

```
/sbin/service iptables restart
```

Para garantir que seja iniciado quando o sistema é inicializado, submeta o comando:

```
/sbin/chkconfig --level 345 iptables on
```

O serviço `ipchains` não está incluso no Red Hat Enterprise Linux. No entanto, se o `ipchains` é instalado (por exemplo: foi executada uma atualização e o sistema já tinha o `ipchains` instalado anteriormente) o serviço `ipchains` não deve ser ativado junto ao serviço `iptables`. Para garantir que o serviço `ipchains` esteja desabilitado e configurado para não iniciar no momento da inicialização da máquina, execute os dois comandos a seguir:

```
/sbin/service ipchains stop
/sbin/chkconfig --level 345 ipchains off
```

A **Ferramenta de Configuração dos Serviços** pode ser usada para habilitar ou desabilitar os serviços `iptables` e `ipchains`.

redhat

Capítulo 21.

# Controlando Acesso aos Serviços

Manter a segurança em seu sistema é extremamente importante. Uma forma de lidar com a segurança de seu sistema é gerenciar cuidadosamente o acesso aos serviços do sistema. Seu sistema pode precisar de acesso aberto a determinados serviços (por exemplo: `httpd` se você estiver rodando um servidor Web). No entanto, se você não precisa oferecer um serviço, deve desligá-lo para minimizar sua exposição a possíveis exploits.

Há diversos métodos diferentes para gerenciar o acesso aos serviços do sistema. Decida qual método utilizar baseado no serviço, na configuração de seu sistema e no seu nível de conhecimento do Linux.

A maneira mais fácil de proibir acesso a um serviço é desligá-lo. Tanto os serviços gerenciados pelo `xinetd` (abordados posteriormente nesta seção) quanto os serviços da hierarquia `/etc/rc.d/init.d` (também conhecidos como serviços SysV) podem ser configurados para iniciar e parar usando três aplicações diferentes:

- **Ferramenta de Configuração dos Serviços** — uma aplicação gráfica que exibe a descrição de cada serviço. Mostra se cada serviço é iniciado no momento da inicialização da máquina (para níveis de execução 3, 4 e 5), e permite que os serviços sejam iniciados, parados ou reiniciados.
- **ntsysv** — uma aplicação baseada em texto que permite a você configurar quais serviços são iniciados no momento da inicialização da máquina para cada nível de execução (runlevel). As alterações não têm efeito imediato para serviços não-`xinetd`. Os serviços não-`xinetd` não podem ser iniciados, parados ou reiniciados usando este programa.
- `chkconfig` — um utilitário de linha de comando que permite a você ligar e desligar serviços para níveis de execução diferentes. As alterações não têm efeito imediato nos servcos não-`xinetd`. Os serviços não-`xinetd` não podem ser iniciados, parados ou reiniciados usando este programa.

Talvez você ache que estas ferramentas sejam mais fácies de usar do que as alternativas — editar manualmente as numerosas ligações simbólicas localizadas nos diretórios abaixo de `/etc/rc.d` ou editar os arquivos de configuração `xinetd` em `/etc/xinetd.d`.

Outra maneira de gerenciar o acesso aos serviços do sistema é usar o `iptables` para configurar um firewall IP. Se você for um novo usuário do Linunx, por favor note que o `iptables` talvez não seja a melhor solução para você. Configurar o `iptables` pode ser complicado e é melhor resolvido por administradores de sistemas Linux experientes.

Por outro lado, o benefício de utilizar o `iptables` é sua flexibilidade. Por exemplo: se você precisa de uma solução personalizada com a possibilidade de determinadas máquinas acessarem determinados serviços, o `iptables` pode oferecer isso. Consulte o *Guia de Referência do Red Hat Enterprise Linux* e o *Guia de Segurança do Red Hat Enterprise Linux* para mais informações sobre o `iptables`.

Alternativamente, se você procura uma ferramenta para definir regras gerais de acesso para seu computador pessoal e/ou se você for um novo usuário do Linux, experimente a **Ferramenta de Configuração do Nível de Segurança** (`redhat-config-securitylevel`). Ela permite selecionar o nível de segurança de seu sistema, similar à tela da **Configuração do Firewall** no programa de instalação.

Consulte o Capítulo 20 para mais informações. Se você precisar de regras de firewall mais específicas, consulte o capítulo `iptables` no *Guia de Referência do Red Hat Enterprise Linux.*

## 21.1. Níveis de Execução (Runlevels)

Antes de você configurar o acesso aos serviços, deve entender os níveis de execução do Linux. Um nível de execução é um estado ou um *modo*, que é definido pelos serviços listados no diretório `/etc/rc.d/rc<x>.d`, onde <x> é o número do nível de execução.

Os níveis de execução são os seguintes:

- 0 — Halt
- 1 — Modo de usuário simples
- 2 — Não usado (definível pelo usuário)
- 3 — Modo de multi-usuário
- 4 — Não usado (definível pelo usuário)
- 5 — Modo de multi-usuário (com uma tela gráfica de login)
- 6 — Reinicializar

Se você usar uma tela texto de login, está operando no nível de execução 3. Se você usar uma tela gráfica de login, está operando no nível de execução 5.

O nível de execução default pode ser alterado modificando o arquivo `/etc/inittab`, que contém uma linha próxima ao topo parecida com a seguinte:

```
id:5:initdefault:
```

Altere o número nesta linha para o nível de execução desejado. A alteração não terá efeito até que você reinicialize o sistema.

Para alterar o nível de execução imediatamente, use o comando `telinit` seguido do número do nível de execução. Você deve estar como root para usar este comando. O comando `telinit` não altera o arquivo `/etc/inittab`, somente o nível de execução rodando no momento. Quando o sistema for reinicializado, o nível de execução será aquele especificado em `/etc/inittab`.

## 21.2. TCP Wrappers

Muitos administradores de sistemas UNIX são acostumados a usar o TCP wrappers para gerenciar acesso a determinados serviços de rede. Quaisquer serviços de rede gerenciados pelo `xinetd` (assim como qualquer programa com suporte embutido para o `libwrap`) podem usar o TCP wrappers para gerenciar o acesso. O `xinetd` pode usar os arquivos `/etc/hosts.allow` e `/etc/hosts.deny` para configurar o acesso aos serviços do sistema. Como os nomes implicam, `hosts.allow` contém uma lista de regras que permitem a clientes acessarem os serviços de rede controlados pelo `xinetd`; e `hosts.deny` contém regras para negar acesso. O arquivo `hosts.allow` impõe-se sobre o `hosts.deny`. As permissões para oferecer e negar acesso podem ser baseadas nos endereços IP individuais (ou nomes das máquinas) ou em um padrão de clientes. Consulte o *Guia de Referência do Red Hat Enterprise Linux* e o arquivo `hosts_access` na seção 5 das páginas man (`man 5 hosts_access`) para mais detalhes.

### 21.2.1. `xinetd`

Para controlar o acesso a serviços de Internet use o `xinetd`, que é uma substituição segura para o `inetd`. O daemon do `xinetd` conserva so recursos do sistema, oferece controle de acesso e autenticação, e pode ser usado para iniciar servidores com propósitos especiais. O `xinetd` pode ser usado para oferecer acesso a determinadas máquinas apenas, para negar acesso a determinadas máquinas, para oferecer acesso a um determinado serviço em horários específicos, para limitar a taxa de conexões de entrada (incoming) e/ou limitar a carga criada pelas conexões, dentre outras funções.

O `xinetd` roda constantemente e escuta os serviços que gerencia em todas as portas. Quando chega um pedido de conexão para um dos serviços que gerencia, o `xinetd` inicializa o servidor apropriado para este serviço.

O arquivo de configuração do `xinetd` é o `/etc/xinetd.conf`, mas o arquivo contém somente algumas regras default e uma instrução para incluir o diretório `/etc/xinetd.d`. Para habilitar ou desabilitar um serviço `xinetd` edite seu arquivo de configuração no diretório `/etc/xinetd.d`. Se o atributo `disable` estiver definido como **no**, o serviço está habilitado. Você pode editar quaisquer arquivos de configuração do `xinetd` ou alterar seu status 'habilitado' usando a **Ferramenta de Configuração dos Serviços**, a **ntsysv**, ou o `chkconfig`. Para obter uma lista dos serviços de rede controlados pelo `xinetd`, reveja o conteúdo do diretório `/etc/xinetd.d` com o comando `ls /etc/xinetd.d`.

## 21.3. Ferramenta de Configuração dos Serviços

A **Ferramenta de Configuração dos Serviços** é uma aplicação gráfica desenvolvida pela Red Hat para configurar quais serviços SysV no diretório `/etc/rc.d/init.d` são iniciados no momento da inicialização da máquina (para os níveis de execução 3, 4 e 5) e quais serviços `xinetd` são habilitados. Também permite que você inicie, pare e reinicie serviços SysV, assim como reiniciar o `xinetd`.

Para iniciar a **Ferramenta de Configuração dos Serviços** pela área de trabalho, clique no **Botão do Menu Principal** (no Painel) => **Configurações do Sistema => Configurações do Servidor => Serviços** ou digite o comando `redhat-config-services` em uma janela de comandos (por exemplo: em um **XTerm** ou um **terminal do GNOME**).

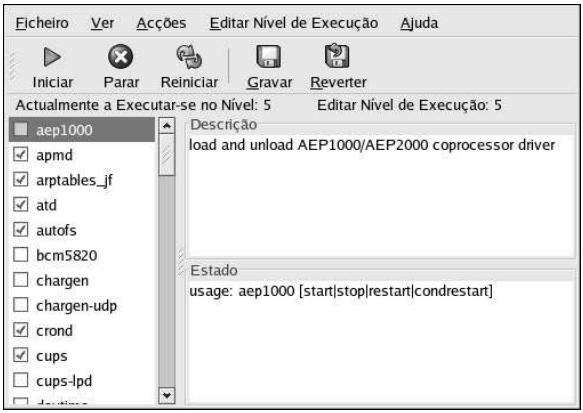


**Figura 21-1. Ferramenta de Configuração dos Serviços**

A **Ferramenta de Configuração dos Serviços** exibe o nível de execução atual assim como o nível de execução que você está editando. Para editar um nível de execução diferente, selecione **Editar Nível de Execução** no menu suspenso e selecione o nível de execução 3, 4 ou 5. Consulte a Seção 21.1 para uma descrição dos níveis de execução.

A **Ferramenta de Configuração dos Serviços** lista os serviços do diretório `/etc/rc.d/init.d` assim como os serviços controlados pelo `xinetd`. Clique no nome do serviço na lista do lado esquerdo da aplicação para visualizar uma breve descrição deste serviço e o status do mesmo. Se o serviço não for `xinetd`, a janela de status mostra se o serviço está rodando no momento. Se o serviço for controlado pelo `xinetd`, a janela de status exibe a frase **xinetd service**.

Para iniciar, parar ou reiniciar um serviço imediatamente, selecione o serviço da lista e clique no botão apropriado da barra de ferramentas (ou escolha a ação no menu suspenso **Ações**). Se for um serviço `xinetd`, os botões de ação estarão desabilitados porque não podem ser iniciados ou parados separadamente.

Se você habilitar/desabilitar um serviço `xinetd` selecionando ou desselecionando a caixa de verificação próxima ao nome do serviço, você deve selecionar **Arquivo => Salvar Alterações** a partir do menu suspenso para reiniciar o `xinetd` e imediatamente habilitar/desabilitar o serviço `xinetd` alterado. O `xinetd` também é configurado para lembrar a configuração. Você pode habilitar/desabilitar múltiplos serviços `xinetd` de uma só vez e salvar as alterações quando terminar.

Por exemplo: assuma que você selecione `rsync` para habilitá-lo no nível de execução 3 e então salve as alterações. O serviço `rsync` é habilitado imediatamente. Na próxima vez que o `xinetd` for iniciado, o `rsync` ainda estará habilitado.

**Aviso**

Quando você salva alterações nos serviços `xinetd`, o `xinetd` é reiniciado e as alterações têm efeito imediato. Quando você salva alterações em outros serviços, o nível de execução é reconfigurado, mas as alterações não têm efeito imediato.

Para habilitar um serviço não-`xinetd` para iniciar no momento da inicialização da máquina no nível de execução atualmente selecionado, selecione a caixa de verificação ao lado do nome do serviço na lista. Após configurar o nível de execução, aplique as alterações selecionando **Arquivo => Salvar Alterações** no menu suspenso. A configuração do nível de execução é alterada, mas o nível de execução não é reiniciado; portanto, as alterações não têm efeito imediato.

Por exemplo: assuma que você está configurando o nível de execução 3. Se alterar o valor para o serviço `httpd` de selecionado para desselecionado e então clicar em **Salvar Alterações**, a configuração do nível de execução 3 não é reinicializada, portanto o `httpd` ainda está rodando. A esta altura, selecione uma das seguintes opções:

1. Parar o serviço `httpd` — Pare o serviço selecionando-o na lista e clicando no botão **Parar**. Aparece uma mensagem afirmando que o serviço foi parado com sucesso.
2. Reinicializar o nível de execução — Reinicialize o nível de execução em uma janela de comandos, digitando o comando `telinit 3` (ondde 3 é o número do nível de execução).Esta esta é recomendada se você alterar o valor **Iniciar no momento da Inicialização** de múltiplos serviços e quiser ativar as alterações imediatamente. opçã
3. Não fazer mais nada — Não é necessário parar o serviço `httpd`. Você pode esperar o sistema ser reinicializado para o serviço parar. Na próxima vez em que o sistema for reinicializado, o nível de execução será iniciado sem que o serviço `httpd` esteja rodando.

Para adicionar um serviço a um nível de execução, selecione o nível no menu suspenso **Editar Nível de Execução** e então selecione **Ações => Adicionar Serviço**. Para apagar um serviço de um nível de execução, selecione o nível do menu suspenso **Editar Nível de Execução**, selecione o serviço a ser apagado na lista esquerda, e então **Ações => Apagar Serviço**.

## 21.4. ntsysv

O utilitário **ntsysv** oferece uma interface simples para ativar ou desativar serviços. Você pode usar o **ntsysv** para ligar ou desligar um serviço gerenciado pelo `xinetd`. Você também pode usar o **ntsysv** para configurar níveis de execução. Por default, apenas o nível de execução atual é configurado. Para configurar um outro nível de execução, especifique um ou mais níveis de execução com a opção `--level`. Por exemplo: o comando `ntsysv --level 345` configura os níveis de execução 3, 4 e 5.

A interface **ntsysv** funciona como o programa de instalação em modo texto. Use as teclas para cima e para baixo para navegar pela lista. A barra de espaço seleciona/desseleciona os serviços e também é usada para "pressionar" os botões **Ok** e **Cancelar**. Para movimentar-se entre a lista de serviços e os

botões **Ok** e **Cancelar**, use a tecla [Tab]. Um * significa que o serviço está configurado como ligado. Pressionando a tecla [F1] exibe uma breve descrição do serviço selecionado.

**Aviso**

Serviços gerenciados pelo `xinetd` são imediatamente afetados pelo **ntsysv**. Para todos os outros serviços, as alterações não têm efeito imediato. Você deve iniciar ou parar o serviço com o comando `service` *`daemon`* `stop`. No exemplo anterior, substitua *`daemon`* pelo nome do serviço que você deseja parar; por exemplo: `httpd`. Substitua `stop` por `start` ou por `restart` para iniciar ou reiniciar o serviço.

## 21.5. `chkconfig`

O comando `chkconfig` também pode ser usado para ativar e desativar serviços. O comando `chkconfig --list` exibe uma lista de serviços do sistema e se eles estão iniciados (`on`) ou parados (`off`) nos níveis de execução 0-6. No fim da lista 'a uma seção para serviços gerenciados pelo `xinetd`.

Se o comando `chkconfig --list` for usado para questionar um serviço gerenciado pelo `xinetd`, exibirá se o serviço do `xinetd` está ativado (`on`) ou desativado (`off`). Por exemplo: o comando `chkconfig --list finger` retorna o seguinte output:

```
finger          on
```

Conforme exibido, o `finger` está ativado como um serviço do `xinetd`. Se o `xinetd` estiver rodando, o `finger` estará ativado.

Se você usar `chkconfig --list` para questionar um serviço em `/etc/rc.d`, a configuração do serviço para cada nível de execução é exibida. Por exemplo: o comando `chkconfig --list httpd` retorna o seguinte output:

```
httpd          0:off   1:off   2:on    3:on    4:on    5:on    6:off
```

O `chkconfig` também pode ser usado para configurar um serviço para ser iniciado (ou não) em um nível de execução específico. Por exemplo: para desligar o `nscd` nos níveis de execução 3, 4 e 5, use o seguinte comando:

```
chkconfig --level 345 nscd off
```

**Aviso**

Serviços gerenciados pelo `xinetd` são imediatamente afetados pelo `chkconfig`. Por exemplo: se o `xinetd` estiver rodando, o `finger` está desabilitado. Se o comando `chkconfig finger on` for executado, `finger` é imediatamente ativado sem que haja necessidade de reiniciar o `xinetd` manualmente. Alterações para outros serviços não têm efeito imediato após o uso do `chkconfig`. Você deve parar ou iniciar o serviço separadamente com o comando `service` *`daemon`* `stop`. No exemplo anterior, substitua *`daemon`* pelo nome do serviço que deseja parar, como por exemplo: `httpd`. Substitua `stop` por `start` ou por `restart` para iniciar ou reiniciar o serviço.

## 21.6. Recursos Adicionais

Para mais informações, consulte os seguintes recursos:

### 21.6.1. Documentação Instalada

- As páginas man de `ntsysv`, `chkconfig`, `xinetd` e `xinetd.conf`.
- `man 5 hosts_access` — A página man para o formato dos arquivos de controle de acesso para máquinas (na seção 5 das páginas man).

### 21.6.2. Websites Úteis

- http://www.xinetd.org — O site do `xinetd`. Contém uma lista mais detelhada das características e amostra de arquivos de configuração.

### 21.6.3. Livros Relacionados

- *Guia de Referência do Red Hat Enterprise Linux*, Red Hat, Inc. — Este manual contém informações detalhadas sobre como o TCP wrappers e o `xinetd` permitem ou negam acesso e também como configurar o acesso à rede usando-os. Alem disso, ainda oferece instruções para criar regras `iptables` para firewalls.
- *Guia de Segurança do Red Hat Enterprise Linux* Red Hat, Inc. — Este manual aborda a proteção de serviços com TCP wrappers e `xinetd`, como o registro de tentativas de conexão negadas.

# Capítulo 22.

# OpenSSH

OpenSSH é uma implementação gratuita e open source dos protocolos SSH (*S*ecure *SH*ell). Ele substitui o `telnet`, o `ftp`, o `rlogin`, o `rsh` e o `rcp` por ferramentas de conexão de rede criptografadas e seguras. OpenSSH suporta as versões 1.3, 1.5 e 2 do protocolo SSH. Desde a versão 2.9 do OpenSSH, o protocolo default é a versão 2, que usa chaves RSA por default.

## 22.1. Por que usar OpenSSH?a versão

Se você usa ferramentas OpenSSH, está aumentando a segurança de sua máquina. Todas as comunicações com ferramentas OpenSSH, inclusive senhas, são criptogradas. O `Telnet` e o `ftp` usam senhas somente texto e enviam todas as informações sem criptografar. As informações podem ser interceptadas, as senhas podem ser recuperadas e então o sistema pode ser comprometido se uma pessoa não-autorizada se autenticar em seu sistema usando uma das senhas interceptadas. O conjunto de utilitários do OpenSSH deve ser usado sempre que possível para evitar estes problemas de segurança.

Uma outra razão para usar OpenSSH é que este encaminha a variável `DISPLAY` automaticamente para a máquina cliente. Em outras palavras, se você está rodando o Sistema X Window em sua máquina e se autenticar em uma máquina remota usando o comando `ssh`, quando rodar um programa que precise do X na máquina remota, você o verá na sua máquina local. Esta funcionalidade é conveniente se você prefere trabalhar com ferramentas de administração gráficas, mas nem sempre tem acesso físico ao seu servidor.

## 22.2. Configurando um Servidor OpenSSH

Para rodar um servidor OpenSSH, você deve primeiramente certificar-se de ter os pacotes RPM apropriados instalados. O pacote `openssh-server` é necessário e depende do pacote `openssh`.

O daemon OpenSSH usa o arquivo de configuração `/etc/ssh/sshd_config`. O arquivo de configuração default deve ser suficiente na maioria dos casos. Se você quer configurar o daemon de uma maneira diferente do `sshd_config` default, leia a página man do `sshd` para uma lista das palavras-chave que podem ser definidas no arquivo de configuração.

Para iniciar o serviço OpenSSH, use o comando `/sbin/service sshd start`. Para parar o servidor OpenSSH, use o comando `/sbin/service sshd stop`. Se quiser que o daemon inicie automaticamente no momento da inicialização da máquina, consulte o Capítulo 21 para informações sobre o gerenciamento de serviços.

Se você executar uma reinstalação e houver clientes conectados ao sistema com alguma ferramenta OpenSSH antes da reinstalação, os usuários cliente verão a seguinte mensagem após a reinstalação:

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@    WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!     @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
It is also possible that the RSA host key has just been changed.
```

O sistema reinstalado cria um novo conjunto de chaves de identificação, apesar do aviso sobre a mudança da chave RSA da máquina. Se você deseja guardar as chaves geradas para o sistema, faça um backup dos arquivos `/etc/ssh/ssh_host*key*` e armazene-os após a reinstalação. Este processo retém a identidade do sistema e, quando os clientes tentarem conectar o sistema após a reinstalação, não receberão a mensagem de aviso.

## 22.3. Configurando um Cliente OpenSSH

Para conectar uma máquina cliente a um servidor OpenSSH, você deve ter os pacotes `openssh-clients` e `openssh` instalados na máquina cliente.

### 22.3.1. Usando o comando `ssh`

O comando `ssh` é um subtituto seguro para os comandos `rlogin`, `rsh` e `telnet`. Permite que você se autentique e execute comandos em uma máquina remota.

Se autenticar (log in) em uma máquina remota com `ssh` é similar a usar o `telnet`. Para se autenticar em uma máquina remota chamada penguin.example.net, digite o seguinte comando em uma janela de comandos:

```
ssh penguin.example.net
```

A primeira vez em que você usar o `ssh` em uma máquina remota, você verá uma mensagem parecida com a seguinte:

```
The authenticity of host 'penguin.example.net' can't be established.
DSA key fingerprint is 94:68:3a:3a:bc:f3:9a:9b:01:5d:b3:07:38:e2:11:0c.
Are you sure you want to continue connecting (yes/no)?
```

Digite **`yes`** para continuar. Isto adicionará o servidor à sua lista de máquinas conhecidas, conforme pode-se observar na mensagem a seguir:

```
Warning: Permanently added 'penguin.example.net' (RSA) to the list of known hosts.
```

Em seguida, você verá um diálogo pedindo sua senha para a máquina remota. Após inserir sua senha, você estará em uma janela de comandos da máquina remota. Se você não especificar um nome de usuário, o usuário com o qual você está autenticado na máquina cliente local será passado para a máquina remota. Se você quiser especificar um nome diferente de usuário, use o seguinte comando:

```
ssh username@penguin.example.net
```

Você também pode usar a sintaxe `ssh -l nomedousuário penguin.example.net`.

O comando `ssh` pode ser usado para executar um comando na máquina remota sem precisar autenticar em uma shell. A sintaxe é `ssh nomedamáquina comando`. Por exemplo, Se você quer executar o comando `ls /usr/share/doc` na máquina remota penguin.example.net, digite o seguinte comando em uma janela de comandos:

```
ssh penguin.example.net ls /usr/share/doc
```

Após inserir a senha correta, o conteúdo do diretório `/usr/share/doc` remoto será exibido e você retornará para a sua janela de comandos local.

### 22.3.2. Usando o Comando `scp`

O comando `scp` pode ser usado para transferir arquivos entre máquinas, através de uma conexão segura e criptografada. É parecido com o comando `rcp`.

A sintaxe geral para transferir um arquivo local para um sistema remoto é a seguinte:

```
scp localfile username@tohostname:/newfilename
```

O *`arquivolocal`* especifica a fonte e o *`usuário@máquina:/novonomedoarquivo`* especifica o destino.

Para transferir o arquivo local `shadowman` para a sua conta em penguin.example.net, digite o seguinte em uma janela de comandos substitua *`username`* pelo seu nome de usuário):

```
scp shadowman username@penguin.example.net:/home/username
```

Isso transferirá o arquivo local `shadowman` para `/home/`*`nomedousuário`*`/shadowman` em penguin.example.net.

A sintaxe geral para transferir um arquivo remoto para o sistema local é a seguinte:

```
scp username@tohostname:/remotefile /newlocalfile
```

O *`arquivoremoto`* especifica a fonte e o *`novoarquivolocal`* especifica o destino.

Pode-se especificar múltiplos arquivos como os arquivos fonte. Por exemplo: para transferir o conteúdo do diretório `/downloads` para um diretório existente chamado `uploads` na máquina remota penguin.example.net, digite o seguinte em uma janela de comandos:

```
scp /downloads/* username@penguin.example.net:/uploads/
```

### 22.3.3. Usando o Comando `sftp`

O utilitário `sftp` pode ser usado para abrir uma sessão FTP interativa protegida. É similar ao `ftp`, exceto pelo fato de utilizar uma conexão segura e criptografada. A sintaxe geral é *`sftp usuário@máquina.com`*. Uma vez autenticado, você pode usar uma série de comandos similares àqueles usados pelo FTP. Consulte a página man do `sftp` para obter uma lista destes comandos. Para ler a página man, execute o comando `man sftp` em uma janela de comandos. O utilitário `sftp` está disponível somente nas versões 2.5.0p1 e mais recentes do OpenSSH.

### 22.3.4. Gerando Pares de Chaves

Se você não deseja inserir sua senha toda vez que usar `ssh`, `scp` ou `sftp` para conectar a uma máquina remota, pode gerar um par de chaves de autorização.

As chaves devem ser geradas para cada usuário. Para gerar chaves para um usuário, siga os passos como o usuário que deseja conectar-se a máquinas remotas. Se você completar estes passos como root, somente root poderá usar estas chaves.

Iniciando com o OpenSSH versão 3.0, os `~/.ssh/authorized_keys2`, `~/.ssh/known_hosts2` e `/etc/ssh_known_hosts2` são obsoletos. O Protocolo SSH 1 e 2 compartilham os arquivos `~/.ssh/authorized_keys`, `~/.ssh/known_hosts` e `/etc/ssh/ssh_known_hosts`.

O Red Hat Enterprise Linux 3 usa o Protocolo SSH 2 e chaves RSA por default.

**Dica**

Se você reinstalar e quiser salvar seu par de chaves geradas, faça backup do diretório `.ssh` em seu diretório home. Após reinstalar, copie este diretório de volta ao seu diretório home. Este processo pode ser feito para todos os usuários de seu sistema, inclusive para root.

#### 22.3.4.1. Gerando um Par de Chaves RSA para a Versão 2

Siga os seguintes passos para gerar um par de chaves RSA para a versão 2 do protocolo SSH. Este é o início default com o OpenSSH 2.9.

1. Para gerar um par de chaves RSA que funcione com a versão 2 do protocolo, digite o seguinte comando em uma janela de comandos:
   ```
   ssh-keygen -t rsa
   ```
   Aceite a localização default do arquivo em `~/.ssh/id_rsa`. Indique uma frase de senha diferente da senha da sua conta e confirme-a digitando novamente.

   A chave pública é gravada no `~/.ssh/id_rsa.pub`. A chave privada é gravada no `~/.ssh/id_rsa`. Nunca divulgue sua chave privada para ninguém.
2. Altere as permissões do diretório `.ssh` usando o seguinte comando:
   ```
   chmod 755 ~/.ssh
   ```
3. Copie o conteúdo do `~/.ssh/id_rsa.pub` para `~/.ssh/authorized_keys` na máquina com a qual você deseja se conectar. Se o arquivo `~/.ssh/authorized_keys` existir, anexe o conteúdo do arquivo `~/.ssh/id_rsa.pub` ao arquivo `~/.ssh/authorized_keys` na outra máquina.
4. Altere as permissões do arquivo `authorized_keys` usando o seguinte comando:
   ```
   chmod 644 ~/.ssh/authorized_keys
   ```
5. Se você estiver rodando o GNOME, pule para a Seção 22.3.4.4. Se você estiver rodando o Sistema X Window, pule para a Seção 22.3.4.5.

#### 22.3.4.2. Gerando um Par de Chaves DSA para a Versão 2

Use os seguintes passos para gerar um par de chaves DSA para a versão 2 do protocolo SSH.

1. Para gerar um par de chaves DSA que funcione com a versão 2 do protocolo, digite o seguinte comando em uma janela:
   ```
   ssh-keygen -t dsa
   ```
   Aceite a localização default do `~/.ssh/id_dsa`. Indique uma frase de senha diferente da senha da sua conta e confirme-a digitando novamente.

   
   **Dica**

   Uma frase de senha é um trecho de palavras e caracteres usado para autenticar um usuário. Frases de senha diferem das senhas, pois você pode usar espaços ou tabs na frase de senha. Frases de senha geralmente são mais longas que as senhas porque usualmente são frases ao invés de uma única palavra.

   A chave pública é gravada no `~/.ssh/id_dsa.pub`. A chave privada é gravada no `~/.ssh/id_dsa`. Importante: nunca forneça a chave privada a ninguém.
2. Altere as permissões do diretório `.ssh` com o seguinte comando:
   ```
   chmod 755 ~/.ssh
   ```
3. Copie o conteúdo do `~/.ssh/id_dsa.pub` no `~/.ssh/authorized_keys` na máquina que você deseja conectar. Se o arquivo `~/.ssh/authorized_keys` existir, anexe o conteúdo do arquivo `~/.ssh/id_dsa.pub` ao arquivo `~/.ssh/authorized_keys` na outra máquina.
4. Altere as permissões do arquivo `authorized_keys` usando o seguinte comando:
   ```
   chmod 644 ~/.ssh/authorized_keys
   ```

5. Se você estiver rodando o GNOME, pule para a Seção 22.3.4.4. Se você estiver rodando o Sistema X Window, pule para a Seção 22.3.4.5.

#### 22.3.4.3. Gerando uma Par de Chaves RSA para as Versões 1.3 e 1.5

Use os seguntes passos para gerar um par de chaves RSA, que são usadas pela versão 1 do Protocolo SSH. Se você está conectando somente entre sistemas que usam DSA, não precisa de um par de chaves RSA versão 1.3 ou 1.5.

1. Para gerar um par de chaves RSA (para as versões 1.3 e 1.5 do protocolo), digite o seguinte em uma janela de comandos:
   ```
   ssh-keygen -t rsa1
   ```
   Aceite a localização default (`~/.ssh/identity`). Indique uma frase de senha diferente da senha de sua conta. Confirme a frase de senha digitando-a novamente.

   A chave pública é gravada no `~/.ssh/identity.pub`. A chave privada é gravada no `~/.ssh/identity`. Não forneça a chave privada a ninguém.
2. Altere as permissões de seu diretório `.ssh` e de sua chave com os comandos `chmod 755 ~/.ssh`e `chmod 644 ~/.ssh/identity.pub`.
3. Copie o conteúdo de `~/.ssh/identity.pub` para o arquivo `~/.ssh/authorized_keys` na máquina em que você deseja se conectar. Se o arquivo `~/.ssh/authorized_keys` não existir, você pode copiar o arquivo `~/.ssh/identity.pub` no arquivo `~/.ssh/authorized_keys` na máquina remota.
4. Se você está rodando GNOME, pule para a Seção 22.3.4.4. Se você não está rodando GNOME, pule para a Seção 22.3.4.5.

#### 22.3.4.4. Configurando o `ssh-agent` com GNOME

O utilitário `ssh-agent` pode ser usado para salvar sua frase de senha para que você não precise inserí-la toda vez que iniciar uma conexão `ssh` ou `scp`. Se você está usando o GNOME, o utilitário `openssh-askpass-gnome` pode ser usado para pedir a frase da senha quando você se autenticar no GNOME, e salvá-la até que você saia (faça o logout) do GNOME. Você não precisará inserir sua senha ou frase de senha para nenhuma conexão `ssh` ou `scp` feita durante esta sessão do GNOME. Se você não está usando GNOME, consulte a Seção 22.3.4.5.

Para salvar sua frase de senha durante a sessão do GNOME, siga estes passos:

1. Você precisa ter o pacote `openssh-askpass-gnome` instalado; pode usar o comando `rpm -q openssh-askpass-gnome` para determinar se está instalado ou não. Se não está instalado, instale-o pelo seu conjunto de CD-ROMs do Red Hat Enterprise Linux, pelo site espelho FTP da Red Hat, ou usando a Red Hat Network.
2. Selecione **Botão do Menu Principal** (no Painel) => **Preferências** => **Mais Preferências** => **Sessões** e clique na aba **Programas Startup**. Clique em **Adicionar** e insira **`/usr/bin/ssh-add`** no campo **Comando Startup**. Defina para este uma prioridade de número acima que quaisquer comandos existentes para garantir que seja executado por último. Um bom número de prioridade para o `ssh-add` é 70 ou maior. Quanto maior o número da prioridade, mais baixa é a prioridade. Se você tem outros programas listados, este deve ter a prioridade mais baixa. Clique em **Fechar** para sair do rpograma.
3. Faça o logout e então se autentique novamente (log in) no GNOME; em outras palavras, reinicie o X. Após o GNOME ser reiniciado, aparece uma caixa de diálogo pedindo sua(s) frase(s) de senha. Indique a frase de senha requisitada. Se você tem ambos pares de chaves DSA e RSA

configurados, terá que indicar ambos. A partir deste ponto, o `ssh`, o `scp` ou o `sftp` não devem mais solicitar senhas.

#### 22.3.4.5. Configurando o `ssh-agent`

O `ssh-agent` pode ser usado para armazenar sua frase de senha para que assim você não precise inserí-la toda vez que fizer uma conexão `ssh` ou `scp`. Se você não está rodando o Sistema X Window, siga estes passos em uma janela de comandos. Se está rodando GNOME, mas não quer configurá-lo de modo que peça sua frase de senha quando se autenticar (veja a Seção 22.3.4.4), este procedimento funcionará em uma janela de terminal, como um XTerm. Se você está rodando X, mas não GNOME, este procedimento funcionará em uma janela de terminal. Entretanto, sua frase de senha será lembrada somente para aquela janela de terminal; não é uma configuração global.

1. Digite o seguinte em uma janela de comandos:
   ```
   exec /usr/bin/ssh-agent $SHELL
   ```
2. Então digite o comando:
   ```
   ssh-add
   ```
   e indique sua(s) frase(s) de senha. Se você tem mais de um par de chaves configurado, terá que inserir cada um deles.
3. Quando fizer logout, sua(s) frase(s) de senha serão esquecidas. Você deve executar estes dois comando cada vez que se autenticar em um console virtual ou abrir uma janela de terminal.

## 22.4. Recursos Adicionais

Os projetos OpenSSH e OpenSSL estão em desenvolvimento constante, e as informações mais atualizadas sobre eles estão disponíveis em seus sites na Internet. As páginas man das ferramentas OpenSSH e OpenSSL também são boas fontes de informações detalhadas.

### 22.4.1. Documentação Instalada

- As páginas man do `ssh`, `scp`, `sftp`, `sshd` e do `ssh-keygen` — Estas páginas man incluem informações sobre o uso destes comandos assim como todos os parâmetros que podem ser usados com eles.

### 22.4.2. Sites Úteis

- http://www.openssh.com/ — O FAQ do OpenSSH, relatórios de erros, listas de discussão, objetivos do projeto e uma explicação mais técnica das funcionalidades de segurança.
- http://www.openssl.org/ — O FAQ do OpenSSL, listas de discussão e uma descrição do objetivo do projeto.
- http://www.freessh.org/ — Software para cliente SSH para outras plataformas.

### 22.4.3. Livros Relacionados

- *Guia de Referência do Red Hat Enterprise Linux* — Aprenda a sequência de eventos de uma conexão SSH, reveja a lista de arquivos de configuração e descubra como o SSH pode ser usado para o encaminhamento do X (X forwarding).

Capítulo 23.

# Sistema de Arquivo de Rede (NFS - Network File System)

O Sistema de Arquivo de Rede (NFS) é uma maneira de compartilhar arquivos entre máquinas de uma rede, como se estes arquivos estivessem localizados no disco rígido local do cliente. O Red Hat Enterprise Linux pode ser um servidor NFS e um cliente NFS, o que significa que pode exportar sistemas de arquivo para outros sistemas e montar sistemas de arquivo exportados de outras máquinas.

## 23.1. Por que usar o NFS?

O NFS é útil para compartilhar diretórios de arquivos entre múltiplos usuários da mesma rede. Por exemplo: um grupo de usuários trabalhando no mesmo projeto podem ter acesso aos arquivos deste projeto usando um diretório compartilhado do sistema de arquivo NFS (comumente conhecido como partilha do NFS) montado no diretório `/myproject`. Para accessar os arquivos compartilhados, o usuário vai ao diretório `/myproject`. Não há senhas ou comandos especiais para lembrar. Os usuários trabalham como se o diretório estivesse em suas máquinas locais.

## 23.2. Montando Sistemas de Arquivo NFS

Use o comando `mount` para montar um diretório NFS compartilhado de uma outra máquina:

```
mount shadowman.example.com:/misc/export /misc/local
```

**Atenção**

O diretório do ponto de montagem na máquina local (`/misc/local` no exemplo anterior) deve existir.

Neste comando, `shadowman.example.com` é o nome da máquina do servidor de arquivos NFS; `/misc/export` é o diretório que `shadowman` está exportando e `/misc/local` é a localidade para montar o sistema de arquivo na máquina local. Após rodar o comando `mount` (e se o cliente tiver as devidas permissões do servidor NFS `shadowman.example.com`) o usuário cliente pode executar o comando `ls /misc/local` para exibir uma lista dos arquivos do `/misc/export` em `shadowman.example.com`.

### 23.2.1. Montando Sistemas de Arquivo NFS usando `/etc/fstab`

Uma maneira alternativa de montar uma partilha NFS de uma outra máquina é adicionar uma linha ao arquivo `/etc/fstab`. A linha deve especificar o nome da máquina (hostname) do servidor NFS, o diretório do servidor sendo exportado e o diretório da máquina local onde a partilha do NFS deve ser montada. Você deve estar como root para modificar o arquivo `/etc/fstab`.

A sintaxe geral da linha no `/etc/fstab` é a seguiinte:

```
server:/usr/local/pub     /pub    nfs     rsize=8192,wsize=8192,timeo=14,intr
```

O ponto de montagem `/pub` deve existir na máquina cliente. Após adicionar esta linha ao `/etc/fstab` no sistema cliente, digite o comando `mount /pub` em uma janela de comandos, e o ponto de montagem `/pub` será montado pelo servidor.

### 23.2.2. Montando Sistemas de Arquivo NFS usando autofs

Uma terceira opção para montar uma partilha NFS é usar o autofs. Autofs usa o daemon automount para administrar seus pontos de montagem, montando-os dinamicamente somente quando são acessados.

O autofs consulta o arquivo de configuração do mapa mestre `/etc/auto.master` para determinar quais pontos de montagem estão definidos. Então, o autofs inicia um processo de auto-montagem com os parâmetros apropriados para cada ponto de montagem. Cada linha do mapa mestre define um ponto de montagem e um arquivo de mapa separado, que define os sistemas de arquivo a serem montados sob este ponto de montagem. Por exemplo: o arquivo `/etc/auto.misc` pode definir pontos de montagem no diretório `/misc`; esta relação seria definida no arquivo `/etc/auto.master`.

Cada entrada do `auto.master` tem três campos. O primeiro campo é o ponto de montagem. O segundo é a localidade do arquivo de mapa e o terceiro é opcional. O terceiro campo poode conter informações como o valor de tempo limite (timeout).

Por exemplo: para montar o diretório `/proj52` na máquina remota penguin.example.net no ponto de montagem `/misc/myproject` em sua máquina, adicione a seguinte linha ao `auto.master`:

```
/misc   /etc/auto.misc --timeout 60
```

Adicione a seguinte linha ao `/etc/auto.misc`:

```
myproject  -rw,soft,intr,rsize=8192,wsize=8192 penguin.example.net:/proj52
```

O primeiro campo do `/etc/auto.misc` é o nome do sub-diretório `/misc`. Este diretório é criado dinamicamente pela auto-montagem e não deve existir de verdade na máquina cliente. O segundo campo contém pontos de montagem como `rw` para acesso de leitura e gravação (read and write). O terceiro campo é a localidade da exportação NFS, incluindo nome da máquina e diretório.

**Nota**

O diretório `/misc` deve existir no sistema de arquivo local. Não deve haver sub-diretórios no `/misc` do sistema de arquivo local.

O autofs é um serviço. Para iniciá-lo, digite os seguintes comandos em uma shell:

```
/sbin/service autofs restart
```

Para visualizar os pontos de montagem ativos, digite o seguinte comando em uma shell:

```
/sbin/service autofs status
```

Se você modificar o arquivo de configuração `/etc/auto.master` enquanto o autofs rodar, deve dizer ao(s) daemon(s) automount para recarregar, digitando o seguinte em uma janela de comandos:

```
/sbin/service autofs reload
```

Para aprender a configurar o autofs de modo a iniciar no momento da inicialização, consulte o Capítulo 21 para informações sobre a administração de serviços.

### 23.2.3. Usando TCP

O protocolo de transporte default para o NFS é UDP, no entanto, o kernel do Red Hat Enterprise Linux 3 inclui suporte ao NFS sobre o TCP. Para usar o NFS sobre o TCP, inclua a opção `-o tcp` ao comando `mount` quando montar o sistema de arquivo exportado pelo NFS no sistema cliente. Por exemplo:

```
mount -o tcp shadowman.example.com:/misc/export /misc/local
```

Se a montagem NFS é especificada no `/etc/fstab`:

```
server:/usr/local/pub    /pub   nfs    rsize=8192,wsize=8192,timeo=14,intr,tcp
```

Se é especificada em um arquivo de configuração do autofs:

```
myproject  -rw,soft,intr,rsize=8192,wsize=8192,tcp penguin.example.net:/proj52
```

Já que o default é UDP, se a opção `-o tcp` não for especificada, o sistema de arquivo exportado pelo NFS é acessado via UDP.

As vantagens de usar TCP incluem as seguintes:

- Durabilidade da conexão melhorada, consequentemente menos mensagens de `NFS stale file handles`.
- Ganho de desempenho nas redes altamente carregadas porque o TCP reconhece todos os pacotes, ao contrário do UDP que só reconhece a conclusão.
- O TCP tem um bom controle de congestionamento, enquanto o UDP não tem. Em uma rede muito congestionada, os pacotes UDP são os primeiros tipos de pacotes a cair. Isto significa que se o NFS está salvando dados (em blocos de 8K), todos os 8K devem ser retransmitidos. Com o TCP, devido a sua confiabilidade, uma parte dos 8K de dados é transmitida de cada vez.
- Detecção de erros. Quando uma conexão tcp é interrompida (devido à queda do servidor), o cliente pára de enviar dados e começa o processo de reconexão. Com o UDP, como não há conexão, o cliente continua a lotar a rede com dados até que o servidor volte.

A desvantagem principal é que há um nível de desempenho baixo devido à sobrecarga associada ao protocolo TCP.

### 23.2.4. Preservando as ACLs

O kernel do Red Hat Enterprise Linux 3 oferece suporte a ACL para os sistemas de arquivo ext3 e ext3 montados com os protocolos NFS ou Samba. Consequentemente, se um sistema de arquivo ext3 tem ACLs habilitadas e é exportado através do NFS, e se um cliente NFS pode ler as ACLs, estas são usadas pelo cliente NFS também.

Para mais informações sobre a montagem de sistemas de arquivo NFS com ACLs, consulte o Capítulo 8.

## 23.3. Exportando Sistemas de Arquivo NFS

Compartilhar arquivos de um servidor NFS é conhecido como exportar os diretórios. A **Ferramenta de Configuração do Servidor NFS** pode ser usada para configurar um sistema como um servidor NFS.

Para usar a **Ferramenta de Configuração do Servidor NFS**, você deve rodar o Sistema X Window, ter privilégios root e ter o pacote RPM `redhat-config-nfs` instalado. Para iniciar a aplicação,

selecione **Botão do Menu Principal** (no Painel) => **Configurações do Sistema => Configurações do Servidor => NFS**, ou digite o comando `redhat-config-nfs`.

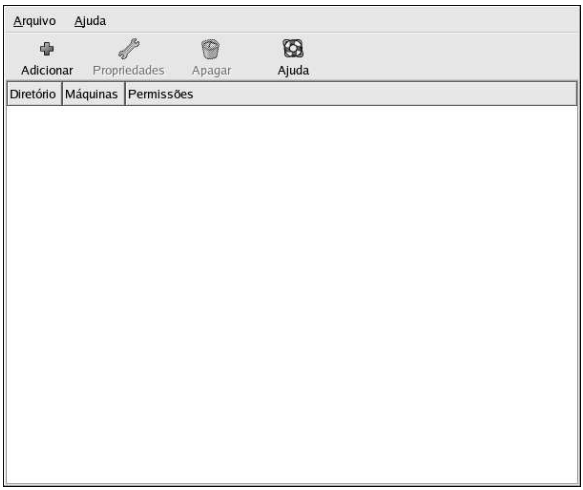


**Figura 23-1. Ferramenta de Configuração do Servidor NFS**

Para adicionar uma partilha NFS, clique no botão **Adicionar**. O diálogo exibido na Figura 23-2 aparecerá.

A aba **Básica** requer as seguintes informações:

- **Diretório** — Especifique o diretório a compartilhar, tal como `/tmp`.
- **Máquina(s)** — Especifique a(s) máquina(s) entre as quais compartilhar o diretório. Consulte a Seção 23.3.2 para uma explicação sobre os possíveis formatos.
- **Permissões básicas** — Especifique se o diretório deve ter permissões somente-leitura ou leitura e gravação.

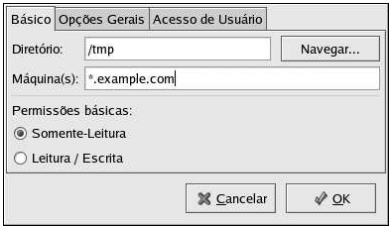


**Figura 23-2. Adicionar Partilha**

A aba **Opções Gerais** permite que as seguintes opções sejam configuradas:

- **Permitir conexões da porta 1024 e acima** — Os serviços iniciados em portas de números abaixo de 1024 devem ser iniciados como root. Selecione esta opção para permitir que o serviço NFS seja iniciado por outro usuário, além do root. Esta opção corresponde ao comando `insecure`.
- **Permitir bloqueio de arquivo inseguro** — Não requer um pedido de bloqueio. Esta opção corresponde ao `insecure_locks`.
- **Desabilitar verificação da sub-árvore** — Se um sub-diretório de um sistema de arquivo é exportado, mas não o sistema de arquivo inteiro, o servidor verifica se o arquivo solicitado está no sub-diretório exportado. Esta verificação é chamada *verificação da sub-árvore*. Selecione esta opção para desabilitar a verificação da sub-árvore. Se o sistema de arquivo inteiro é exportado, selecionar desabilitar a verificação da sub-árvore pode aumentar a taxa de transferência. Esta opção corresponde ao `no_subtree_check`.
- **Sincronizar operações de gravação a pedido** — Habilitada por default, esta opção não permite que o servidor responda a pedidos antes que as alterações feitas pelo pedido sejam salvas no disco. Esta opção corresponde ao `sync`. Se não estiver selecionada, a opção `async` é usada.
  - **Forçar sincronia das operações de gravação imediatamente** — Não atrasa a gravação no disco. Esta opção corresponde ao `no_wdelay`.

A aba **Acesso do Usuário** permite configurar as seguintes opções:

- **Tratar usuário root remoto como root local** — Por default, os IDs de usuário e grupo do usuário root são ambos definidos como 0. O esmagamento do root mapeia o ID 0 do usuário e o ID 0 do grupo para os IDs de usuário e grupo de anônimo, para que o root do cliente não tenha privilégios root no servidor NFS. Se esta opção é selecionada, root não é mapeado para anônimo, e o root do cliente tem privilégios root nos diretórios exportados. Selecionar esta opção pode reduzir drasticamente a segurança do sistema. Não selecione-a a não ser que seja absolutamente necessário. Esta opção corresponde ao `no_root_squash`.
- **Tratar todos os usuários cliente como anônimos** — Se esta opção é selecionada, todos os IDs de usuário e de grupo são mapeados para o usuário anônimo. Esta opção corresponde ao `all_squash`.
  - **Especificar ID do usuário local para usuários anônimos** — Se **Tratar todos os usuários cliente como anônimos** é selecionada, esta opção permite que você especifique um ID de usuário para o usuário anônimo. Esta opção corresponde ao `anonuid`.
  - **Especificar ID do grupo local para usuários anônimos** — Se **Tratar todos os usuários cliente como anônimos** é selecionada, esta opção permite que você especifique um ID de grupo para o usuário anônimo. Esta opção corresponde ao `anongid`.

Para editar uma partilha NFS, selecione-a da lista e clique no botão **Propriedades**. Para apagar uma partilha NFS, selecione-a da lista e clique no botão **Apagar**.

Após clicar no botão **OK** para adicionar, editar ou apagar uma partilha NFS da lista, as alterações têm efeito imediato — o daemon do servidor é reiniciado e o arquivo da configuração antiga é salvo como `/etc/exports.bak`. A nova configuração é salva no arquivo `/etc/exports`.

A **Ferramenta de Configuração do Servidor NFS** lê e salva diretamente no arquivo de configuração `/etc/exports`. Consequentemente, o arquivo pode ser modificado manualmente após usar a ferramenta, e a ferramenta pode ser usada após modificar o arquivo manualmente (desde que o arquivo seja modificado com a sintaxe correta).

### 23.3.1. Configuração da Linha de Comando

Se você prefere editar arquivos de configuração usando um editor de texto ou se não tem o Sistema X Window instalado, pode modificar o arquivo de configuração diretamente.

O arquivo `/etc/exports` controla quais diretórios o servidor NFS exporta. Seu formato é o seguinte:

```
directory hostname(options)
```

A única opção que precisa ser especificada é uma destas: `sync` ou `async` (`sync` é recomendado). Se `sync` é especificado, o servidor não responde a pedidos antes que as alterações feitas pelo pedido sejam gravadas no disco.

Por exemplo:

```
/misc/export      speedy.example.com(sync)
```

permitirá que usuários da `speedy.example.com` montem `/misc/export` com as permissões default somente-leitura, mas:

```
/misc/export      speedy.example.com(rw,sync)
```

permitirá que usuários da `speedy.example.com` montem `/misc/export` com privilégios de leitura e gravação.

Consulte a Seção 23.3.2 para uma explicação sobre os possíveis formatos do nome da máquina.

Consulte o *Guia de Referência do Red Hat Enterprise Linux* para uma lista de opções que podem ser especificadas.

**Cuidado**

Tome cuidado com espaços no arquivo `/etc/exports`. Se não há espaços entre o nome da máquina e as opções entre parênteses, as opções se aplicam somente àquela máquina. Se há um espaço entre o nome da máquina e as opções, as opções se aplicam para o resto do mundo. Por exemplo: examine as linhas a seguir.

```
/misc/export speedy.example.com(rw,sync)
/misc/export speedy.example.com (rw,sync)
```

A primeira linha dá aos usuários da `speedy.example.com` acesso de leitura e gravação e proíbe todos os outros usuários. A segunda linha dá aos usuários da `speedy.example.com` acesso somente-leitura (o default) e permite acesso de leitura e gravação para o resto do mundo.

Cada vez que você modificar o `/etc/exports`, deve informar a alteração ao daemon do NFS, ou recarregar o arquivo de configuração com o seguinte comando:

```
/sbin/service nfs reload
```

### 23.3.2. Formatos de Nomes de Máquina

As máquinas podem ter os seguintes formatos:

- Uma máquina — Um nome de domínio totalmente qualificado (que pode ser resolvido pelo servidor), um nome de máquina (que pode ser resolvido pelo servidor) ou um endereço IP
- Uma série de máquinas especificadas com wildcards — Use o caractere * ou ? para especificar uma série. Os wildcards não devem ser usado com endereços IP; no entanto, eles podem funcionar acidentalmente se a procura de DNS inverso falhar. Ao especificar os wildcards em nomes de domínio totalmente qualificados, os pontos (.) não são inclusos. Por exemplo: `*.example.com` inclui one.example.com, mas não inclui one.two.example.com.

- Redes IP — Use `a.b.c.d/z`, onde `a.b.c.d` é a rede e `z` é o número de bits na máscara de rede (ex.: 192.168.0.0/24). Um outro formato aceitável é `a.b.c.d/netmask`, onde `a.b.c.d` é a rede e `netmask` é a máscara de rede (ex.: 192.168.100.8/255.255.255.0).
- Grupos de Rede (netgroups) — No formato `@group-name`, onde `group-name` é o nome do grupo de rede NIS.

### 23.3.3. Iniciando e Parando o Servidor

O serviço `nfs` deve estar rodando no servidor que está exportando sistemas de arqiuvo NFS.

Visualize o estado do daemon NFS com o seguinte comando:

```
/sbin/service nfs status
```

Inicie o daemon NFS com o seguinte comando:

```
/sbin/service nfs start
```

Pare o daemon NFS com o seguinte comando:

```
/sbin/service nfs stop
```

Para iniciar o serviço `nfs` no momento da inicialização, use o comando:

```
/sbin/chkconfig --level 345 nfs on
```

Você também pode usar o `chkconfig`, a **ntsysv** ou a **Ferramenta de Configuração dos Serviços** para determinar quais serviços iniciam no momento da inicialização. Consulte o Capítulo 21 para detalhes.

## 23.4. Recursos Adicionais

Este capítulo aborda os conceitos básicos do uso do NFS. Para informações mais detalhadas, consulte os seguintes recursos:

### 23.4.1. Documentação Instalada

- As páginas man do `nfsd`, `mountd`, `exports`, `auto.master` e do `autofs` (nas seções 5 e 8 do manual) — Estas páginas man exibem a sintaxe correta dos arquivos de configuração do NFS e do autofs.

### 23.4.2. Sites Úteis

- http://nfs.sourceforge.net/ — a página do NFS na Internet, inclui links para as listas de discussão e FAQs.
- http://www.tldp.org/HOWTO/NFS-HOWTO/index.html — O *Linux NFS-HOWTO* da Documentação do Projeto Linux.

### 23.4.3. Livros Relacionados

- *Managing NFS and NIS Services* de Hal Stern; O'Reilly & Associates, Inc.

# Capítulo 24.

# Samba

O Samba usa o protocolo SMB para compartilhar arquivos e impressoras ao longo de uma rede. Os sistemas operacionais que suportam este protocolo incluem o Microsoft Windows, SO/2 e o Linux.

O kernel do Red Hat Enterprise Linux 3 contém suporte à *Lista de Controle de Acesso* (ACL) para sistemas de arquivo ext3. Se o servidor Samba compartilha um sistema de arquivo ext3 com ACLs habilitadas, e o kernel do sistema cliente contém suporte para a leitura de ACLs a partir de sistemas de arquivo ext3, o cliente reconhece automaticamente e usa as ACLs. Consulte o Capítulo 8 para mais informações sobre ACLs.

## 24.1. Por que Usar o Samba?

O Samba é útil se você tem uma rede com máquinas Windows e Linux. O Samba permite que arquivos e impressoras sejam compartilhados por todos os sistemas de uma rede. Para compartilhar arquivos somente entre máquinas Linux, use o NFS conforme abordado no Capítulo 23. Para compartilhar impressoras somente entre máquinas Linux, não é necessário usar o Samba; consulte o Capítulo 36.

## 24.2. Configurando um Servidor Samba

O arquivo de configuração default (`/etc/samba/smb.conf`) permite a usuários visualizar seus diretórios home como uma partilha do Samba. Também compartilha todas as impressoras configuradas para o sistema como impressoras compartilhadas. Em outras palavras, você pode anexar uma impressora ao sistema e imprimir nela a partir de máquinas Windows de sua rede.

### 24.2.1. Configuração Gráfica

Para configurar o Samba usando uma interface gráfica, use a **Ferramenta de Configuração do Servidor Samba**. Para configuração pela linha de comandos, pule para a Seção 24.2.2.

A **Ferramenta de Configuração do Servidor Samba** é uma interface gráfica para administrar as partilhas, usuários e configurações básicas do Samba. Ela modifica os arquivos de configuração no diretório `/etc/samba/`. Todas as alterações destes arquivos feitas sem o uso da aplicação são preservadas.

Para usar esta aplicação, você deve rodar o Sistema X Window, ter privilégios root e ter o pacote RPM `redhat-config-samba` instalado. Para inciar a **Ferramenta de Configuração do Servidor Samba** pela área de trabalho, clique no **Botão do Menu Principal** (no Painel) => **Configurações do Sistema** => **Configurações do Servidor** => **Samba** ou digite o comando `redhat-config-samba` em uma janela de comandos (ex.: em um XTerm ou terminal do GNOME).


**Figura 24-1. Ferramenta de Configuração do Servidor Samba**

**Nota**

A **Ferramenta de Configuração do Servidor Samba** não exibe impressoras compartilhadas ou a estrofe default que permite a usuários visualizarem seus próprios diretórios home no servidor Samba.

#### 24.2.1.1. Definindo as Configurações do Servidor

O primeiro passo para configurar um servidor Samba é definir as configurações básicas e algumas opções de segurança. Após iniciar a aplicação, selecione **Preferências => Configurações do Servidor** no menu suspenso. A aba **Básica** é exibida conforme a Figura 24-2.

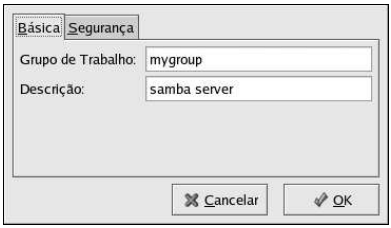


**Figura 24-2. Definindo as Configurações Básicas do Servidor**

Na aba **Básica**, especifique em qual grupo de trabalho o computador deve estar, assim como uma breve descrição do computador. Estas correspondem às opções `workgroup` e `server string` do arquivo `smb.conf`.

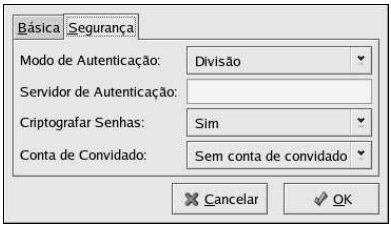


**Figura 24-3. Definindo as Configurações de Segurança do Servidor**

A aba **Segurança** contém as seguintes opções:

- **Modo de Autenticação** — Corresponde à opção `segurança`. Selecione um dos tipos de autenticação a seguir.
  - **ADS** — O servidor Samba atua como um membro do domínio em um reino de Domínio de Diretório Ativo (ADS - Active Directory Domain ). Para esta opção, o Kerberos deve estar instalado e configurado no servidor, e o Samba deve tornar-se um membro do reino ADS, usando o utilitário `net`, parte do pacote `samba-client`. Consulte a página man do `net` para mais detalhes. Esta opção não configura o Samba para ser um Controlador ADS.
  - **Domínio** — O servidor Samba baseia-se em um Controlador de Domínio de Backup ou Primário do Windows NT para verificar o usuário. O servidor passa o nome e senha do usuário ao Controlador e espera que ele retorne. Especifique o nome do NetBIOS do Controlador de Domínio de Backup ou Primário no campo **Servidor de Autenticação**.

    A opção **Senhas Criptografadas** deve ser definida como **Sim** se esta for selecionada.
  - **Servidor** — O servidor Samba tenta verificar a combinação nome e senha do usuário passando-os para outro servidor Samba. Se não puder fazer isso, o servidor tenta verificar usando o modo de autenticação do usuário. Especifique o nome NetBIOS do outro servidor Samba no campo **Servidor de Autenticação**.
  - **Partilha** — Os usuários do Samba não precisam indicar uma combinação de nome e senha em cada servidor do Samba. Não é necessário indicar nome e senha do usuário até que tente conectar a um diretório compartilhado específico através de um servidor Samba.
  - **Usuário** — (Default) usuários do Samba devem prover um nome e senha de usuário válidos em cada servidor do Samba. Selecione esta opção se você deseja que a opção **Nome do Usuário do Windows** funcione. Consulte a Seção 24.2.1.2 para mais detalhes.

- **Criptografar Senhas** — Esta opção deve ser habilitada se os clientes estão conectando a partir de um Windows 98, Windows NT 4.0 com Pacote de Serviço 3, ou outras versões mais recentes do Microsoft Windows. As senhas são transferidas entre o servidor e o cliente de forma criptografada, ao invés da forma em texto puro, que é fácil de ser interceptada. Isto corresponde à opção `senhas criptografadas`. Consulte a Seção 24.2.3 para mais informações sobre senhas criptografadas do Samba.
- **Conta Convidado** — Quando usuários ou usuários convidados se autenticam no servidor Samba, devem ser mapeados a um usuário válido no servidor. Selecione um dos nomes de usuários existentes no sistema para ser a conta convidado do Samba. Quando os convidados se autenticarem no servidor Samba, eles têm os mesmos privilégios que o usuário. Isto corresponde à opção `guest account`.

Após clicar em **OK**, as alterações são gravadas no arquivo de configuração e o daemon é reiniciado; portanto, as alterações têm efeito imediato.

#### 24.2.1.2. Administrando Usuários do Samba

A **Ferramenta de Configuração do Servidor Samba** requer que uma conta de usuário existente esteja ativa no sistema, atuando como o servidor Samba antes que um usuário do Samba possa ser adicionado. O usuário do Samba é associado à conta de usuário existente.

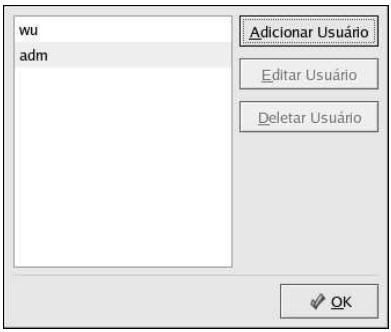


**Figura 24-4. Administrando Usuários do Samba**

Para adicionar um usuário ao Samba, selecione **Preferências => Usuários do Samba** no menu suspenso e clique no botão **Adicionar Usuário**. Na janela **Criar Novo Usuário do Samba**, selecione **Nome de Usuário Unix** na lista de usuários existentes no sistema local.

Se o usuário tem um nome de usuário diferente em uma máquina Windows e se autenticará no servidor Samba pela máquina Windows, especifique este nome de usuário Windows no campo **Nome de Usuário Windows**. O **Modo de Autenticação** na aba **Segurança** das preferências das **Configurações do Servidor** deve ser definido para **Usuário** para que esta opção funcione.

Também configure uma **Senha do Samba** para o Usuário do Samba e confirme-a digitando-a novamente. Mesmo se você selecionar usar senhas criptografadas para o Samba, é recomendado que as senha do Samba para todos os usuários sejam diferentes das suas senhas de sistema.

Para editar um usuário existente, selecione-o na lista e clique em **Editar Usuário**. Para apagar um usuário do Samba, selecione-o e clique no botão **Apagar Usuário**. Apagar um usuário do Samba não apaga a conta de usuário associada no sistema.

Os usuários são modificados imediatamente após clicar no botão **OK**.

#### 24.2.1.3. Adicionando uma Partilha

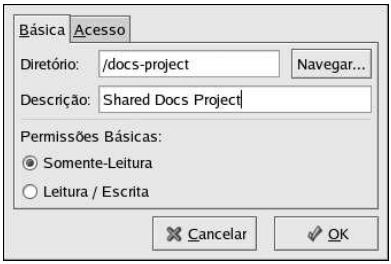


**Figura 24-5. Adicionando uma Partilha**

Para adicionar uma partilha, clique no botão **Adicionar**. A aba **Básica** configura as seguintes opções:

- **Diretório** — O diretório a compartilhar via Samba. O diretório deve existir.
- **Descrições** — Uma breve descrição da partilha.
- **Permissões Básicas** — Determina se os usuários podem ler (read) os arquivos no diretório compartilhado ou se podem ler e gravar (read and write) no diretório compartilhado.

Na aba **Acesso**, selecione se permitirá que somente usuários especificados ou se permitirá que todos os usuários do Samba acessem a partilha. Se você selecionar permitir o acesso de usuários específicos, selecione os usuários na lista de usuários disponíveis do Samba.

A partilha é adicionada imediatamente após clicar em **OK**.

### 24.2.2. Configuração na Linha de Comandos

O Sama usa o `/etc/samba/smb.conf` como seu arquivo de configuração. Se você alterá-lo, as alterações não têm efeito até que reinicie o daemon do Samba com o comando `service smb restart`.

Para especificar o grupo de trabalho do Windows e uma breve descrição do servidor Samba, edite as seguintes linhas de seu arquivo `smb.conf`:

```
workgroup = WORKGROUPNAME
server string = BRIEF COMMENT ABOUT SERVER
```

Substitua *`WORKGROUPNAME`* pelo nome do grupo de trabalho do Windows ao qual esta máquina deve pertencer. O *`BRIEF COMMENT ABOUT SERVER`* é opcional e é usado como o comentário do Windows sobre o sistema Samba.

Para criar um diretório da partilha Samba no seu sistema Linux, adicione a seguinte seção ao seu arquivo `smb.conf` (após modificá-lo para refletir suas necessidades e sistema):

```
[sharename]
comment = Insert a comment here
path = /home/share/
valid users = tfox carole
public = no
writable = yes
printable = no
create mask = 0765
```

O exemplo acima permite aos usuários tfox e carole ler e gravar (read and write) no diretório `/home/share`, no servidor Samba, a partir de um cliente Samba.

### 24.2.3. Senhas Criptografadas

Senhas criptografadas são habilitadas por default porque são mais seguras. Se as senhas criptografadas não forem usadas, serão usadas senhas em texto puro, que podem ser interceptadas por alguém usando um sniffer de pacote de rede. É recomendado usar as senhas criptigrafadas.

O Protocolo SMB da Microsoft originalmente usava senhas em texto puro. No entanto, o Windows NT 4.0 com Pacote de Serviço 3 ou mais recente, Windows 98, Windows 2000, Windows ME e o Windows XP requerem senhas do Samba criptografadas. Para usar o Samba entre um sistema Linux e um sistema usando um destes sistemas operacionais Windows, você pode editar seu registro Windows para usar senhas em texto puro ou configurar o Samba em seu sistema Linux para usar senhas criptografadas. Se optar por mudar seu registro, deve fazê-lo em todas as máquinas Windows — isto é arriscado e pode causar conflitos futuros. Para sua maior segurança, recomendamos o uso de senhas criptografadas.

Para configurar o Samba a usar senhas criptografadas, siga estes passos:

1. Crie um arquivo de senhas separado para o Samba. Para criar um baseado em seu arquivo `/etc/passwd` existente, digite o seguinte em uma janela de comandos:
   ```
   cat /etc/passwd | mksmbpasswd.sh > /etc/samba/smbpasswd
   ```
   Se o sistema usa NIS, digite o seguinte comando:
   ```
   ypcat passwd | mksmbpasswd.sh > /etc/samba/smbpasswd
   ```
   O script `mksmbpasswd.sh` é instalado em seu diretório `/usr/bin` com o pacote `samba`.
2. Altere as permissões do arquivo de senhas do Samba para que somente root tenha permissões de leitura e gravação (read and write).
   ```
   chmod 600 /etc/samba/smbpasswd
   ```
3. O script não copia senhas de usuários ao novo arquivo, e uma conta de usuário do Samba não está ativa até que uma senha seja definida para esta. Para maior segurança, é recomendado que a senha Samba dos usuários seja diferente da senha do usuário no sistema. Para cada senha de usuário no Samba, use o seguinte comando (substitua *`username`* pelo nome de cada usuário):
   ```
   smbpasswd username
   ```
4. As senhas criptografadas devem ser habilitadas. Como estas são habilitadas por default, não precisam ser especificamente habilitadas no arquivo de configuração. Entretanto, também não podem ser desabilitadas no arquivo de configuração. No arquivo `/etc/samba/smb.conf`, certifique de que a linha seguinte não existe:
   ```
   encrypt passwords = no
   ```
   Se existir, mas for comentada com um ponto e vírgula (`;`) no começo da linha, então a inha é ignorada e as senhas criptografadas são habilitadas. Se esta linha existir, mas não for comentada, remova-a ou comente-a.

   Para habilitar especificamente as senhas criptografadas no arquivo de configuração, adicione as linhas seguintes ao `etc/samba/smb.conf`:
   ```
   encrypt passwords = yes
   smb passwd file = /etc/samba/smbpasswd
   ```
5. Assegure que o serviço `smb` seja iniciado, digitando o comando `service smb restart` em uma janela de comandos.
6. Se você deseja que o serviço `smb` inicie automaticamente, use a **ntsysv**, `chkconfig` ou a **Ferramenta de Configuração dos Serviços** para habilitá-lo na hora da execução. Consulte o Capítulo 21 para mais detalhes.

O módulo PAM `pam_smbpass` pode ser usado para sincronizar senhas Samba de usuários com suas senhas no sistema quando o comando `passwd` for usado. Se um usuário invocar o comando `passwd`, a senha que ele usa para autenticar-se no sistema Red Hat Enterprise Linux e a senha usada para conectar à partilha do Samba são alteradas.

Para habilitar esta funcionalidade, adicione a linha seguinte ao `/etc/pam.d/system-auth` abaixo de `pam_cracklib.so`:

```
password required /lib/security/pam_smbpass.so nullok use_authtok try_first_pass
```

### 24.2.4. Iniciando e Parando o Servidor

O serviço `smb` deve estar rodando no servidor que está compartilhando diretórios através do Samba.

Visualize o estado do daemon do Samba com o seguinte comando:

```
/sbin/service smb status
```

Inicie o daemon com o seguinte comando:

```
/sbin/service smb start
```

Pare o daemon com o seguinte comando:

```
/sbin/service smb stop
```

Para iniciar o serviço `smb` no momento da inicialização, use o comando:

```
/sbin/chkconfig --level 345 smb on
```

Você também pode usar `chkconfig`, **ntsysv** ou a **Ferramenta de Configuração dos Serviços** para configurar quais serviços iniciar no momento da inicialização. Consulte o Capítulo 21 para mais detalhes.

**Dica**

Para visualizar as conexões ativas do sistema, execute o comando `smbstatus`.

## 24.3. Conectando a uma Partilha Samba

Você pode usar o **Nautilus** para visualizar as partilhas do Samba disponíveis em sua rede. Selecione o **Botão do Menu Principal** (no Painel) => **Servidores de Rede** para visualizar uma lista dos grupos de trabalho do Samba em sua rede. Você também pode digitar **`smb:`** na barra **Localidade:** do Nautilus para visualizar os grupos de trabalho.

Conforme mostra a Figura 24-6, aparece um ícone para cada grupo de trabalho SMB disponível na rede.

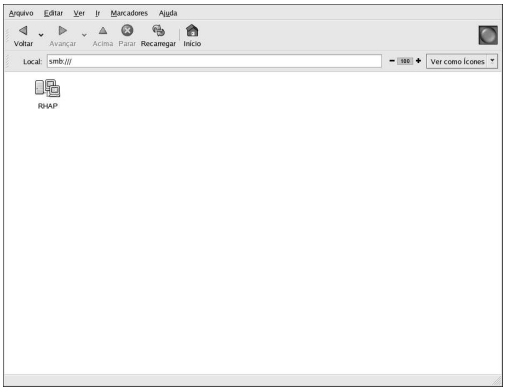


**Figura 24-6. Grupos de Trabalho SMB no Nautilus**

Duplo-clique em um dos ícones de grupo de trabalho para visualizar uma lista de componentes deste grupo de trabalho.

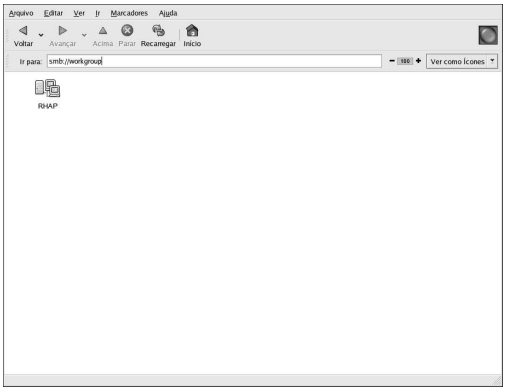


**Figura 24-7. Máquinas SMB no Nautilus**

Como você pode observar na Figura 24-7, há um ícone para cada máquina dentro do grupo de trabalho. Duplo-clique em um ícone para visualizar as partilhas Samba na máquina. Se for necessária ujma combinação de nome senha de usuário, você deverá inserí-los.

Alternativamente, você também pode especificar o servidor e o nome da partilha do Samba na barra **Localidade:** do **Nautilus** usando a seguinte sintaxe (substitua *<servername>* e *<sharename>* pelos valores apropriados):

```
smb://<servername>/<sharename>/
```

### 24.3.1. Linha de Comandos

Para buscar servidores Samba na rede, use o comando `findsmb`. Para cada servidor encontrado, ele exibe seu endereço IP, nome NetBIOS, nome do grupo de trabalho, sistema operacional e versão do servidor SMB.

Para conectar a uma partilha Samba pela janela de comandos, digite o seguinte:

```
smbclient //<hostname>/<sharename> -U <username>
```

Substitua <*hostname*> pelo nome da máquina ou endereço IP do servidor Samba ao qual deseja conectar; <*sharename*> pelo nome do diretório compartilhado onde você deseja navegar (browse); e <*username*> pelo nome do usuário Samba para o sistema. Indique a senha correta ou pressione [Enter] se não forem necessárias senhas para o usuário.

Se você ver o prompt `smb:\>`, se autenticou com sucesso. Após se autenticar, digite **`help`** para obter uma lista de comandos. Se deseja navegar pelo conteúdo de seu diretório home, substitua *sharename* pelo seu nome de usuário. Se o comutador `-U` é usado, o nome do usuário corrente é passado ao servidor do Samba.

Para sair do `smbclient`, digite **`exit`** em um prompt `smb:\>`.

### 24.3.2. Montando a Partilha

Às vezes, é útil montar uma partilha Samba em um diretório, para que os arquivos deste diretório sejam tratados como parte do sistema de arquivo local.

Para montar uma partilha Samba em um diretório, crie o diretório (se já não existir) e execute o seguinte comando como root:

```
mount -t  smbfs -o username=<username> //<servername>/<sharename> /mnt/point/
```

Este comando monta a <*sharename*>a partir do <*servername*> no diretório local */mnt/point/*.

## 24.4. Recursos Adicionais

Para opções de configuração não abordadas aqui, por favor consulte os seguintes recursos.

### 24.4.1. Documentação Instalada

- Página man do `smb.conf` — explica como configurar o arquivo de configuração do Samba
- Página man do `smbd` — descreve como o daemon do Samba funciona
- Páginas man do `smbclient` e do `findsmb` — aprenda mais sobre estas ferramentas do cliente
- `/usr/share/doc/samba-`<*version-number*>`/docs/` — arquivos de ajuda inclusos no pacote `samba`

### 24.4.2. Sites Úteis

- http://www.samba.org/ — A homepage do Samba contém uma documentação útil, informações sobre listas de discussão e uma lista de interfaces gráficas (GUI).
- http://www.samba.org/samba/docs/using_samba/toc.html — uma versão online de *Using Samba, 2nd Edition* por Jay Ts, Robert Eckstein e David Collier-Brown; O'Reilly & Associates

redhat.

Capítulo 25.

# Protocolo de Configuração Dinâmica de Máquina (Dynamic Host Configuration Protocol - DHCP)

O Protocolo de Configuração Dinâmica de Máquina (DHCP) é um protocolo para atribuir informações TCP/IP automaticamente para máquinas cliente. Cada cliente DHCP conecta ao servidor DHCP centralmente localizado, que retorna esta configuração de rede do cliente, inclusive o endereço IP, porta de comunicação (gateway) e servidores DNS.

## 25.1. Por que usar o DHCP?

O DHCP é útil para a última entrega da configuração de rede do cliente. Ao configurar o sistema cliente, o administrador pode optar pelo DHCP e não ter que inserir o endereço IP, a máscara de rede, a porta de comunicação ou os servidores DNS. O cliente recupera estas informações no servidor DHCP. O DHCP também é útil se um administrador deseja alterar os endereços IP de um número grande de sistemas. Ao invés de reconfigurar todos os sistemas, ele pode simplesmente editar um arquivo de configuração DHCP no servidor para o novo conjunto de endereços IP. Se os servidores DNS de uma empresa forem alterados, as alterações são feitas no servidor DHCP e não nos clientes DHCP. Após reiniciar a rede nos clientes (ou reinicializar os clientes), as alterações tomam efeito.

Mais adiante, se um laptop ou qualquer tipo de computador portátil é configurado para DHCP, pode ser transportado de um escritório para outro sem precisar reconfigurar, desde que cada escritório tenha um servidor DHCP que permita conectá-lo à rede.

## 25.2. Configurando um Servidor DHCP

Para configurar um servidor DHCP, altere o arquivo de configuração `/etc/dhcpd.conf`.

O DHCP também usa o arquivo `/var/lib/dhcp/dhcpd.leases` para armazenar o banco de dados de aluguel de clientes. Consulte a Seção 25.2.2 para mais informações.

### 25.2.1. Arquivo de Configuração

O primeiro passo para configurar um servidor DHCP é criar o arquivo de configuração que armazena as informações de rede dos clientes. É possível declarar opções globais para todos os clientes, e também declarar opções para cada sistema cliente separadamente.

O arquivo de configuração pode conter espaços tab ou linhas em branco para uma formatação mais fácil. As palavras-chave são sensíveis a caixa alta e baixa, e as linhas iniciadas com a marca do jogo da velha (#) são consideradas comentários.

Atualmente são implementados dois esquemas de atualização do DNS — o modo de atualização do DNS improvisado e o modo de atualização do esquema de interação do intervalo DHCP-DNS. Se e quando estes dois são aceitos como parte do processo padrão IETF, haverá um terceiro modo — o método de atualização do DNS padrão. O servidor DHCP deve ser configurado para usar um dos dois esquemas atuais. A versão 3.0b2pl11 e a anterior usaram o modo improvisado; no entanto, este foi desaprovado. Para manter o mesmo comportamento, adicione a linha seguinte no topo do arquivo de configuração:

```
ddns-update-style ad-hoc;
```

Para usar o modo recomendado, adicione a seguinte linha no topo do arquivo de configuração:

```
ddns-update-style interim;
```

Consulte a página man do `dhcpd.conf` para detalhes sobre os diferentes modos.

Há dois tipos de declarações no arquivo de configuração:

- Parâmetros — determinam como executar uma tarefa, se deve-se executar a tarefa, ou quais opções de configuração de rede devem ser enviadas ao cliente.
- Declarações — descrevem a topologia da rede e os clientes, provêm endereços para os clientes, ou aplicam um grupo de parâmetros a um grupo de declarações.

Alguns parâmetros devem iniciar com a palavra-chave `option` e são referidos como opções. Elas configuram as opções DHCP; enquanto os parâmetros configuram os valores não-opcionais ou controlam o modo como o servidor DHCP se comporta.

Os parâmetros (incluindo as opções) declarados antes do fechamento de uma seção com chaves ({ }) são considerados globais. Os parâmetros globais são aplicados a todas as seções abaixo deles.

**Importante**

Se o arquivo de configuração é alterado, as alterações não terão efeito até que o daemon DHCP seja reiniciado com o comando `service dhcpd restart`.

Na Exemplo 25-1, as opções `routers`, `subnet-mask`, `domain-name`, `domain-name-servers` e `time-offset` são usadas para qualquer declaração de `host` abaixo delas.

Conforme mostra a Exemplo 25-1, uma `subnet` pode ser declarada. Uma declaração da `subnet` deve ser inclusa para cada sub-rede na rede. Se não for, o servidor DHCP falha na inicialização.

Neste exemplo há opções globais para cada cliente DHCP da sub-rede e um `range` (intervalo) declarado. Clientes são atribuídos com um endereço IP dentro do `range`.

```
subnet 192.168.1.0 netmask 255.255.255.0 {
        option routers                  192.168.1.254;
        option subnet-mask              255.255.255.0;

        option domain-name              "example.com";
        option domain-name-servers       192.168.1.1;

        option time-offset              -18000;     # Eastern Standard Time

 range 192.168.1.10 192.168.1.100;
}
```

**Exemplo 25-1. Declaração de Sub-rede**

Todas as sub-redes que compartilham a mesma rede física devem ser indicados em uma declaração `shared-network`, conforme mostra a Exemplo 25-2. Os parâmetros dentro da `shared-network` mas fora das declarações `subnet` fechadas são considerados globais. O nome da `shared-network` dever ser um título descritivo da rede, como test-lab, para descrever todas as sub-redes de um ambiente de laboratório de testes.

```
shared-network name {
    option domain-name              "test.redhat.com";
    option domain-name-servers      ns1.redhat.com, ns2.redhat.com;
    option routers                  192.168.1.254;
    more parameters for EXAMPLE shared-network
    subnet 192.168.1.0 netmask 255.255.255.0 {
        parameters for subnet
        range 192.168.1.1 192.168.1.31;
    }
    subnet 192.168.1.32 netmask 255.255.255.0 {
        parameters for subnet
        range 192.168.1.33 192.168.1.63;
    }
}
```

**Exemplo 25-2. Declaração de Rede Compartilhada**

Como demonstrado na Exemplo 25-3, a declaração de `group` pode ser usada para aplicar parâmetros globais a um grupo de declarações. Por exemplo: redes compartilhadas (shared networks), sub-redes (subnets), máquinas (hosts) ou outros grupos podem ser agrupados.

```
group {
   option routers                  192.168.1.254;
   option subnet-mask              255.255.255.0;

   option domain-name              "example.com";
   option domain-name-servers       192.168.1.1;

   option time-offset              -18000;     # Eastern Standard Time

   host apex {
      option host-name "apex.example.com";
      hardware ethernet 00:A0:78:8E:9E:AA;
      fixed-address 192.168.1.4;
   }

   host raleigh {
      option host-name "raleigh.example.com";
      hardware ethernet 00:A1:DD:74:C3:F2;
      fixed-address 192.168.1.6;
   }
}
```

**Exemplo 25-3. Declaração de Grupo**

Para configurar um servidor DHCP que aluga um endereço IP dinâmico para um sistema em uma sub-rede, modifique o Exemplo 25-4 com seus valores. Este declara um tempo default de aluguel, um tempo máximo de aluguel e valores de configuração de rede dos clientes. Este exemplo atribui endereços IP no `range` 192.168.1.10 a 192.168.1.100 para sistemas cliente.

```
default-lease-time 600;
max-lease-time 7200;
option subnet-mask 255.255.255.0;
option broadcast-address 192.168.1.255;
option routers 192.168.1.254;
option domain-name-servers 192.168.1.1, 192.168.1.2;
option domain-name "example.com";

subnet 192.168.1.0 netmask 255.255.255.0 {
   range 192.168.1.10 192.168.1.100;
}
```

**Exemplo 25-4. Parâmetro de Escala**

Para atribuir um endereço IP a um cliente, baseado no endereço MAC da placa de interface da rede, use o parâmetro `hardware ethernet` em uma declaração `host`. Conforme mostra a Exemplo 25-5, a declaração `host apex` especifica que a placa de interface de rede com o endereço MAC 00:A0:78:8E:9E:AA sempre recebe o endereço IP 192.168.1.4.

Note que o parâmetro opcional `host-name` pode ser usado para atribuir um nome de máquina para o cliente.

```
host apex {
   option host-name "apex.example.com";
   hardware ethernet 00:A0:78:8E:9E:AA;
   fixed-address 192.168.1.4;
}
```

**Exemplo 25-5. Endereço IP Estático usando DHCP**

**Dica**

A amostra do arquivo de configuração provido pode ser usada como um ponto de partida. Opções personalizadas de configuração podem ser adicionadas a ele. Para copiá-lo à localidade apropriada, use o segunte comando:

```
cp /usr/share/doc/dhcp-<version-number>/dhcpd.conf.sample /etc/dhcpd.conf
```

(onde <*version-number*> é o número da versão do DHCP).

Para uma lista completa das opções de declaração e suas funções, consulte a página man `dhcp-options`.

### 25.2.2. Banco de Dados de Aluguel

No servidor DHCP, o arquivo `/var/lib/dhcp/dhcpd.leases` armazena o banco de dados de aluguel do cliente DHCP. Este arquivo não deve ser modificado manualmente. As informações de aluguel DHCP de cada endereço IP recentemente atribuído são armazenadas automaticamente no banco de dados de aluguel. As informações incluem datas do aluguel e os endereços MAC da placa de interface de rede usada para recuperar o aluguel.

Todos os horários do banco de dados de aluguel estão em GMT (Greenwich Mean Time) e não horário local.

O banco de dados de aluguel é recriado de tempos em tempos para que não fique muito grande. Primeiramente, todos os aluguéis conhecidos são salvos em um banco de dados temporário de aluguel. Então, o arquivo `dhcpd.leases` é renomeado para `dhcpd.leases~`, e o banco de dados temporário é salvo como `dhcpd.leases`.

O daemon DHCP pode ser finalizado (killed) ou o sistema pode falhar (crash) após o banco de dados de aluguel ter sido renomeado como o arquivo backup, mas antes do novo arquivo ser salvo. Se isto acontecer, o arquivo `dhcpd.leases` não existe, mas é necessário para iniciar o serviço. Não crie um novo arquivo de aluguel. Se você o fizer, todos os aluguéis antigos serão perdidos e causarão muitos problemas. A solução correta é renomear o arquivo backup `dhcpd.leases~` como `dhcpd.leases` e então iniciar o daemon.

### 25.2.3. Iniciando e Parando o Servidor

**Importante**

Quando o servidor DHCP é iniciado pela primeira vez, ele falhará a não ser que o arquivo `dhcpd.leases` exista. Use o comando `touch /var/lib/dhcp/dhcpd.leases` para criar este arquivo se ainda não existir.

Para iniciar o serviço DHCP, use o comando `/sbin/service dhcpd start`. Para parar o servidor DHCP, use o comando `/sbin/service dhcpd stop`. Para configurar o daemon para inciar automaticamente no momento da inicialização, consulte o Capítulo 21 para informações sobre a administração dos serviços.

Se houver mais de uma interface de rede ligada ao sistema, mas o servidor DHCP deve ser iniciado em apenas uma das inaterfaces, configure o servidor para iniciar somente naquele dispositivo. No `/etc/sysconfig/dhcpd`, adicione o nome da interface à lista de `DHCPDARGS`:

```
# Command line options here
DHCPDARGS=eth0
```

Isto é útil para uma máquina firewall com duas placas de rede. Uma placa de rede pode ser configurada como um cliente DHCP para recuperar um endereço IP para a Internet. A outra placa de rede pode ser usada como um servidor DHCP da rede interna por trás do firewall. Especificar somente a placa de rede ligada à rede interna torna o sistema mais seguro, porque os usuários podem conectar ao daemon via Internet.

Outras opções de comando de linha que podem ser usadas no `/etc/sysconfig/dhcpd` incluem:

- `-p <portnum>` — Especifica o número da porta udp que deve ser escutada pelo `dhcpd`. A porta default é a 67. O servidor DHCP transmite respostas aos clientes DHCP em uma porta de um número maior que a porta udp especificada. Por exemplo: se a porta default usada é a 67, o servidor escuta na porta 67 por pedidos e responde ao cliente na porta 68. Se a porta é especificada aqui e o agente DHCP relay é usado, deve-se especificar a mesma porta na qual o agente DHCP relay escuta. Consulte o Seção 25.2.4 para mais detalhes.
- `-f` — Roda o daemon como um processo em primeiro plano. Isto é usado principalmente para a depuração.
- `-d` — Registra o daemon do servidor DHCP no descirtor de erro padrão. Isto é usado principalmente para a depuração. Se não é especificado, o registro é salvo como `/var/log/messages`.
- `-cf <filename>` — Especifica a localidade do arquivo de configuração. A localidade default é `/etc/dhcpd.conf`.

- `-lf <filename>` — Especifica a localidade do arquivo de banco de dados de aluguel. Se este arquivo já existir, é muito importante usar o mesmo arquivo toda vez que o servidor DHCP é iniciado. É altamente recomendado que esta opção seja usada somente para fins de depuração em máquinas que não sejam de produção. A localidade default é `/var/lib/dhcp/dhcpd.leases`.
- `-q` — Não imprime a mensagem de direitos autorais na íntegra ao iniciar o daemon.

### 25.2.4. Agente DHCP Relay

O Agente DHCP Relay (`dhcrelay`) permite o revezamento de pedidos DHCP e BOOTP de uma sub-rede sem um servidor DHCP, para um ou mais servidores DHCP em outras sub-redes.

Quando um cliente DHCP solicita informações, o Agente DHCP Relay encaminha o pedido à lista de servidores DHCP especificada quando o Agente DHCP Relay é iniciado. Quando um servidor DHCP retorna uma resposta, esta deve ser transmitida amplamente ou somente para a rede que enviou o pedido original.

O Agente DHCP Relay escuta pedidos DHCP em todas as interfaces, a não ser que as interfaces estejam especificadas no `/etc/sysconfig/dhcrelay` com a diretiva `INTERFACES`.

Para iniciar o Agente DHCP Relay, use o comando `service dhcrelay start`.

## 25.3. Configurando um Cliente DHCP

Este primeiro passo para configurar um cliente DHCP é certificar-se de que o kernel reconhece a placa de interface de rede. A maioria das placas são reconhecidas durante o processo de instalação, e o sistema é configurado para usar o módulo correto do kernel para a placa. Se uma placa é adicionada após a instalação, o **Kudzu**[1] deve reconhecê-la e pedir pela configuração do módulo correspondente do kernel. Certifique-se de verificar a Lista de Compatibilidade de Hardware, disponível online: http://hardware.redhat.com/hcl/. Se a placa de rede não for configurada pelo programa de instalação ou pelo **Kudzu** e você sabe qual módulo do kernel carregar para esta, consulte o Capítulo 40 para detalhes sobre o carregamento de módulos do kernel.

Para configurar um cliente DHCP manualmente, modifique o arquivo `/etc/sysconfig/network` para habilitar o networking e o arquivo de configuração de cada dispositivo de rede no diretório `/etc/sysconfig/network-scripts`. Neste diretório, cada dispositivo deve ter um arquivo de configuração nomeado `ifcfg-eth0`, onde `eth0` é o nome do dispositivo de rede.

O arquivo `/etc/sysconfig/network` deve conter a seguinte linha:

```
NETWORKING=yes
```

A variável `NETWORKING` deve ser definida para `yes` se você deseja que o networking seja iniciado no momento da inicialização da máquina.

O arquivo `/etc/sysconfig/network-scripts/ifcfg-eth0` deve conter as seguintes linhas:

```
DEVICE=eth0
BOOTPROTO=dhcp
ONBOOT=yes
```

É necessário um arquivo de configuração para cada dispositivo a ser configurado para usar DHCP.

Outras opções para o script de rede incluem:

1. **Kudzu** é uma ferramenta de detecção de hardware executada no momento da inicialização para determinar o hardware adicionado ou removido do sistema.

- `DHCP_HOSTNAME` — Use esta opção somente se o servidor DHCP requer que o cliente especifique um nome de máquina antes de receber um endereço IP. (O daemon do servidor DHCP no Red Hat Enterprise Linux não suporta esta funcionalidade.)
- `PEERDNS=<answer>`, onde `<answer>` é um dos seguintes:
  - `yes` — Modifique o `/etc/resolv.conf` com informações do servidor. Se estiver usando DHCP, a opção `yes` é a default.
  - `no` — Não modifique o `/etc/resolv.conf`.

- `SRCADDR=<address>`, onde `<address>` é o endereço IP fonte especificado para pacotes saindo (outgoing).
- `USERCTL=<answer>`, onde `<answer>` é um dos seguintes:
  - `yes` — É permitido a usuários não-root controlar este dispositivo.
  - `no` — Não é permitido a usuários não-root controlar este dispositivo.

Para uma interface gráfica de configuração de um cliente DHCP, consulte o Capítulo 19 para detalhes sobre o uso da **Ferramenta de Administração de Rede** para configurar uma interface de rede para usar DHCP.

## 25.4. Recursos Adicionais

Para opções de configuração não abordadas aqui, consulte os seguintes recursos.

### 25.4.1. Documentação Instalada

- Página man do `dhcpd` — descreve como funciona o daemon DHCP
- Página man do `dhcpd.conf` — explica como configurar o arquivo de configuração DHCP, incluindo alguns exemplos
- Página man do `dhcpd.leases` — explica como configurar o arquivo de aluguéis DHCP, incluindo alguns exemplos
- Página man do `dhcp-options` — explica a sintaxe para declarar opções DHCP no `dhcpd.conf`, incluindo alguns exemplos
- Página man do `dhcrelay` — explica o Agente DHCP Relay e suas opções de configuração.

Capítulo 26.

# Configuração do Servidor HTTP Apache

O Red Hat Enterprise Linux oferece a versão 2.0 do Servidor HTTP Apache. Se você deseja migrar um arquivo de configuração existente manualmente, consulte o manual de migração em `/usr/share/doc/httpd-<ver>/migration.html` ou o *Guia de Referência do Red Hat Enterprise Linux* para mais detalhes.

Se você configurou o Servidor HTTP Apache com a **Ferramenta de Configuração do HTTP** nas versões anteriores do Red Hat Enterprise Linux e então executou uma atualização, pode usar a **Ferramenta de Configuração do HTTP** para migrar o arquivo de configuração para o novo formato da versão 2.0. Inicie a **Ferramenta de Configuração do HTTP**, faça quaisquer alterações na configuração e salve-as. O arquivo de configuração salvo será compatível com a versão 2.0.

A **Ferramenta de Configuração do HTTP** permite que você configure o arquivo de configuração `/etc/httpd/conf/httpd.conf` para o Servidor HTTP Apache. Ela não usa os arquivos de configuração antigos, `srm.conf` ou `access.conf`; deixe-os vazios. Através da interface gráfica, é possível configurar diretivas como virtual hosts (máquinas virtuais), logging attributes (atributos de autenticação) e maximum number of connections (número máximo de conexões).

Somente os módulos oferecidos pelo Red Hat Enterprise Linux podem ser configurados com a **Ferramenta de Configuração do HTTP**. Se instalar módulos adicionais, eles não poderão ser configurados usando esta ferramenta.

Os pacotes RPM `httpd` e `redhat-config-httpd` precisam ser instalados para usar a **Ferramenta de Configuração do HTTP**. Esta também requer o Sistema X Window e acesso root. Para iniciar a aplicação, vá para **Botão do Menu Principal => Configurações do Sistema => Configurações do Servidor => HTTP** ou digite o comando `redhat-config-httpd` em uma janela de comandos (em um Xterm ou um Terminal GNOME, por exemplo).

**Cuidado**

Não edite o arquivo de configuração `/etc/httpd/conf/httpd.conf` manualmente se você deseja usar esta ferramenta. A **Ferramenta de Configuração do HTTP** gera este arquivo após você salvar suas alterações e sair do programa. Se quiser adicionar outros módulos ou opções de configuração que não estão disponíveis na **Ferramenta de Configuração do HTTP**, você não pode usar esta ferramenta.

As instruções gerais para configurar o Servidor HTTP Apache usando a **Ferramenta de Configuração do HTTP** são as seguintes:

1. Defina as configurações básicas na aba **Principal** (main).
2. Clique na aba **Máquinas Virtuais** e defina as configurações default.
3. Na aba **Máquinas Virtuais**, configure a Máquina Virtual Default.
4. Se você quer oferecer mais de uma URL ou máquina virtual, adicione as máquinas virtuais.
5. Defina as configurações do servidor na aba **Servidor**.
6. Defina as configurações das conexões na aba **Ajuste de Desempenho** (Performance Tuning).
7. Copie todos os arquivos necessários nos diretórios `DocumentRoot` e `cgi-bin`.
8. Saia da aplicação e escolha salvar suas configurações.

## 26.1. Configurações Básicas

Use a aba **Principal** para definir as configurações básicas do servidor.

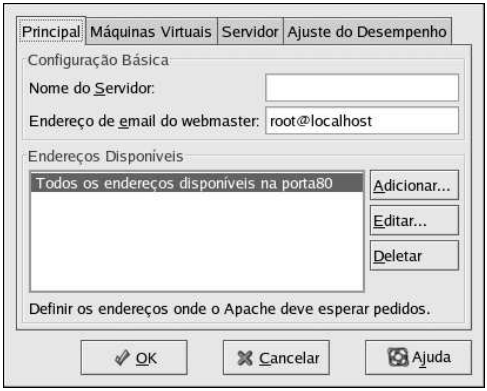


**Figura 26-1. Configurações Básicas**

Insira um nome de domínio totalmente qualificado que você possa usar no campo **Nome do Servidor**. Esta opção corresponde à diretiva `ServerName`no `httpd.conf`. A diretiva `ServerName` define o nome da máquina do servidor web. É usada ao criar URLs de redirecionamento. Se você não definir um nome para o servidor, o servidor web tenta descobrir pelo endereço IP do sistema. O nome do servidor não precisa ser o nome de domínio descoberto pelo endereço IP. Por exemplo: você pode querer definir o nome do servidor como www.exemplo.com enquanto nome DNS real do seu servidor é, na verdade, foo.exemplo.com.

Insira o endereço de e-mail da pessoa que mantém o servidor web no campo **Endereço de e-mail do webmaster**. Esta opção corresponde à diretiva `ServerAdmin` no `httpd.conf`. Se você configurar as páginas de erro do servidor para conter um endereço de e-mail, este endereço será usado para que os usuários possam reportar um problema através de um e-mail para o administrador do servidor. O e-mail default é root@localhost.

Use o campo **Endereços Disponíveis** para definir as portas através das quais cada servidor aceitará a entrada de pedidos. Esta opção corresponde à diretiva `Listen` no `httpd.conf`. Por default, a Red Hat configura o Servidor HTTP Apache para escutar na porta 80 por comunicações web não-seguras.

Clique no botão **Adicionar** para definir portas adicionais das quais aceitar pedidos. Aparecerá uma janela, conforme a Figura 26-2. Escolha a opção **Escutar todos endereços** para escutar todos os endereços IP na porta definida, ou então especifique um endereço IP através do qual o servidor aceitará as conexões no campo **Endereço**. Especifique apenas um endereço IP por número de porta. Se quiser especificar mais de um endereço IP com o mesmo número de porta, crie uma entrada para cada endereço IP. Se for possível, use um endereço IP ao invés de um nome de domínio para evitar uma falha de pesquisa do DNS. Visite http://httpd.apache.org/docs-2.0/dns-caveats.html para mais informações sobre *Questões Relacionadas a DNS e Apache*.

Inserir um asterisco (*) no campo **Endereço** é o mesmo que escolher **Escutar todos endereços**. Clicar no botão **Editar** no quadro **Endereços Disponíveis** exibe a mesma janela que o botão **Adicionar** exceto pelos campos preenchidos para a entrada selecionada. Para apagar uma entrada, selecione-a e clique no botão **Apagar**.

**Dica**

Se você definir que o servidor escute uma porta abaixo da 1024, você deve estar como root para iniciá-lo. Nas portas 1024 e acima, o `httpd` pode ser iniciado por um usuário comum.

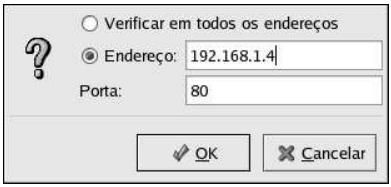


**Figura 26-2. Endereços Disponíveis**

## 26.2. Configurações Default

Após definir o **Nome do Servidor**, o **Endereço de e-mail do webmaster** e os **Endereços Disponíveis**, clique na aba **Máquinas Virtuais** e depois no botão **Editar Configurações Default**. A janela exibida na Figura 26-3 aparecerá. Defina as configurações default do seu servidor web nesta janela. Se você adicionar uma máquina virtual (virtual host), as configurações definidas para esta prevalecem sobre quaisquer configurações prévias. No caso de uma diretiva não definida dentre as configurações da máquina virtual, o valor default é usado.

### 26.2.1. Configuração do Site

Os valores default da **Lista de Busca das Páginas do Diretório** e **Páginas de Erro** funcionarão para a maioria dos servidores. Se você não estiver seguro sobre estes valores, não modifique-os.

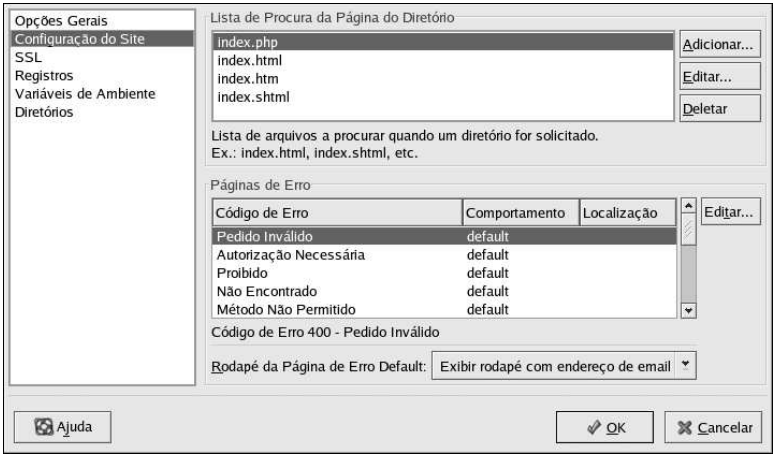


**Figura 26-3. Configuração do Site**

As entradas listadas na **Lista de Busca das Páginas do Diretório** definem a diretiva `DirectoryIndex`. A `DirectoryIndex` é a página default provida pelo servidor quando um usuário requisitar um índice de um diretório inserindo uma barra (/) no final do nome do diretório.

Por exemplo: quando um usuário requisita a página http://*www.exemplo.com/este_diretório/*, recebe a página `DirectoryIndex` se existir, ou uma lista do diretório gerada pelo servidor. O servidor tentará localizar um dos arquivos listados na diretiva `DirectoryIndex` e retornará a primeira que encontrar. Se não encontrar nenhum destes arquivos, e se `Options Indexes` está definido para este diretório, o servidor gerará e retornará uma lista, no formato HTML, dos sub-diretórios e arquivos deste diretório.

Use a seção **Código do Erro** para definir o Servidor HTTP Apache para redirecionar o cliente a uma URL local ou externa, no caso de um erro ou problema. Esta opção corresponde à diretiva `ErrorDocument`. Se houver um erro ou problema enquanto o cliente tentar conectar ao Servidor HTTP Apache, a ação default é exibir a mensagem curta de erro que aparece na coluna **Código do Erro**. Para sobrescrever esta configuração default, selecione o código do erro e clique no botão **Editar**. Selecione **Default** para exibir a mensagem curta default do erro. Selecione **URL** para redirecionar o cliente a uma URL externa e indique uma URL completa, includino http:// no campo **Localização**. Selecione **Arquivo** para redirecionar o cliente a uma URL interna e indique a localidade do arquivo sob o documento raiz do servidor web. A localidade deve começar com a barra (/) e ser relacionada ao Documento Raiz.

Por exemplo: para redirecionar um código do erro 404 Não Encontrada a uma página web que você criou em um arquivo chamado `404.html`, copie `404.html` para o *`DocumentRoot`*`/../error/404.html`. Neste caso, *`DocumentRoot`* é o diretório do Documento Raiz que você definiu (o default é `/var/www/html/`). Se o Documento Raiz é deixado na localidade default, o arquivo deve ser copiado em `/var/www/error/404.html`. Então, selecione **Arquivo** como o Comportamento (Behavior) do código do erro **404 - Não Encontrada** e indique `/error/404.html` como a **Localização**.

No menu **Rodapé da Página de Erro Default**, você pode escolher uma das seguintes opções:

- **Exibir rodapé com endereço de e-mail** — Exibe o rodapé default na base de todas as páginas de erro, junto com o endereço de e-mail do mantenedor do website especificado pela diretiva `Server-`

`Admin`. Consulte a Seção 26.3.1.1 para informações sobre a configuração da diretiva `ServerAdmin`.

- **Exibir rodapé** — Exibe somente o rodapé default na base das páginas de erro.
- **Sem rodapé** — Não exibe um rodapé na base das páginas de erro.

## 26.2.2. Registrando

Por default, o servidor grava o registro de transferência no arquivo `/var/log/httpd/access_log` e o registro de erro no arquivo `/var/log/httpd/error_log`.

O arquivo de transferência contém uma lista de todas as tentativas de acesso ao servidor web. Registra o endereço IP do cliente que tenta conectar, a data e hora da tentativa e o arquivo do servidor web que está tentando recuperar. Indique a localidade e o nome do arquivo para armazenar esta informação. Se a localidade e o arquivo não começam com uma barra (/), a localidade é relacionada ao diretório root do servidor conforme configurado. Esta opção corresponde à diretiva `TransferLog`.

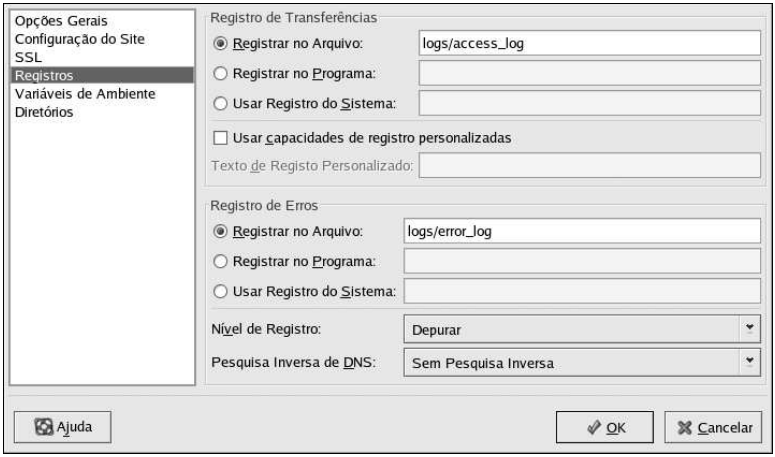


**Figura 26-4. Registrando**

Você pode configurar um formato de registro personalizado, selecionando **Usar funcionalidades de registro personalizado** e indicar uma linha de registro personalizado no respectivo campo. Isto configura a diretiva `LogFormat`. Visite http://httpd.apache.org/docs-2.0/mod/mod_log_config.html#formats para mais detalhes sobre o formato dessa diretiva.

O registro de erro contém uma lista de todos os erros que ocorrem no servidor. Indique a localidade e o arquivo que armazena esta informação. Se a localidade e o nome do arquivo não começam com uma barra (/), esta localidade é relacionada ao diretório root do servidor conforme configurado. Esta opção corresponde à diretiva `ErrorLog`

Use o menu **Nível de Registro** para determinar o quão verbais serão as mensagens de erro em seus registros. Elas podem ser definidas, da menos verbal para a mais verbal, como emerg (emergencial), alert (alerta), crit (crítica), error (erro), warn (atenção), notice (aviso), info (informação) ou debug (depuração). Esta opção corresponde a diretiva `LogLevel`.

O valor escolhido pelo menu **Pesquisa Inversa de DNS** define a diretiva `HostnameLookups`. Selecionar **Sem Pesquisa Inversa** define o valor para off (desligado). Selecionar **Pesquisa Inversa** define o valor para on (ligado). Selecionar **Pesquisa Inversa Dupla** define-o para double (o dobro).

Se você selecionar **Pesquisa Inversa**, seu servidor descobrirá o endereço IP automaticamente para cada conexão que requisitar um documento do servidor web. Descobrir endereços IP significa que seu servidor fará uma ou mais conexões ao DNS a fim de descobrir o nome da máquina que corresponde a um determinado endereço IP.

Se você selecionar **Pesquisa Inversa Dupla**, seu servidor executará um DNS inverso duplo. Em outras palavras, após o servidor executar uma pesquisa inversa, executa uma pesquisa encaminhada (forward lookup) no resultado. Pelo menos um endereço IP da pesquisa encaminhada deve coincidir com o endereço da primeira pesquisa inversa.

Geralmente, você deve deixar esta opção definida como **Sem Pesquisa Inversa**, porque os pedidos do DNS adicionam uma carga em seu servidor e podem torná-lo mais lento. Se seu servidor estiver ocupado, os efeitos de tentar executar estas pesquisas inversas ou pesquisas inversas duplas podem ser bastante notáveis.

Pesquisas inversas e pesquisas inversas duplas também são um problema para a Internet toda. Todas as conexões individuais feitas para pesquisar cada nome de máquina são somadas. Consequentemente, para o benefício de seu próprio servidor e também da Internet, você deve deixar esta opção como **Sem Pesquisa Inversa**.

### 26.2.3. Variáveis do Ambiente

Às vezes, é necessário alterar as variáveis do ambiente para scripts CGI ou páginas SSI (server-side include). O Servidor HTTP Apache pode usar o módulo `mod_env` para configurar as variáveis do ambiente que são passadas aos scripts CGI e páginas SSI. Use a página **Variáveis do Ambiente** para configurar as diretivas deste módulo.

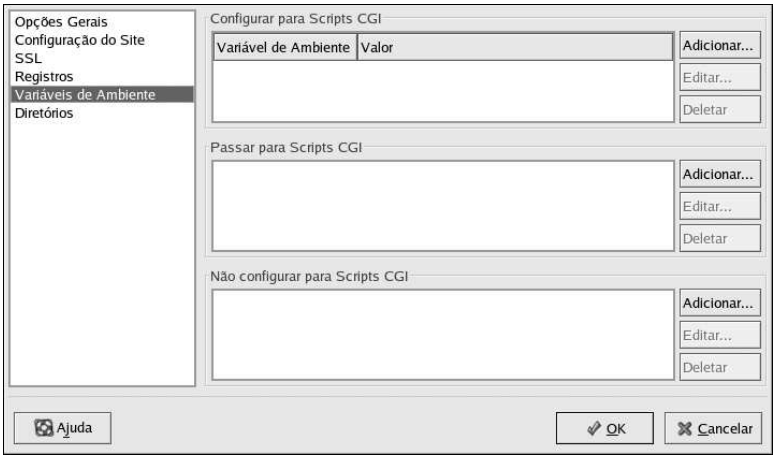


**Figura 26-5. Variáveis do Ambiente**

Use a seção **Definir como Scripts CGI** para definir uma variável de ambiente que é passada para scripts CGI e páginas SSI. Por exemplo: para definir a variável de ambiente `MAXNUM` como `50`, clique no botão **Adicionar** dentro da seção **Definir como Scripts CGI**, conforme mostra a Figura 26-5 e

digite **MAXNUM** no campo **Variável de Ambiente** e 50 no campo **Valor a definir**. Clique no botão **OK** para adicioná-la à lista. A seção **Definir como Scripts CGI** configura a diretiva SetEnv.

Use a seção **Passar para Scripts CGI** para passar os valores de uma variável do ambiente, quando o servidor é iniciado pela primeira vez, para scripts CGI. Para ver essa variável do ambiente, digite o comando env em uma janela de comandos. Clique no botão **Adicionar** dentro da seção **Passar para Scripts CGI** e indique o nome da variável do ambiente na caixa de diálogo que aparecer. Clique em **OK** para adicioná-la à lista. A seção **Passar para Scripts CGI** configura a diretiva PassEnv .

Se você deseja remover uma variável de ambiente para que o valor não seja passado para scripts CGI e páginas SSI, use a seção **Não passar para Scripts CGI**. Clique em **Adicionar** na seção **Não passar para Scripts CGI** e indique o nome da variável de ambiente a desconfigurar. Clique em **OK** para adicioná-la a lista. Isto corresponde à diretiva UnsetEnv.

Para editar qualquer um destes valores de ambiente, selecione-o da lista e clique no botão **Editar** correspondente. Para apagar uma entrada da lista, selecione-a e clique no botão **Apagar** correspondente.

Para saber mais sobre variáveis de ambiente no Servidor HTTP Apache, consulte o seguinte:

```
http://httpd.apache.org/docs-2.0/env.html
```

### 26.2.4. Diretórios

Use a página **Diretórios** para configurar as opções de diretórios específicos. Isto corresponde à diretiva <Directory>.

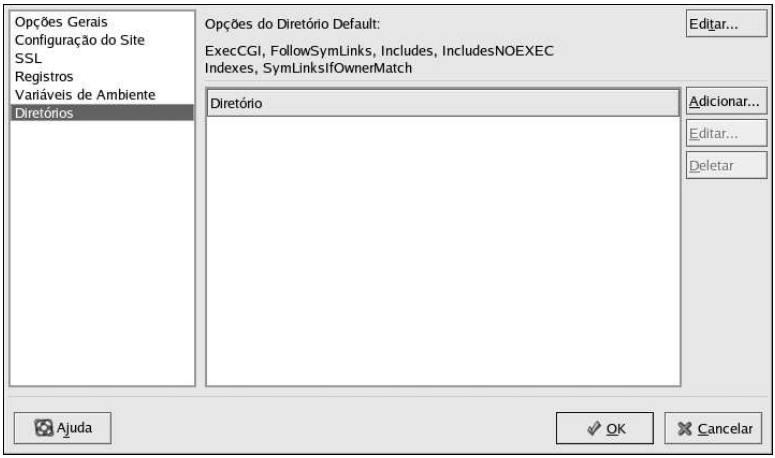


**Figura 26-6. Diretórios**

Clique no botão **Editar** no canto superior direito para configurar as **Opções Default de Diretório** para todos os diretórios que não estão especificados na lista **Diretório** logo abaixo. As opções que você escolhe são listadas como a diretiva Opções dentro da diretiva <Directory>. Você pode configurar as seguintes opções:

- **ExecutarCGI** — Permite a execução de scripts CGI. Os scripts CGI não são executados se esta opção não for selecionada.

- **SeguirLinksSimbólicos** — Permite que ligações simbólicas sejam seguidas.
- **Includes** — Permite server-side includes (SSI).
- **IncludesNÃOEXEC** — Permite server-side includes, mas desabilita os comandos `#exec` e `#include` nos scripts CGI.
- **Índices** — Exibe uma lista formatada do conteúdo do diretório, caso não exista um `DirectoryIndex` (como `index.html`) no diretório requisitado.
- **Multivisualização** — Suporta multi-visualizações negociadas com o conteúdo; essa opção é desabilitada por default.
- **SymLinksIfOwnerMatch** — Segue ligações simbólicas somente se o arquivo ou diretório alvo tem o mesmo properietário (owner) que a ligação (link).

Para especificar opções para determinados diretórios, clique no botão **Adicionar** ao lado do quadro da lista **Diretório**. Aparece a janela exibida na Figura 26-7. Indique o diretório a configurar no campo **Diretório** na parte inferior da janela. Selecione as opções na lista do lado direito e configure a diretiva `Order` com as opções do lado esquerdo. A diretiva `Order` controla a ordem na qual as diretivas de permissão e recusa são avaliadas. Nos campos **Permitir máquinas de** e **Recusar máquinas de**, você pode especificar um dos itens a seguir:

- Permitir todas as máquinas — Digite **`all`** para permitir acesso a todas as máquinas.
- Nome de domínio parcial — Permite todas as máquinas cujos nomes coincidem ou terminam com uma linha específica.
- Endereço IP completo — Permite o acesso a um endereço IP específico.
- Uma sub-rede — Como **`192.168.1.0/255.255.255.0`**
- Uma especificação de CDIR de rede — como **`10.3.0.0/16`**

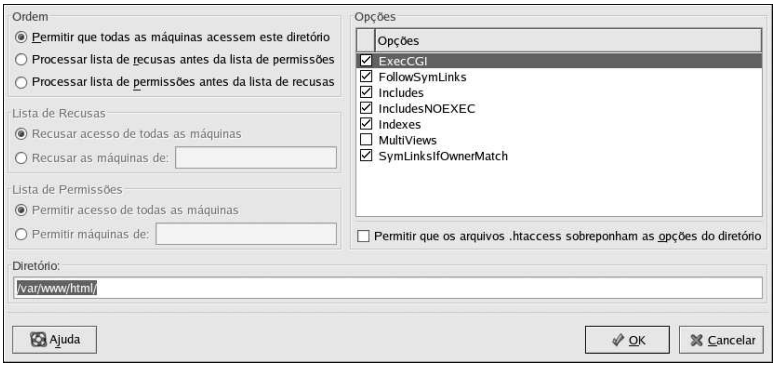


**Figura 26-7. Configurações de Diretório**

Se você selecionar **Deixar arquivos .htaccess sobrescreverem opções de diretório**, as diretivas de configuração no arquivo `.htaccess` prevalecem.

## 26.3. Configurações de Máquinas Virtuais

Você pode usar a **Ferramenta de Configuração do HTTP** para configurar máquinas virtuais. As máquinas virtuais permitem rodar servidores diferentes para endereços IP diferentes, nomes de máquinas diferentes ou para portas diferentes na mesma máquina. Por exemplo: você pode rodar o site http://www.exemplo.com e o http://www.outroexemplo.com no mesmo servidor web usando máquinas virtuais. Esta opção corresponde à diretiva <VirtualHost> da máquina virtual default e das máquinas virtuais baseadas no IP. Corresponde à diretiva <`NameVirtualHost`> da máquina virtual baseada no nome.

As diretivas definidas para uma máquina virtual se aplicam somente a esta determinada máquina virtual. Se a diretiva for definida para todo o servidor usando o botão **Editar Configurações Default** e não for definida nas configurações da máquna virtual, as configurações default são usadas. Por exemplo: você pode definir um **Endereço de e-mail do webmaster** na aba **Principal** e não definir endereços de e-mail individuais para cada máquina virtual.

A **Ferramenta de Configuração do HTTP** inclui uma máquina virtual default, conforme mostra a Figura 26-8.

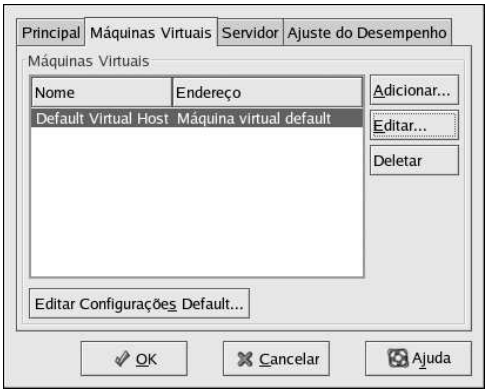


**Figura 26-8. Máquinas Virtuais**

A URL http://httpd.apache.org/docs-2.0/vhosts/ e a documentação do Servidor HTTP Apache em sua máquina oferecem mais informações sobre máquinas virtuais.

### 26.3.1. Adicionando e Editando uma Máquina Virtual

Para adicionar uma máquina virtual, clique na aba **Máquinas Virtuais** e então clique no botão **Adicionar**. Você também pode editar uma máquina virtual da lista, clicando no botão **Editar**.

#### 26.3.1.1. Opções Gerais

As configurações das **Opções Gerais** se aplicam somente à máquina virtual que você está configurando. Defina o nome da máquina virtual no campo **Nome da Máquina Virtual**. Este nome é usado pela **Ferramenta de Configuração do HTTP** para diferenciar de outras máquinas virtuais.

Defina o valor **Diretório do Documento Raiz** para o diretório que contém o documento raiz (como index.html) da máquina virtual. Esta opção corresponde à diretiva `DocumentRoot` directive within the <`VirtualHost`>. O `DocumentRoot` default é `/var/www/html`.

O **Endereço de e-mail do webmaster** corresponde à diretiva `ServerAdmin` dentro da diretiva `VirtualHost`. Este endereço de e-mail é usado no rodapé das páginas de erro se você assim escolher.

Na seção **Informações da máquina** section, selecione **Máquina Virtual Default**, **Máquina Virtual baseada no IP**, ou **Máquina Virtual Baseada no Nome**.

**Máquina Virtual Default**

Você deve configurar somente uma máquina virtual default (lembre-se que há uma configuração por default). As configurações da máquina virtual default são usadas quando o endereço IP requisitado não está explicitamente listado em outra máquina virtual. Se não há uma máquina virtual default definida, as configurações do servidor principal serão usadas.

**Máquina Virtual Baseada no IP**

Se você escolher a **Máquina Virtual Baseada no IP**, aparece uma janela para configurar a diretiva <VirtualHost> basaeda no endereço IP do servidor. Especifique este endereço IP no campo **Endereço IP**. Para especificar mais de um endereço IP, separate-os por espaços.Para especificar uma porta, use a sintaxe *`Endereço IP:Porta`*. Use :* para configurar todas as portas do endereço IP. Especifique o nome da máquina virtual no campo **Nome da Máquina do Servidor**

**Máquina Virtual Baseada no Nome**

Se você escolher a **Máquina Virtual Baseada no Nome**, aparece uma janela para configurar a diretiva `NameVirtualHost` baseada no nome da máquna do servidor. Especifique o IP no campo **Endereço IP**. Para especificar mais de um endereço IP, separe-os por espaços. Para especificar uma porta, use a sintaxe *`Endereço IP:Porta`*. Use :* para configurar todas as portas de um endereço IP. Especifique o nome da máquina virtual no campo **Nome da Máquina do Servidor**. Na seção **Apelidos**, clique em **Adicionar** para adicionar um apelido ao nome da máquina. Adicionar um apelido aqui corresponde à adição de uma diretiva `ServerAlias` directive within the `NameVirtualHost`.

#### 26.3.1.2. SSL

**Nota**

Não é possível usar máquinas virtuais baseadas no nome com o SSL, porque o o SSL handshake (quando o navegador aceita o certificado do servidor web seguro) ocorre antes do pedido HTTP, que identifica a máquina virtual apropriada baseada no nome. Se você quer usar máquinas virtuais baseadas no nome, elas funcionarão apenas com seu servidor web não-seguro.

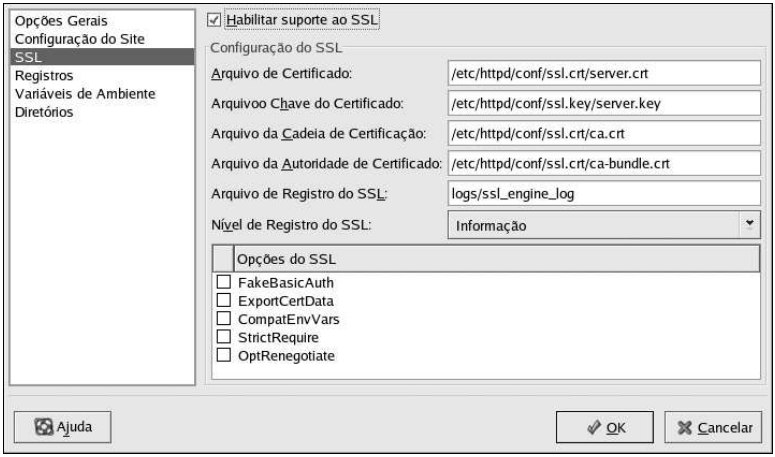


**Figura 26-9. Suporte ao SSL**

Se um Servidor HTTP Apache não está configurado com suporte SSL, as comunicações entre um Servidor HTTP Apache e seus clientes não são criptografadas. isto é indicado para sites sem informações pessoais ou confidenciais. Por exemplo: um site open source que distrbui software e documentação open source não precisa de comunicações seguras. No entanto, um site de comércio eletrônico que requer dados de cartão de crédito deve usar o suporte ao Apache SSL para criptografar suas comunicações. Habilitar o suporte ao Apache SSL habilita o uso do módulo de segurança `mod_ssl`. Para habilitá-lo através da **Ferramenta de Configuração do HTTP** você deve permitir o acesso pela porta 443 na aba **Principal => Endereços Disponíveis**. Consulte a Seção 26.1 para detalhes. Então, selecine o nome da máquina virtual na aba **Máquinas Virtuais**, clique no botão **Editar**, escolha **SSL** no menu esquerdo, e selecione a opção **Habilitar Suporte ao SSL** conforme mostra a Figura 26-9. A seção **Configuração do SSL** é pré-configurada com o certificado digital modelo. Este executa a autenticação para seu servidor web seguro e identifica o servidor seguro aos navegadores web (browsers) dos clientes. Você deve adquirir seu prórpio certificado digital. Não use o modelo provido para seu site. Para detalhes sobre a compra de um certificado digital aprovado pela CA (Certification Authority), conslute o Capítulo 27.

#### 26.3.1.3. Opções de Máquinas Virtuais Adicionais

As opções **Configuração do Site**, **Variáveis de Ambiente** e **Diretórios** das máquinas virtuais são as mesmas diretivas que você definiu ao clicar no botão **Editar Configurações Default**, exceto pelas opções definidas aqui para a configuração das máquinas virtuais individualmente. Consulte a Seção 26.2 para detalhes sobre estas opções.

## 26.4. Configurações do Servidor

A aba **Servidor** permite definir as configurações básicas do servidor. As configurações default destas opções são apropriadas para a maioria das situações.

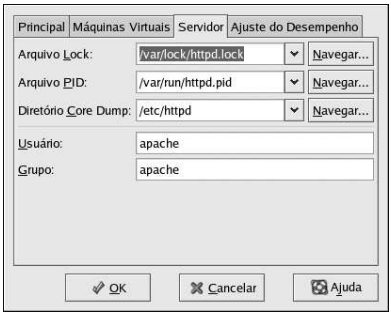


**Figura 26-10. Configuração do Servidor**

O valor do **Arquivo Lock** corresponde à diretiva `LockFile`. Essa diretiva define o caminho ao arquivo lock usado quando o servidor é compilado com USE_FCNTL_SERIALIZED_ACCEPT ou com USE_FLOCK_SERIALIZED_ACCEPT. Este deve ser armazenado no disco local e ser deixado com os valores default, a não ser que o diretório `logs` esteja localizado em uma partição NFS. Se for o caso, o valor default deve ser alterado para o disco local e para um diretório legível somente por root.

O valor **Arquivo PID** corresponde à diretiva `PidFile`. Esta diretiva define o arquivo no qual o servidor registra seus IDs de processos (pid). Este arquivo deve ser legível somente por root. Na maioria dos casos, deve ser deixado com o valor default.

O valor do **Diretório Core Dump** corresponde à diretiva `CoreDumpDirectory`. O Servidor HTTP Apache tenta comutar para este diretório antes do dumping core (erro). O valor default é o `ServerRoot`. Entretanto, se o usuário que está rodando o servidor não pode salvar (write) neste diretório, o core dump não pode ser salvo. Mude este valor para um diretório com permissão 'writable' pelo usuário que roda o servidor, como se você quisesse salvar os detalhes do erro (core dumps) em um disco para fins de depuração.

O valor **Usuário** corresponde à diretiva `User`, Define o id do usuário pelo servidor para responder a pedidos. Estas configurações do usuário determinam o acesso ao servidor. Quaisquer arquivos inacessíveis a este usuário também o serão para os visitantes do seu site na Internet. O default de `User` é apache.

O usuário deve ter privilégios somente para acessar arquivos que são supostamente visíveis para o mundo externo. O usuário também é dono (owner) de quaisquer processos CGI gerados pelo servidor. O usuário não deve poder executar nenhum código que não seja em resposta aos pedidos HTTP.

**Aviso**

A não ser que você saiba exatamente o que está fazendo, não defina a diretiva `User` como root. Se o fizer, pode criar grandes brechas de segurança em seu servidor web.

O processo `httpd` pai primeiro roda como root durante as operações normais, mas então é passado imediatamente para o usuário apache. O servidor deve iniciar como root porque precisa se ligar a uma porta abaixo da 1024. As portas abaixo de 1024 são reservadas para uso do sistema, portanto não podem ser usadas por ninguém a não ser root. Após o servidor se conectar à sua porta, passa o processo para o usuário apache antes de aceitar quaisquer pedidos de conexão.

O valor **Group** corresponde à diretiva `Group`. A diretiva **Group** é similar à diretiva `User`. A **Group** define o grupo sob o qual o servidor responderá pedidos. O grupo default também é apache.

## 26.5. Ajuste de Desempenho

Clique na aba **Ajuste de Desempenho** para configurar o número máximo de processos filho do servidor que você quer e para configurar as opções Servidor HTTP Apache para conexões cliente. As configurações default destas opções são apropriadas para a maioria das situações. Alterá-las pode afetar o desempenho geral do seu servidor web.

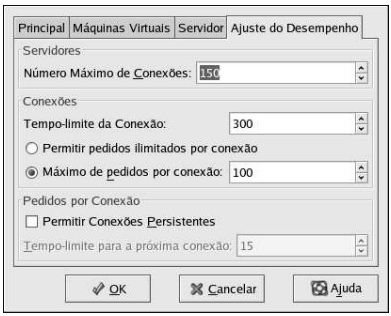


**Figura 26-11. Ajuste de Desempenho**

Defina o **Número Máximo de Conexões** como o número máximo de pedidos siumultâneos de clientes que o servidor suportará. Para cada conexão, é criado um processo `httpd` filho. Após atingir este número máximo de processos, ninguém mais conseguirá se conectar ao servidor web até que um processo filho seja liberado. Não é possível definir este valor maior que 256 sem recompilar. Esta opção corresponde à diretiva `MaxClients`.

O **Tempo Limite da Conexão** define, o tempo em segundos que seu servidor esperará por recibos e transmissões durante as comunicações. Especificamente, o **Tempo Limite da Conexão** define por quanto tempo seu servidor esperará para receber um pedido GET, o quanto esperará para receber pacotes TCP em um pedido POST ou PUT e o quanto esperará entre as respostas ACKs aos pacotes TCP. Por default, o **Tempo Limite da Conexão** está definido para 300 segundos, o que é apropriado para a maioria das situações. Esta opção corresponde à diretiva `TimeOut`.

Defina o **Máximo de pedidos por conexão** para o número máximo de pedidos permitidos por conexão persistente. O valor default é 100, o que deve ser apropriado para a maioria das situações. Esta opção corresponde à diretiva `MaxRequestsPerChild`.

Se você selecionar a opção **Permitir pedidos ilimitados por conexão**, e configurar a diretiva `MaxKeepAliveRequests` para 0, os pedidos ilimitados serão permitidos.

Se você desselecionar a opção **Permitir Conexões Persistentes**, a diretiva `KeepAlive` é definida como falsa. Se você selecioná-la, a diretiva `KeepAlive` é definida como verdadeira, e a diretiva `KeepAliveTimeout` é definida para o número selecionado como valor do **Tempo Limite da próxima Conexão**. Essa diretiva define o núneor de segundos que seu servidor esperará pelo pedido subsequente, após um pedido ter sido atendido e antes de encerrar a conexão. Uma vez que um pedido foi recebido, os valores de **Tempo Limite da Conexão** são aplicados.

Definir as **Conexões Persistentes** para um valor alto pode causar uma lentidão no servidor, dependendo de quantos usuários estão tentando a conexão. Quanto maior o número, maior a quantidade de processos do servidor esperando por uma outra conexão do último cliente que conectou-se àquele servidor.

## 26.6. Salvando Suas Configurações

Se você não quer salvar as configurações do seu Servidor HTTP Apache, clique no botão **Cancelar** no canto inferior direito da janela da **Ferramenta de Configuração do HTTP**. Você será questionado a confirmar esta decisão. Se você clicar **Sim** para confirmar sua escolha, suas configurações não serão salvas.

Se você quer salvar as configurações do seu Servidor HTTP Apache, clique no botão **OK** no canto inferior direito da janela da **Ferramenta de Configuração do HTTP**. Aparecerá uma janela de diálogo. Se você responder **Sim**, suas configurações serão salvas no `/etc/httpd/conf/httpd.conf`. Lembre-se que o arquivo com suas configurações originais será sobrescrito.

Se esta é a primeira vez que você usa a **Ferramenta de Configuração do HTTP**, verá uma janela avisando que o arquivo de configuração foi modificado manualmente. Se a **Ferramenta de Configuração do HTTP** detectar que o arquivo de configuração `httpd.conf` foi modificado manualmente, salvará este arquivo como `/etc/httpd/conf/httpd.conf.bak`.

**Importante**

Após salvar suas configurações, você deve reiniciar o daemon `httpd` com o comando `service httpd restart`. Você deve estar logado como root para executar este comando.

## 26.7. Recursos Adicionais

Para aprender mais sobre o Servidor HTTP Apache, consulte os seguintes recursos.

### 26.7.1. Documentação Instalada

- `/usr/share/docs/httpd-<version>/migration.html` — O documento *Como Migrar o Apache* contém uma lista de alterações da versão 1.3 para a versão 2.0, assim como informações sobre como migrar o arquivo de configuração manualmente.

### 26.7.2. Sites Úteis

- http://www.apache.org/ — *The Apache Software Foundation*.
- http://httpd.apache.org/docs-2.0/ — A documentação da The Apache Software Foundation sobre o Servidor HTTP Apache versão 2.0, incluindo o *Manual do Usuário do Servidor HTTP Apache Versão 2.0*.
- http://www.redhat.com/support/resources/web_ftp/apache.html — O Suporte da Red Hat matém uma lista de links úteis sobre o Servidor HTTP Apache.
- http://www.redhat.com/support/docs/faqs/RH-apache-FAQ/book1.html — 'The Apache Centralized Knowledgebase' compilado pela Red Hat.

### 26.7.3. Livros Relacionados

- *Apache: The Definitive Guide* de Ben Laurie e Peter Laurie; O'Reilly & Associates, Inc.

- *Guia de Referência do Red Hat Enterprise Linux*; Red Hat, Inc. — Este manual extra inclui instruções para migrar da versão 1.3 do Servidor HTTP Apache para a versão 2.0 manualmente, mais detalhes sobre as diretivas do Servidor HTTP Apache e instruções para adicionar módulos ao Servidor HTTP Apache.

redhat.

Capítulo 27.

# Configuração do Servidor Seguro HTTP Apache

## 27.1. Introdução

Este capítulo oferece informações básicas sobre o Servidor HTTP Apache com o módulo de segurança `mod_ssl` habilitado para usar a biblioteca e as ferramentas do OpenSSL. A combinação destes três componentes é referida neste capítulo como o servidor Web seguro ou somente como servidor seguro.

O `mod_ssl` é um módulo de segurança para o Servidor HTTP Apache. O módulo `mod_ssl` usa as ferramentas providas pelo Projeto OpenSSL para adicionar uma funcionalidade muito importante ao Servidor HTTP Apache — a habilidade de criptografar comunicações. Em contraste, com o uso regular do HTTP, as comunicações entre um navegador (browser) e um servidor Web são enviadas em texto simples, que pode ser interceptado e lido por alguém no meio do caminho entre o navegador e o servidor.

Este capítulo não pretende oferecer documentação completa e exclusiva para nenhum destes programas. Sempre que possível, este guia aponta as fontes apropriadas onde você pode encontrar uma documentação mais detalhada sobre determinados assuntos.

Este capítulo mostra como instalar estes programas. Você também pode aprender os passos necessários para gerar uma chave particular e um pedido de certificado, como gerar seu próprio certificado auto-assinado, e como instalar um certificado para usar com seu servidor seguro.

O arquivo de configuração `mod_ssl` está localizado em `/etc/httpd/conf.d/ssl.conf`. Para carregar este arquivo, e portanto para que o `mod_ssl` funcione, você deve ter a declaração `Include conf.d/*.conf` in `/etc/httpd/conf/httpd.conf`. Esta declaração é inclusa por default no arquivo de configuração do Servidor HTTP Apache default.

## 27.2. Uma Visão Geral dos Pacotes Relacionados à Segurança

Para habilitar o servidor seguro, você deve ter, no mínimo, os seguintes pacotes instalados:

`httpd`

O pacote `httpd` contém o daemon `httpd` e utilitários relacionados, arquivos de configuração, ícones, módulos do Servidor HTTP Apache, páginas man e outros arquivos usados pelo Servidor HTTP Apache.

`mod_ssl`

O pacote `mod_ssl` inclui o módulo `mod_ssl`, que provém criptografia forte para o Servidor HTTP Apache através dos protocolos SSL (Secure Sockets Layer) e TLS (Transport Layer Security).

`openssl`

O pacote `openssl` contém o kit de ferramentas do OpenSSL. Este kit implementa os protocolos SSL e TLS e também inclui uma biblioteca de criptografia para propósitos genéricos.

Adicionalmente, outros pacotes de software oferecem determinadas funcionalidades de segurança (mas não são necessários para o funcionamento do servidor):

`httpd-devel`

O pacote `httpd-devel` contém os arquivos include, arquivos de cabeçalho e o utilitário APXS do Servidor HTTP Apache. Você precisa de todos eles, se pretende carregar qualquer módulo extra, além dos módulos oferecidos com estes produto. Veja o *Guia de Referência do Red Hat Enterprise Linux* para mais informações sobre o carregamento de módulos para seu servidor seguro usando a funcionalidade DSO do Apache.

Se você não pretende carregar outros módulos para o seu Servidor HTTP Apache, não precisa instalar este pacote.

Pacotes do OpenSSH

Os pacotes do OpenSSH oferecem o conjunto de ferramentas de conectividade de rede para autenticação e execução de comandos em uma máquina remota. As ferramentas OpenSSH criptografam todo o tráfego (inclusive senhas), para que você possa evitar o eavesdropping, sequestro de conexão e outros ataques nas comunicações entre sua máquina e a máquina remota.

O pacote `openssh` inclui arquivos centrais necessários apara ambos, programas cliente e servidor OpenSSH. O pacote `openssh` também contém o `scp`, um substituto seguro para o `rcp` (para copiar arquivos entre máquinas).

O pacote `openssh-askpass` suporta a exibição de uma janela de diálogo que pede uma senha durante o uso do Agente OpenSSH.

O pacote `openssh-askpass-gnome` pode ser usado em conjunto com o ambiente GNOME, para exibir uma janela gráfica de diálogo quando os programas do OpenSSH programs pedem uma senha. Se você está rodando o GNOME e utilitários do OpenSSH , deve instalar este pacote.

O pacote `openssh-server` contém o daemon da shell segura `sshd` e arquivos relacionados. O daemon da shell segura é o lado do servidor no conjunto OpenSSH e deve ser instalado na sua máquina para permitir que clientes SSH se conectem à sua máquina.

O pacote `openssh-clients` contém os programas cliente, necessários para efetuar conexões criptografadas a servidores SSH, incluindo os seguintes: `ssh`, um substituo seguro do `rsh`; `sftp`, um substituo seguro do `ftp` (para transferir arquivos entre máquinas); e `slogin`, um substituo seguro do `rlogin` (para autenticação remota) e `telnet` (para comunicar com outra máquina através do protocolo Telnet).

Para mais informções sobre o OpenSSH, veja o Capítulo 22, o *Guia de Referência do Red Hat Enterprise Linux*e o site do OpenSSH: http://www.openssh.com.

`openssl-devel`

O pacote `openssl-devel` contém as bibliotecas estáticas e o arquivo include necessários para compilar aplicações com suporte para vários algoritmos e protocolos criptográficos. Você precisa instalar este pacote somente se estiver desenvolvendo aplicações que incluem suporte ao SSL — este pacote não é necessário para usar o SSL.

`stunnel`

O pacote `stunnel` oferece o Stunnel SSL wrapper. O Stunnel suporta a criptografia SSL de conexões TCP, para que possa oferecer criptografaia de daemons e protocolos não-SSL (como POP, IMAP e LDAP) sem precisar de nenhuma alteração no código do daemon.

A Tabela 27-1 apresenta um sumário dos pacotes do servidor seguro e se cada pacote é opcional ou não para a instalação de um servidor seguro.

| Nome do Pacote | Opcional? |
|---|---|
| `httpd` | não |

| Nome do Pacote | Opcional? |
|---|---|
| mod_ssl | não |
| openssl | não |
| httpd-devel | sim |
| openssh | sim |
| openssh-askpass | sim |
| openssh-askpass-gnome | sim |
| openssh-clients | sim |
| openssh-server | sim |
| openssl-devel | sim |
| stunnel | sim |

**Tabela 27-1. Pacotes de Segurança**

## 27.3. Uma Visão Geral de Certificados e Segurança

Seu servidor seguro oferece segurança usando uma combinação do protocolo SSL (Secure Sockets Layer) e, na maioria dos casos, de um certificado digital de uma Autoridade de Certificação (Certificate Authority, CA). O SSL executa as comunicações criptografadas e a autenticação mútua entre os navegadores (browsers) e seu servidor seguro. O certificado digital aprovado pela CA provém a autenticação para seu servidor seguro (a CA coloca sua reputação por trás da certificação de identidade da sua empresa). Quando seu navegador de comunica usando a criptografia SSL, o prefixo `https://` é usado no começo da URL (Uniform Resource Locator) na barra de navegação.

A criptografia depende do uso de chaves (pense nelas como anéis secretos de codificação/decodificação no formato de dados). Na criptografia convencional ou simétrica, ambas extremidades da transação têm a mesma chave, que são usadas para decodificar as tranmissões da outra extremidade. Na criptografia pública ou assimétrica, duas chaves co-existem: uma pública e uma particular. Uma pessoa ou empresa mantém sua chave particular em segredo e divulga sua chave pública. Os dados criptografados com a chave pública só podem ser decodifcados com a chave particular; dados criptografados com a chave particular só podem ser decodificados com a chave pública.

Para configurar seu servidor seguro, use criptografia pública para criar um par de chaves composto de um pública e um particular. Na maioria dos casos, você envia seu pedido de certificado (incluindo sua chave pública), prova da identidade de sua empresa e um pagamento a uma CA. A CA verifica o pedido de certificado e sua identidade, e então envia de volta um certificado para seu servidor seguro.

Um servidor seguro usa um certificado para se auto-identificar a nevagadores Web. Você pode gerar seu próprio certificado (chamado de certificado "auto-assinado"), ou pode obtê-lo por uma CA. Um certificado de uma CA com boa reputação garante que um site esteja associado a uma determinada companhia ou empresa.

Alternativamente, você pode criar seu próprio certificado auto-assinado. Note, no entanto, que certificados auto-assinados não devem ser usados na maioria dos ambientes de produção. Estes certificados não são automaticamente aceitos pelo navegador (browser) de um usuário — o navegador questiona se o usuário quer aceitar o certificado e criar a conexão segura. Consulte a Seção 27.5 para mais informações sobre as diferenças entre certificados auto-assinados e assinados por uma CA.

Quando você tiver o certificado auto-assinado ou assinado por uma CA de sua escolha, deve instalá-lo no seu servidor seguro.

## 27.4. Usando Chaves e Certificados Pré-Existentes

Se você já tem uma chave ou certificado (ex.: se você pretende instalar o servidor seguro para substituir um outro servidor seguro da empresa), é possível que consiga usar sua chave e certificado existentes com o servidor seguro. Nas duas situações a seguir, não e possível usá-los:

- *Se você está trocando seu endereço IP ou nome de domínio* — Os certificados são atribuídos a um determinado par de endereço IP e nome de domínio. Você deve obter um novo certificado se for alterar seu endereço IP ou nome de domínio.
- *Se você tem um certificado da VeriSign e está trocando o software do seu servidor* — A VeriSign é uma CA utilizada no mundo todo. Se você já tem um certificado da VeriSign para outro propósito, aconselhamos considerar usar seu certificado VeriSign existente com seu novo servidor seguro. Entretanto, talvez não seja possível fazê-lo por que a VeriSign atribui certificados para uma combinação específica de endereço IP/nome de domínio e software de servidor.

  Se você alterar algum destes parâmetros (ex.: se anteriormente usou um produto diferente para seu servidor seguro), o certificado da VeriSign, obteido para ser usado com a configuração anterior, não funcionará com a configuração nova. Você precisa obter um certificado novo.

Se você tem uma chave e certificado existentes que possa usar, não precisa gerar uma nova chave e obter um novo certificado. No entanto, talvez precise mover e renomear os arquivos que contêm sua chave e certificado.

Mova o arquivo de sua chave existente para:

```
/etc/httpd/conf/ssl.key/server.key
```

Mova o arquivo de seu certificado existente para:

```
/etc/httpd/conf/ssl.crt/server.crt
```

Após mover sua chave e certificado, pule para a Seção 27.9.

Se você está atualizando um Servidor Web Seguro Red Hat, sua chave (`httpsd.key`) e certificado (`httpsd.crt`) antigos estão localizados em `/etc/httpd/conf/`. Mova-os e renomeie-os para que o servidor seguro possa usá-lo. Use os dois comandos a seguir para mover e renomear seus arquivos de chave e certificado:

```
mv /etc/httpd/conf/httpsd.key /etc/httpd/conf/ssl.key/server.key
mv /etc/httpd/conf/httpsd.crt /etc/httpd/conf/ssl.crt/server.crt
```

Então inicie seu servidor seguro com o comando:

```
/sbin/service httpd start
```

Para um servidor seguro, você deverá inserir sua senha. Após você inserí-la e pressionar [Enter], o servidor inicia.

## 27.5. Tipos de Certificados

Se você instalou seu servidor seguro pelo pacote RPM provido pela Red Hat, são gerados uma chave e certificado teste randômicos e inseridos nos diretórios apropriados. Antes de começar a usar seu servidor seguro, no entanto, você deve gerar sua própria chave e obter um certificado que identifica corretamente seu servidor.

Você precisa de uma chave e um certificado para operar seu servidor seguro — o que significa que você pode gerar um certificado auto-assinado ou adquirir um certificado assinado por uma CA. Quais são as diferenças antre eles?

Um certificado assinado por uma CA oferece duas capacidades importantes para seu servidor:

- Os navegadores (browsers) geralmente reconhecem automaticamente o certificado e permitem efetuar a conexão segura, sem questionar o usuário.
- Quando uma CA atribui um certificado assinado, está garantindo a identidade da empresa que fornece as páginas web ao navegador.

Se o seu servidor seguro é acessado por um grande público, precisa de um certificado assinado por uma CA, para que as pessoas que visitem seu site saibam que é realmente de propriedade da empresa. Antes de assinar um certificado, uma CA verifica se a empresa requisitando o certificado é realmente quem diz ser.

A maioria dos navegadores web que suportam a SSL tem uma lista de CAs cujos certificados são aceitos automaticamente. Se encontrar um certificado cuja CA autorizadora não se encontra na lista, o navegador pergunta ao usuário se deseja aceitar ou negar a conexão.

Você pode gerar um certificado auto-assinado para seu servidor seguro, mas esteja ciente de que este tipo de certificado não oferece a mesma funcionalidade que um certificado assinado por uma CA. Um certificado auto-assinado não é automaticamnete reconhecido pela maioria dos navegadores web e não oferece nenhuma garantia em relação à identidade da empresa que está provendo o site. Um certificado assinado por uma CA oferece estas duas importantes capacidades para um servidor seguro. Se o seu servidor seguro é usado num ambiente de produção, você provavelmente precisa de um certificado assinado por uma CA.

O processo de obtenção de um certificado por uma CA é bem tranquilo. Veja uma visão geral a seguir:

1. Crie um par de chaves pública e particular de criptografia.
2. Crie um pedido de certificado baseado na chave pública. Este pedido contém informações sobre seu servidor e da empresa que o hospeda.
3. Envie o pedido do certificado, juntamente com documentos comprovando seu identidade, para uma CA. Não podemos lhe dizer qual certificado escolher. Sua decisão deve ser baseada em suas experiências no passado, ou nas experiências de seus amigos e colegas, ou puramente em fatores financeiros.

   Após você tomar uma decisão sobre a CA, deve seguir as instruções oferecidas sobre como obter um certificado para ela.
4. Quando a CA estiver convicta de que você realmente é quem clama ser, envia um certificado digital a você.
5. Instale este certificado no seu servidor seguro e comece a efetuar transações seguras.

Com ambos certificados, de uma CA ou auto-assinado, o primeiro passo é gerar a chave. Consulte a Seção 27.6 para instruções sobre a geração da chave.

## 27.6. Gerando uma Chave

Você deve estar como root para gerar uma chave.

Primeiro, `cd` para o diretório `/etc/httpd/conf/`. Remova a chave e certificado falsos, que foram gerados durante a instalação, com os seguintes comandos:

```
rm ssl.key/server.key
rm ssl.crt/server.crt
```

Em seguida, é necessário criar sua própria chave randômica. Mude para o diretório `/usr/share/ssl/certs/` e digite o seguinte comando:

```
make genkey
```

Seu sistema exibe uma mensagem similar à seguinte:

```
umask 77 ; \
/usr/bin/openssl genrsa -des3 1024 > /etc/httpd/conf/ssl.key/server.key
Generating RSA private key, 1024 bit long modulus
.......++++++
.....................................................................++++++
e is 65537 (0x10001)
Enter pass phrase:
```

Agora, você precisa digitar uma senha. Para maoir segurança, esta deve conter no mínimo oito caracteres, incluir números e/ou pontuação, e não ser uma palavra de dicionário. Também lembre-se que sua senha é sensível a letras maiúsculas e minúsculas.

**Nota**

Você deve lembrar e inserir esta senha toda vez que iniciar seu servidor seguro, portanto não esqueça dela.

Re-digite a senha para verificar que está correta. Após digitá-la corretamente, o arquivo `/etc/httpd/conf/ssl.key/server.key`, contendo sua chave, é criado.

Note que se você não deseja inserir uma senha toda vez que iniciar seu servidor seguro, precisa usar os dois comandos a seguir ao invés do `make genkey` para criar a chave.

Use o seguinte comando para criar sua chave:

```
/usr/bin/openssl genrsa 1024 > /etc/httpd/conf/ssl.key/server.key
```

Então use o seguinte comando para garantir que as permissões do arquivo estejam definidas corretamente:

```
chmod go-rwx /etc/httpd/conf/ssl.key/server.key
```

Após usar os comandos acima para criar sua chave, você não precisa mais usar uma senha para iniciar seu servidor seguro.

**Atenção**

Desabilitar a funcionalidade da senha do seu servidor seguro é um risco de segurança. NÃO é recomendado desabilitar a funcionalidade da senha para seu servidor seguro.

Os problemas associados com a falta do uso da senha são diretamente relacionados à segurança mantida na máquina hospedeira. Por exemplo: se um indivíduo inescrupuloso comprometer a segurança UNIX regular da máquina hospedeira, esta pessoa pode obter sua chave particular (o conteúdo de seu arquivo `server.key`). A chave pode ser usada para oferecer páginas web que parecem ser do seu servidor seguro.

Se as práticas de segurança do UNIX forem rigorosamente mantidas no computador hospedeiro (todos os consertos e atualizações do sistema operacional baixados assim que são lançados, sem operar serviços arriscados ou desnecessários e assim por diante), a senha do servidor seguro pode parecer

desnecessária. No entanto, como seu servidor seguro não deve ser reiniciado com frequência, a segurança extra provida pela senha pode valer a pena na maioria dos casos.

O arquivo `server.key` deve ser de propriedade do usuário root do seu sistema e não deve ser acessível para nenhum outro usuário. Faça um cópia backup deste arquivo e guarde-a num lugar seguro e protegido. Você precisa da cópia backup porque se algum dia perder o arquivo `server.key` após usá-lo para criar seu pedido de certificado, seu certificado não funcionará mais e a CA não terá como te ajudar. Sua única opção é pedir (e pagar por) um novo certificado.

Se pretende adquirir um certificado de uma CA, continue na Seção 27.7. Se pretende gerar seu próprio certificado auto-assinado, continue na Seção 27.8.

## 27.7. Gerando um Pedido de Certificado para Enviar a uma CA

Após criar a chave, o próximo passo é gerar um pedido de certificado, que precisa ser enviado à sua CA escolhida. Certifique-se de estar no diretório `/usr/share/ssl/certs` e digite o seguinte comando:

```
make certreq
```

Seu sistema exibe o seguinte output e pede sua senha (a não ser que você tenha desabilitado sua opção de senha):

```
umask 77 ; \
/usr/bin/openssl req -new -key /etc/httpd/conf/ssl.key/server.key
-out /etc/httpd/conf/ssl.csr/server.csr
Using configuration from /usr/share/ssl/openssl.cnf
Enter pass phrase:
```

Digite a senha que escolheu quando gerou sua chave. Seu sistema apresenta algumas instruções e pede que você responda uma série de perguntas. Seus inputs são incorporados ao pedido do certificado. O display, com exemplos de respostas, parece com o seguinte:

```
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a
DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [GB]:US
State or Province Name (full name) [Berkshire]:North Carolina
Locality Name (eg, city) [Newbury]:Raleigh
Organization Name (eg, company) [My Company Ltd]:Test Company
Organizational Unit Name (eg, section) []:Testing
Common Name (your name or server's hostname) []:test.example.com
Email Address []:admin@example.com
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

As respootas default aparecem entre colchetes `[]` imediatamente após cada pedido do input. Por exemplo: a primeira informação requisitada é o nome do país onde o certificado será usado, exibido como o seguinte:

```
Country Name (2 letter code) [GB]:
```

O input default, entre colchetes, é `GB`. Para aceitar o default, pressione [Enter] ou preencha o código de duas letras do país.

Você deve digitar os valores restantes. Todos eles devem ser auto-explicativos, mas você deve seguir estas regras:

- Não abrevie a localidade ou estado. Escreva-os (ex.: St. Louis deve ser escrito Saint Louis).
- Se você está enviando este CSR para uma CA, cuidado para prover as informações corretas em todos os campos, e especialmente no `Nome da Empresa` e no `Nome Comum`. As CAs verificam as informações providas no CSR para determinar se sua empresa é responsável pelo que você proveu no campo `Nome Comum`. As CAs rejeitam CSRs que incluem informações que consideram inválidas.
- No `Nome Comum`, certifique-se de digitar o nome *real* do seu servidor seguro (um nome DNS válido) e não apelidos que o servidor tenha.
- O `Endereço de E-mail` deve ser o endereço de e-mail do webmaster ou do administrador de sistemas.
- Evite caracteres especiais como @, #, &, !, etc. Algumas CAs rejeitam um pedido de certificado que contém um caractere especial. Portanto, se o nome de sua empresa inclui um e comercial (&), soletre-o como "e" ao invés de "&."
- Não use nenhum dos atributos extras (`Uma senha desafiadora` e `Um nome opcional para a empresa`). Para continuar sem preencher estes campos, pressione [Enter] para aceitar as opções default em branco para ambos inputs.

O arquivo `/etc/httpd/conf/ssl.csr/server.csr` é criado quando você terminar de inserir as informações. Este arquivo é o seu pedido de certificado, pronto para ser enviado à sua CA.

Após ter escolhido uma CA, siga as instruções que esta provém em seu site. Suas instruções explicam como enviar seu pedido de certificado, quaisquer outros documentos que precisarem e seu pagamento.

Após você atender aos requisistos da CA, esta envia um certificado a você (geralmente por e-mail). Salve (ou recorte e cole) o certificado enviado a você como `/etc/httpd/conf/ssl.crt/server.crt`. Tenha certeza de manter uma cópia backup deste arquivo.

## 27.8. Criando um Certificado Auto-Assinado

Você pode criar seu próprio certificado auto-assinado. Note que este tipo de certificado não oferece as garantias de segurança de um certificado assinado por uma CA. Veja a Seção 27.5 para mais detalhes sobre certificados.

Para criar seu próprio certificado auto-assinado, primeiro crie uma chave randômica usando as intruções da Seção 27.6. Quando você tiver uma chave, tenha certeza de estar no diretório `/usr/share/ssl/certs` e digite o seguinte comando:

```
make testcert
```

É exibido o seguinte output, e você deverá inserir sua senha (a não ser que tenha geraqdo uma chave sem senha):

```
umask 77 ; \
/usr/bin/openssl req -new -key /etc/httpd/conf/ssl.key/server.key
-x509 -days 365 -out /etc/httpd/conf/ssl.crt/server.crt
Using configuration from /usr/share/ssl/openssl.cnf
```

```
Enter pass phrase:
```

Após inserir sua senha (ou sem o pedido da senha, caso tenha criado uma chave sem senha), você deverá indicar mais informações. O output do computador e um conjunto de inputs se parecem com o seguinte (indique as informações corretas sobre sua empresa e máquina hospedeira):

```
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a
DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [GB]:US
State or Province Name (full name) [Berkshire]:North Carolina
Locality Name (eg, city) [Newbury]:Raleigh
Organization Name (eg, company) [My Company Ltd]:My Company, Inc.
Organizational Unit Name (eg, section) []:Documentation
Common Name (your name or server's hostname) []:myhost.example.com
Email Address []:myemail@example.com
```

Após indicar as informações corretas, um certificado auto-assinado é criado em `/etc/httpd/conf/ssl.crt/server.crt`. Reinicialize seu servidor seguro após gerar o certificado com o seguinte comando:

```
/sbin/service httpd restart
```

## 27.9. Testando o Certificado

Para testar o certificado teste instalado por default, um certificado de uma CA ou um certificado auto-assinado, aponte seu navegador web para a seguinte página (substituindo *`server.example.com`* pelo seu nome de domínio):

```
https://server.example.com
```

**Nota**

Note o `s` após `http`. O prefixo `https:` é usado para transações HTTP seguras.

Se você está usando um certificado assinado por uma CA conhecida, seu navegador provavelmente aceita o certificado (sem pedir nenhuma interação sua) e cria a conexão segura. Seu navegador não reconhece automaticamente um certificado auto-assinado porque não é assinado por uma CA. Se não usar um certificado de uma CA, sigas as instruções providas pelo seu navegador para aceitar o certificado.

Após seu navegador aceitar o certificado, seu servidor seguro apresenta uma home page default.

## 27.10. Acessando o Servidor

Para acessar seu servidor seguro, use uma URL similar à seguinte:

`https://server.example.com`

Seu servidor não-seguro pode ser acessado usando uma URL similar à seguinte:

`http://server.example.com`

A porta padrão para comunicações web seguras é a porta 443. A porta padrão para comunicações web não-seguras é a porta 80. A configuração default do servidor seguro escuta estas duas portas padrão. Consequentemente, não é necessário especificar o número da porta numa URL (o sistema assume o número da porta).

No entanto, se você configurar seu servidor para escutar uma porta fora do padrão (ex.: qualquer outra porta além de 80 e 443), deve especificar o número da porta em todas as URLs às quais pretende conectar o servidor em portas fora do padrão.

Por exemplo: você pode configurar seu servidor para ter uma máquina virtual rodando inseguramente na porta 12331. Para todas as URLs que você pretende conectar a esta máquina virtual, deve especificar o número da porta na URL. O exemplo de URL a seguir tenta conectar a um servidor não-seguro escutando na porta 12331:

`http://server.example.com:12331`

## 27.11. Recursos Adicionais

Consulte a Seção 26.7 para mais referências sobre o Servidor HTTP Apache.

### 27.11.1. Sites Úteis

- http://www.redhat.com/mailman/listinfo/redhat-secure-server — A lista de discussão do `redhat-secure-server`.

  Você também pode assinar a lista de discussão `redhat-secure-server`, enviando um e-mail para <`redhat-secure-server-request@redhat.com`> e incluindo a palavra *subscribe* no campo do assunto.
- http://www.modssl.org/ — O site do `mod_ssl` é a fonte de informações essencial sobre o `mod_ssl`. O site traz uma rica documentação, incluindo um *User Manual* (Manual do Usuário) na URL: http://www.modssl.org/docs/.

### 27.11.2. Livros Relacionados

- *Apache: The Definitive Guide* (Guia Essencial do Apache), 2a edição, por Ben Laurie and Peter Laurie, O'Reilly & Associates, Inc.

# Capítulo 28.

# Configuração BIND

Este capítulo assume que o leitor tem um conhecimento básico do BIND e do DNS, pois seus conceitos não são explicados aqui. Este capítulo não explica como usar a **Ferramenta de Configuração do Serviço de Nome de Domínio** (`redhat-config-bind`) para configurar zonas BIND básicas do servidor. A **Ferramenta de Configuração do Serviço de Nome de Domínio** cria o arquivo de configuração `/etc/named.conf` e os arquivos de configuração da zona no diretório `/var/named/` cada vez que as alterações são aplicadas.

**Importante**

Não edite o arquivo de configuração `/etc/named.conf`. A **Ferramenta de Configuração do Serviço de Nome de Domínio** gera este arquivo após as alterações serem aplicadas. Para definir as configurações não configuráveis pela **Ferramenta de Configuração do Serviço de Nome de Domínio**, adicione-as ao arquivo `/etc/named.custom`.

A **Ferramenta de Configuração do Serviço de Nome de Domínio** requer o Sistema X Window e acesso root. Para iniciar a **Ferramenta de Configuração do Serviço de Nome de Domínio**, vá para **Botão do Menu Principal** (no Painel) **=> Configurações do Sistema => Configurações do Servidor => Serviço de Nome de Domínio** ou digite o comando `redhat-config-bind`.

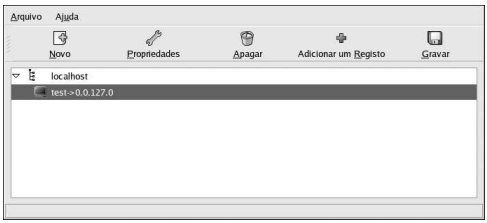


**Figura 28-1. Ferramenta de Configuração do Serviço de Nome de Domínio**

A **Ferramenta de Configuração do Serviço de Nome de Domínio** configura o diretório de zona default como `/var/named/`. Todos os arquivos de zona especificados são relacionados a este diretório. A **Ferramenta de Configuração do Serviço de Nome de Domínio** também inclui uma verificação de sintaxe básica quando os valores são indicados. Por exemplo: se for um valor IP, são permitidos somente números e pontos (.) dentro deste campo.

A **Ferramenta de Configuração do Serviço de Nome de Domínio** permite a adição de uma zona mestre de encaminhamento, uma zona mestre inversa e de uma zona escrava. Após adicionar as zonas, elas podem ser editadas ou apagadas pela janela principal, conforme exibido na Figura 28-1.

Após adicionar, editar ou apagar uma zona, clique no botão **Salvar** ou selecione **Arquivo => Salvar** para salvar o arquivo de configuração `/etc/named.conf` e todos os arquivos de zonas individuais no diretório `/var/named/`. Salvar as alterações também faz com que o serviço `named` recarregue os arquivos de configuração. Selecionar **Arquivo => Sair** salva as alterações antes de fechar a aplicação.

## 28.1. Adicionando uma Zona Mestre de Encaminhamento

Para adicionar uma zona mestre de encaminhamento (também conhecida como mestre principal), clique no botão **Nova**, selecione **Zona Mestre de Encaminhamento** e insira o nome do domínio da zona mestre no campo **Nome de Domínio**.

Aparece uma nova janela, conforme a Figura 28-2, com as seguintes opções:

- **Nome** — Nome do domínio que foi inserido há pouco na janela anterior.
- **Nome do Arquivo** — Nome do arquivo do banco de dados DNS, relacionado ao `/var/named`. Este é pré-definido com `.zone` anexo ao nome de domínio.
- **Contato** — Endereço de e-mail do contato principal da zona mestre.
- **Servidor de Nome Primário (SOA)** — Registro do estado de autoridade (state of authority - SOA). Isto especifica o nome do servidor que é o melhor recurso de informações para este domínio.
- **Número Serial** — O número serial do arquivo do banco de dados DNS. Este número deve ser aumentado cada vez que o arquivo é alterado, assim como os servidores de nome escravos para a zona recuperar os últimos dados. A **Ferramenta de Configuração do Serviço de Nome de Domínio** aumenta este número cada vez que a configuração muda. Também pode ser aumentado manualmente clicando no botão **Definir** próximo ao valor **Número Serial**.
- **Configurações de Hora** — Os valores TTL (Time to Live) **Atualizar**, **Retentar**, **Expirar** e **Mínimo** que estão armazenados no arquivo de banco de dados DNS. Todos os valores estão em segundos.
- **Registros** — Adicione, edite e apague recursos de registro do tipo **Máquina**, **Apelido**, e **Nome do Servidor**.

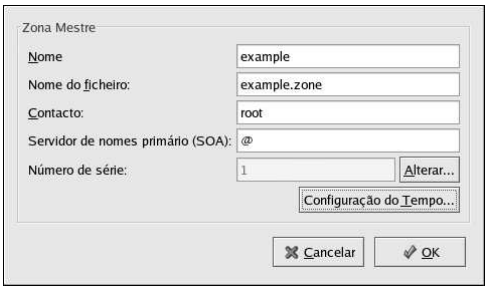


**Figura 28-2. Adicionando uma Zona Mestre de Encaminhamento**

Um **Servidor de Nome Principal (SOA)** deve ser especificado, e pelo menos um registro de nome de servidor clicando no botão **Adicionar** na seção **Registros**.

Após configurar a Zona Mestre de Encaminhamento, clique em **OK** para retornar à janela principal, conforme a Figura 28-1. No menu suspenso, clique **Salvar** para gravar o arquivo de configuração `/etc/named.conf` e todos os arquivos de zonas individuais no diretório `/var/named`, e também para que o daemon recarregue os arquivos de configuração.

A configuração cria uma entrada similar à seguinte no `/etc/named.conf`:

```
zone  "forward.example.com" {
 type master;
 file  "forward.example.com.zone";
};
```

Também cria o arquivo `/var/named/forward.example.com.zone` com as seguintes informações:

```
$TTL 86400
@       IN      SOA     ns.example.com.  root.localhost (
                        2 ; serial
                        28800 ; refresh
                        7200 ; retry
                        604800 ; expire
                        86400 ; ttl
                        )


        IN      NS      192.168.1.1.
```

## 28.2. Adicionando uma Zona Mestre Inversa

Para adicionar uma zona mestre inversa, clique no botão **Nova** e selecione **Zona Mestre Inversa**. Indique os três primeiros octetos do intervalo do endereço IP a ser configurado. Por exemplo, para configurar o endereço IP de intervalo 192.168.10.0/255.255.255.0, indique 192.168.10 no campo **Endereço IP (primeiros 3 Octetos)**.

Aparece uma nova janela, conforme a Figura 28-3, com as seguintes opções:

1. **Endereço IP** — Os três primeiros octetos indicados na janela anterior.
2. **Endereço IP Inverso** — Não-editável. Pré-definido baseado no Endereço IP indicado.
3. **Contato** —Endereço de e-mail do contato principal da zona mestre.
4. **Nome do Arquivo** — Nome do arquivo do banco de dados DNS no diretório `/var/named`.
5. **Servidor de Nome Primário (SOA)** — Registro do estado de autoridade (state of authority - SOA). Isto especifica o nome do servidor que é o melhor recurso de informações para este domínio.
6. **Número Serial** — O número serial do arquivo do banco de dados DNS. Este número deve ser aumentado cada vez que o arquivo é alterado, assim como os servidores de nome escravos para a zona recuperar os últimos dados. A **Ferramenta de Configuração do Serviço de Nome de Domínio** aumenta este número cada vez que a configuração muda. Também pode ser aumentado manualmente clicando no botão **Definir** próximo ao valor **Número Serial**.
7. **Configurações de Hora** — os valores TTL (Time to Live) **Atualizar**, **Retentar**, **Expirar** e **Mínimo** que são armazenados no arquivo de banco de dados DNS.
8. **Servidores de Nome** — Adicione, edite e apague servidores de nome da zona mestre inversa. É necessário pelo menos um servidor de nomes.
9. **Tabela de Endereços Inversos** — Lista de endereços IP dentro da zona mestre inversa e seus nomes de máquinas. Por exemplo: para a zona mestre inversa 192.168.10, pode-se adicionar 192.168.10.1 na **Tabela de Endereços Inversos** com o nome de máquina one.exemplo.com. O nome da máquina deve terminar com um ponto (.) para especificar que é um nome completo de máquina.

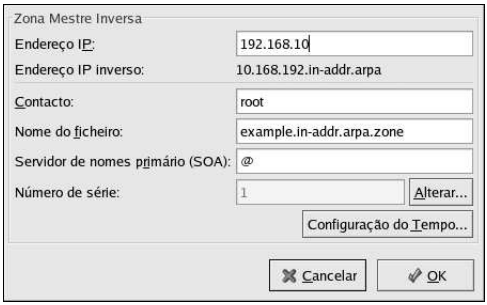


**Figura 28-3. Adicionando uma Zona Mestre Inversa**

O **Servidor de Nome Principal (SOA)** deve ser especificado, e pelo menos um registro de servidor de nome (nameserver) deve ser especificado clicando no botão **Adicionar** na seção **Servidores de Nome**.

Após configurar a Zona Mestre Inversa, clique em **OK** para retornar à janela principal exibida na Figura 28-1. No menu suspenso, clique em **Salvar** para gravar o arquivo de configuração `/etc/named.conf`, gravar todos os arquivos de zonas individuais no diretório `/var/named` e fazer com que o daemon recarregue os arquivos de configuração.

A configuração cria uma entrada similar à seguinte no `/etc/named.conf`:

```
zone  "10.168.192.in-addr.arpa" {
        type master;
        file  "10.168.192.in-addr.arpa.zone";
};
```

Também cria o arquivo `/var/named/10.168.192.in-addr.arpa.zone` com as seguintes informações:

```
$TTL 86400
@       IN      SOA     ns.example.com. root.localhost (
                        2 ; serial
                        28800 ; refresh
                        7200 ; retry
                        604800 ; expire
                        86400 ; ttk
                        )


@       IN      NS      ns2.example.com.

1       IN      PTR     one.example.com.
2       IN      PTR     two.example.com.
```

## 28.3. Adicionando uma Zona Escrava

Para adicionar uma zona escrava (também conhecida como mestre secundária), clique no botão **Nova** e selecione **Zona Escrava**. Indique o nome do domínio da zona escrava no campo **Nome de Domínio**.

Aparece uma nova janela, conforme a Figura 28-4, com as seguintes opções:

- **Nome** — O nome do domínio indicado na janela anterior.

- **Lista dos Mestres** — Os servidores de nome dos quais a zona escrava recupera dados. Cada valor deve ser um endereço IP válido. Somente números e pontos (.) podem ser inseridos neste campo.
- **Nome do Arquivo** — Nome do arquivo do banco de dados DNS em `/var/named`.

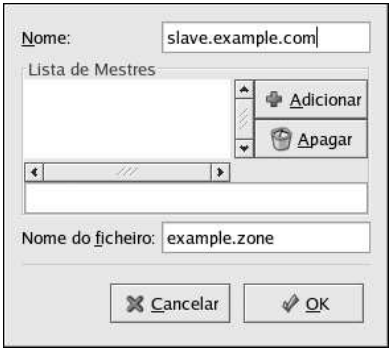


**Figura 28-4. Adicionando uma Zona Escrava**

Após configurar a zona escrava, clique em **OK** para retornar à janela principal, conforme a Figura 28-1. Clique em **Salvar** para gravar o arquivo de configuração `/etc/named.conf` e fazer com que o daemon recarregue os arquivos de configuração.

A configuração cria uma entrada similar à seguinte no `/etc/named.conf`:

```
zone "slave.example.com" {
        type slave;
        file "slave.example.com.zone";
        masters {
                 1.2.3.4;
                };
};
```

O arquivo de configuração `/var/named/slave.example.com.zone` é criado pelo serviço `named` quando este faz o download dos dados da zona pelo(s) servidor(es) mestre.

# Capítulo 29.
# Configuração da Autenticação

Quando um usuário se autentica em um sistema Red Hat Enterprise Linux, a combinação de nome de usuário e senha deve ser verificada ou *autenticada* como um usuário válido e ativo. Às vezes as informações para esta verificação residem no sistema local, e outras vezes o sistema adia a autenticação para um banco de dados de usuários em um sistema remoto.

A **Ferramenta de Configuração da Autenticação** oferece uma interface gráfica para configurar o NIS, o LDAP e o Hesiod para recuperar as informações do usuário, e também para configurar o LDAP, o Kerberos e o SMB como protocolos de autenticação.

**Nota**

Se você configurou um nível de média ou alta segurança durante a instalação, ou com a **Ferramenta de Configuração do Nível de Segurança**, os métodos de autenticação de rede, incluindo NIS e LDAP, não são permitidos através do firewall.

Este capítulo não explica cada um dos tipos de autenticação em detalhes. Ao invés disso, explica como usar a **Ferramenta de Configuração da Autenticação** para configurá-los.

Para iniciar a versão gráfica da **Ferramenta de Configuração da Autenticação** pela área de trabalho, selecione **Botão do Menu Principal** (no Painel) => **Configurações do Sistema** => **Autenticação** ou digite o comando `authconfig-gtk` em uma janela de comandos (em um **XTerm** ou em um **Terminal GNOME**, por exemplo). Para iniciar a versão texto, digite o comando `authconfig` em uma janela de comandos.

**Importante**

Após sair do programa de autenticação, as alterações têm efeito imediato.

## 29.1. Informações do Usuário

A aba **Informações do Usuário** tem diversas opções. Para habilitar uma opção, clique na caixa de verificação ao seu lado. Para desabilitar, clique novamente na caixa de verificação correspondente para desselecionar a opção. Clique em **OK** para sair do programa e aplicar as alterações.

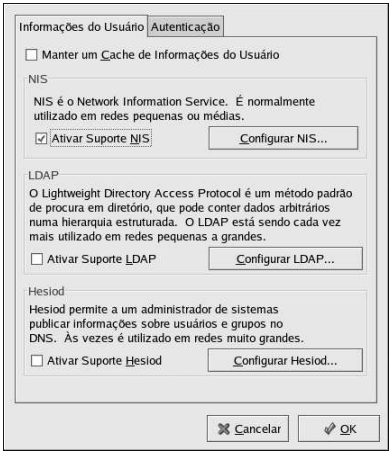


**Figura 29-1. Informações do Usuário**

A lista a seguir explica o que cada opção configura:

- **Cache das Informações de Usuários** — Selecione esta opção para habilitar o deamon cache do serviço de nomes (`nscd`) e configurá-lo para iniciar no momento da inicialização da máquina.

  O pacote `nscd` deve estar instalado para esta opção funcionar.

- **Habilitar Suporte ao NIS** — Selecione esta opção para configurar o sistema como um cliente NIS que conecta a um servidor NIS para autenticar usuário e senha. Clique no botão **Configurar NIS** para especificar o domínio e o servidor NIS. Se o servidor NIS não é especificado, o daemon tenta encontrá-lo através do broadcast.

  O pacote `ypbind` deve estar instalado para esta opção funcionar. Se o suporte ao NIS está habilitado, os serviços `portmap` e `ypbind` são iniciados e também são ativados para iniciarem no momento da inicialização da máquina.

- **Habilitar Suporte ao LDAP** — Selecione esta opção para configurar o sistema de modo a recuperar as informações de usuário através do LDAP. Clique no botão **Configurar LDAP** para especificar a **Base de Procura DN do LDAP** e o **Servidor LDAP**. Se **Usar TLS para criptografar conexões** estiver selecionada, a Segurança da Camada de Transporte (Transport Layer Security) é usada para criptografar senhas enviadas ao servidor LDAP.

  O pacote `openldap-clients` deve estar instalado para esta opção funcionar.

  Para mais informações sobre o LDAP, consulte o *Guia de Referência do Red Hat Enterprise Linux*.

- **Habilitar Suporte ao Hesiod** — Selecione esta opção para configurar o sistema de modo a recuperar as informações (inclusive informações de usuários) de um banco de dados Hesiod remoto.

  O pacote `hesiod` deve estar instalado.

## 29.2. Autenticação

A aba **Autenticação** permite a configuração dos métodos de autenticação de rede. Para habilitar esta opção, clique na caixa de verificação vazia ao seu lado. Para desabilitá-la, clique novamente na caixa para desselecionar a opção.

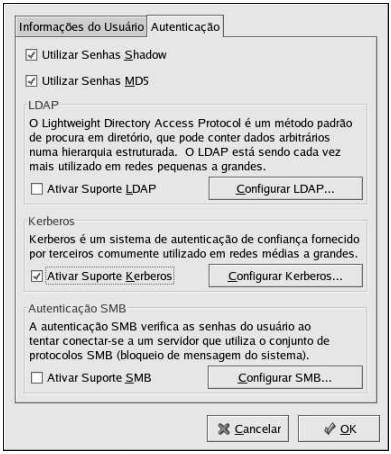


**Figura 29-2. Autenticação**

A seguir a explicação do que é configurado por cada opção:

- **Usar Senhas Shadow** — Selecione esta opção para armazenar senhas no formato shadow no arquivo `/etc/shadow` ao invés do `/etc/passwd`. Senhas shadow são habilitadas por default durante a instalação e são altamente recomendadas para aumentar a segurança do sistema.

  O pacote `shadow-utils` deve estar instalado para esta opção funcionar. Para mais informações sobre senhas shadow, consulte o capítulo *Usuários e Grupos* no *Guia de Referência do Red Hat Enterprise Linux*.
- **Usar Senhas MD5** — Selecione esta opção para habilitar as senhas MD5, que permitem senhas de até 256 caracteres ao invés dos 8 caracteres ou menos. É selecionada por default durante a instalação e é altamente recomendada para aumentar a segurança do sistema.
- **Habilitar Suporte ao LDAP** — Selecione esta opção para ter aplicações padrão habilitadas pelo PAM usando LDAP para autenticação. Clique no botão **Configurar LDAP** para especificar o seguinte:
  - **Usar TLS para criptografar conexões** — Use a Segurança da Camada de Transporte para criptografar senhas enviadas ao servidor LDAP.
  - **Base de Procura DN do LDAP** — Recupere informações de usuários pelo seu Nome Distinto (Distinguished Name - DN).
  - **Servidor LDAP** — Especifique o endereço IP do servidor LDAP.

  O pacote `openldap-clients` deve ester instalado para a opção funcionar. Consulte o *Guia de Referência do Red Hat Enterprise Linux* para mais informações sobre o LDAP.
- **Habilitar Suporte ao Kerberos** — Selecione esta opção para habilitar a autenticação do Kerberos. Clique no botão **Configurar Kerberos** para configurar:
  - **Reino** — Configure o reino do servidor Kerberos. O reino é a rede que usa o Kerberos, composta de um ou mais KDCs e um número potencialmente grande de clientes.
  - **KDC** — Defina o Centro de Distribuição de Chaves (Key Distribution Center - KDC), que é o servidor que usa tickets do Kerberos.
  - **Servidores Admin** — Especifique o servidor(es) de administração rodando `kadmind`.

Os pacotes `krb5-libs` e `krb5-workstation` devem estar instalados para esta opção funcionar. Consulte o *Guia de Referência do Red Hat Enterprise Linux* para mais informações sobre o Kerberos.

- **Habilitar Suporte ao SMB** — Esta opção configura o PAM para usar um servidor SMB para autenticar usuários. Clique no botão **Configurar SMB** para especificar:
  - **Grupo de Trabalho** — Especifique o grupo de trabalho SMB a usar.
  - **Controladores de Domínio** — Especifique os controladores de domínio SMB a usar.

## 29.3. Versão de Linha de Comando

A **Ferramenta de Configuração da Autenticação** também pode ser executada como uma ferramenta de linha de comando sem uma interface. A versão de linha de comando pode ser usada em um script de confiugração ou script do kickstart. As opções de autenticação estão resumidas na Tabela 29-1.

| Opção | Descrição |
|---|---|
| `--enableshadow` | Habilitar senhas shadow |
| `--disableshadow` | Desabilitar senhas shadow |
| `--enablemd5` | Habilitar senhas MD5 |
| `--disablemd5` | Desabilitar senhas MD5 |
| `--enablenis` | Habilitar o NIS |
| `--disablenis` | Desabilitar o NIS |
| `--nisdomain=<`*`domain`*`>` | Especificar o domínio NIS |
| `--nisserver=<`*`server`*`>` | Especificar o servidor NIS |
| `--enableldap` | Habilitar o LDAP para informações de usuários |
| `--disableldap` | Desabilitar o LDAP para informações de usuários |
| `--enableldaptls` | Habilitar o uso do TLS com o LDAP |
| `--disableldaptls` | Desabilitar o uso do TLS com o LDAP |
| `--enableldapauth` | Habilitar o LDAP para autenticação |
| `--disableldapauth` | Desabilitar o LDAP para autenticação |
| `--ldapserver=<`*`server`*`>` | Especificar o servidor LDAP |
| `--ldapbasedn=<`*`dn`*`>` | Especificar a base DN do LDAP |
| `--enablekrb5` | Habilitar o Kerberos |
| `--disablekrb5` | Desabilitar o Kerberos |
| `--krb5kdc=<`*`kdc`*`>` | Especificar o KDC do Kerberos |
| `--krb5adminserver=<`*`server`*`>` | Especificar o servidor de administração do Kerberos |
| `--krb5realm=<`*`realm`*`>` | Especificar o reino do Kerberos |
| `--enablesmbauth` | Habilitar o SMB |
| `--disablesmbauth` | Desabilitar o SMB |

| Opção | Descrição |
|---|---|
| `--smbworkgroup=<`*`workgroup`*`>` | Especificar o grupo de trabalho SMB |
| `--smbservers=<`*`server`*`>` | Especificar os servidores SMB |
| `--enablehesiod` | Habilitar o Hesiod |
| `--disablehesiod` | Desabilitar o Hesiod |
| `--hesiodlhs=<`*`lhs`*`>` | Especificar o LHS do Hesiod |
| `--hesiodrhs=<`*`rhs`*`>` | Especificar o RHS do Hesiod |
| `--enablecache` | Habilitar o `nscd` |
| `--disablecache` | Desabilitar o `nscd` |
| `--nostart` | Não iniciar ou parar os serviços `portmap`, `ypbind` ou `nscd` mesmo que eles estejam configurados |
| `--kickstart` | Não exibir a interface de usuário |
| `--probe` | Detectar e exibir defaults da rede |

**Tabela 29-1. Opções de Linha de Comando**

**Dica**

Estas opções também podem ser encontradas na página man do `authconfig` ou digitando `authconfig --help` em uma janela de comandos.

# V. Configuração do Sistema

Parte do trabalho de um administrador de sistema e configurá-lo para diversas tarefas, tipos de usuários e configurações de hardware. Esta seção explica como configurar um sistema Red Hat Enterprise Linux.

## Índice

# Capítulo 30.

# Acesso ao Console

Quando usuários normais (não root) se autenticam localmente em um computador, lhes são dados dois tipos de permissões especiais:

1. Eles podem rodar determinados programas que, caso contrário, não poderiam rodar
2. Eles podem acessar determinados arquivos (geralmente, arquivos de dispositivos especiais usados para acessar disquetes, CD-ROMs e assim por diante) que, caso contrário, não poderiam acessar

Como há consoles múltiplos em um único computador e múltiplos usuários podem se autenticar (logar) ao computador localmente ao mesmo tempo, um dos usuários deve "ganhar" a corrida de acesso aos arquivos. O primeiro usuário a se autenticar no console possui estes arquivos. Uma vez que o primeiro usuário faz log out, o próximo usuário a se autenticar é que possui os arquivos.

Em contrapartida, *todo* usuário que se autentica no console pode rodar programas para executar tarefas normalmente restritas ao usuário root. Se o X estiver rodando, estas ações podem ser inclusas como itens do menu em uma interface gráfica de usuário. Em sua distribuição, os programas acessíveis pelo console incluem `halt`, `poweroff` e `reboot`.

## 30.1. Desabilitando o Desligamento Através de [Ctrl]-[Alt]-[Del]

Por default, `/etc/inittab` especifica que seu sistema está configurado para ser desligado e reinicializado em resposta a uma combinação de teclas [Ctrl]-[Alt]-[Del] usada no console. Para desabilitar esta função, faça um comment out da segunte linha em `/etc/inittab` colocando uma marca do jogo da velha (`#`) à frente dela:

```
ca::ctrlaltdel:/sbin/shutdown -t3 -r now
```

Alternativamente, talvez você queira permitir a determinados usuários não-root o direito de desligar o sistema pelo console usando [Ctrl]-[Alt]-[Del]. Você pode restringir este privilégio a determinados usuários, seguindo os seguintes passos:

1. Adicione a opção `-a` à linha `/etc/inittab` mostrada acima, para que fique desta forma:
   ```
   ca::ctrlaltdel:/sbin/shutdown -a -t3 -r now
   ```
   O `-a` diz ao comando `shutdown` para procurar o arquivo `/etc/shutdown.allow`.
2. Crie um arquivo chamado `shutdown.allow` em `/etc`. O arquivo `shutdown.allow` deve listar os nomes de quaisquer usuários que têm permissão de desligar o sistema usando [Ctrl]-[Alt]-[Del]. O formato do arquivo `/etc/shutdown.allow` consiste em uma lista de nomes de usuários, um por linha, conforme o seguinte:
   ```
   stephen
   jack
   sophie
   ```

De acordo com este exemplo de arquivo `shutdown.allow`, stephen, jack e sophie tem permissão para desligar o sistema pelo console usando [Ctrl]-[Alt]-[Del]. Quando esta combinação de teclas é usada, o `shutdown -a` no `/etc/inittab` verifica se algum dos usuários do `/etc/shutdown.allow` (ou root) estão autenticados em um console virtual. Se um deles estiver, o desligamento do sistema continua; se não, é gravada uma mensagem de erro no console do sistema.

Para mais informações sobre o `shutdown.allow`, consulte a página man do `shutdown`.

## 30.2. Desabilitando Acesso a Programas do Console

Para desabilitar o acesso de usuários a programas do console, execute o seguinte comando como root:

```
rm -f /etc/security/console.apps/*
```

Em ambientes onde o console é protegido (senhas do gestor de início e do BIOS são definidas, [Ctrl]-[Alt]-[Delete] é desabilitado, os botões power e reset são desabilitados e assim por diante), talvez você não queira permitir que nenhum usuário execute `poweroff`, `halt` e `reboot` no console, o que é permitido por default.

Para remover estas funções, execute os seguinte comandos como root:

```
rm -f /etc/security/console.apps/poweroff
rm -f /etc/security/console.apps/halt
rm -f /etc/security/console.apps/reboot
```

## 30.3. Desabilitando Todo o Acesso ao Console

O módulo PAM `pam_console.so` administra as permissões e autenticações de arquivos do console. (Consulte o *Guia de Referência do Red Hat Enterprise Linux* para mais informações sobre a configuração do PAM.) Para desabilitar todos os acessos ao console, incluindo acessos a programas e arquivos, faça comment out de todas as linhas que referenciam o `pam_console.so` no diretório `/etc/pam.d/`. Como root, execute o script a seguir:

```
cd /etc/pam.d
for i in * ; do
sed '/[^#].*pam_console.so/s/^/#/' < $i > foo && mv foo $i
done
```

## 30.4. Definindo o Console

O módulo `pam_console.so` usa o arquivo `/etc/security/console.perms` para determinar as permissões para usuários no console do sistema. A sintaxe do arquivo é muito flexível; você pode editar o arquivo para que estas regras não sejam aplicadas. Entretanto, o arquivo default tem uma linha parecida com a seguinte:

```
<console>=tty[0-9][0-9]* :[0-9]\.[0-9] :[0-9]
```

Quando os usuários se autenticam, estão ligados a uma espécie de terminal nomeado - um servidor X com um nome como `:0` ou `minhamáquina.exemplo.com:1.0`, ou então a um dispositivo como `/dev/ttyS0` ou `/dev/pts/2`. A prática padrão é definir que os consoles virtuais e servidores X locais sejam considerados locais, mas se você deseja considerar o terminal serial `/dev/ttyS1` próximo à sua porta como local, pode alterar esta linha para o seguinte:

```
<console>=tty[0-9][0-9]* :[0-9]\.[0-9] :[0-9] /dev/ttyS1
```

## 30.5. Tornando Arquivos Acessíveis Pelo Console

No `/etc/security/console.perms`, há uma seção com linhas como:

```
<floppy>=/dev/fd[0-1]* \
         /dev/floppy/* /mnt/floppy*
```

```
<sound>=/dev/dsp* /dev/audio* /dev/midi* \
        /dev/mixer* /dev/sequencer \
        /dev/sound/* /dev/beep
<cdrom>=/dev/cdrom* /dev/cdroms/* /dev/cdwriter* /mnt/cdrom*
```

Você pode adicionar suas prórpias linhas nesta seção, se necessário. Certifique-se de que todas as linhas que adicionar referenciem o dispositivo apropriado. Por exemplo: você pode adicionar a linha a seguir:

```
<scanner>=/dev/scanner /dev/usb/scanner*
```

(Obviamente, certifique-se de que o `/dev/scanner` seja realmente o seu scanner, e não seu disco rígido, por exemplo.)

Este é o primeiro passo. O segundo é definir o que é feito com estes arquivos. Procure na última seção do `/etc/security/console.perms` por linhas similares a:

```
<console> 0660 <floppy> 0660 root.floppy
<console> 0600 <sound>  0640 root
<console> 0600 <cdrom>  0600 root.disk
```

e adicione uma linha como:

```
<console> 0600 <scanner> 0600 root
```

Então, quando você se autenticar no console, lhe será dada a propriedade (ownership) do dispositivo `/dev/scanner` com permissões 0600 (legível e alterável somente por você). Quando você fizer o log out, o dispositivo é de propriedade do usuário root e ainda possui as mesmas permissões 0600 (agora legível e alterável somente por root).

## 30.6. Habilitando o Acesso a Outras Aplicações pelo Console

Para tornar outras aplicações acessíveis a usuários do console, é necessário um pouco mais de trabalho.

Primeiramente, o acesso pelo console funciona *somente* para aplicações que residem em `/sbin/` ou em `/usr/sbin/`, portanto a aplicação que você deseja executar deve estar ali. Após verificar isto, siga estes passos:

1. Crie uma ligação do nome de sua aplicação, como nosso programa de amostra *`foo`*, para a aplicação `/usr/bin/consolehelper`:
   ```
   cd /usr/bin
   ln -s consolehelper foo
   ```
2. Crie o arquivo `/etc/security/console.apps/`*`foo`*:
   ```
   touch /etc/security/console.apps/foo
   ```
3. Crie um arquivo de configuração PAM para o serviço *`foo`* em `/etc/pam.d/`. Uma maneira fácil de fazer isso é começar com uma cópia do arquivo de configuração PAM do serviço halt, e então alterar o arquivo se você quiser alterar o comportamento:
   ```
   cp /etc/pam.d/halt /etc/pam.d/foo
   ```

Agora, quando o `/usr/bin/`*`foo`* é executado, chama o `consolehelper`, que autentica o usuário com a ajuda do `/usr/sbin/userhelper`. Para autenticar o usuário, o `consolehelper` pede pela senha do usuário se o `/etc/pam.d/`*`foo`* for uma cópia do `/etc/pam.d/halt` (caso contrário, faz exatamente o que é especificado no `/etc/pam.d/`*`foo`*), e então executa o `/usr/sbin/`*`foo`* com permissões root.

No arquivo de configuração PAM, pode-se configurar uma aplicação para usar o módulo*pam_timestamp* para lembrar (cache) de uma tentativa de autenticação bem-sucedida.

Quando uma aplicação é iniciada e a devida autenticação é fornecida (a senha root), é criado um arquivo timestamp. Por default, uma autenticação bem-sucedida permanece no cache por cinco minutos. Durante este intervalo, qualquer outra aplicação configurada para usar `pam_timestamp` e ser executada na mesma seção é autenticada automaticamente para o usuário — não é neccesário indicar a senha root novamente.

Este módulo está incluso no pacote `pam` package. Para habilitar esta funcionalidade, o arquivo de configuração PAM no `etc/pam.d/` deve incluir estas linhas:

```
auth sufficient /lib/security/pam_timestamp.so
session optional /lib/security/pam_timestamp.so
```

A primeira linha que começa com `auth` deve estar após quaisquer outras linhas `auth sufficient`; e a linha que começa com `session` deve estar após quaisquer outras linhas `session optional`.

Se uma aplicação configurada para usar `pam_timestamp` for autenticada com sucesso pelo **Botão do Menu Principal** (no Painel), o ícone  é exibido na área de notificação do painel, se você estiver usando os ambientes GNOME ou KDE. Após a autenticação expirar (o default são cinco minutos), o ícone desaparece.

O usuário pode optar por esquecer a autenticação gravada no cache. Bast clicar no ícone e selecionar a opção para esquecer a autenticação.

## 30.7. O Grupo `floppy`

Se, por qualquer motivo, o acesso pelo console não é apropriado e você precisa dar a usuários não-root acesso ao drive de disquete do seu sistema, isto pode ser feito usando o grupo `floppy`. Adicione o(s) usuário(s) ao grupo `floppy` usando sua ferramenta preferida. Por exemplo: o comando `gpasswd` pode ser usado para adicionar o usuário 'fred' ao grupo `floppy`:

```
gpasswd -a fred floppy
```

Agora o usuário fred pode acessar o drive de disquete do sistema pelo console.

Capítulo 31.

# Configuração de Data e Hora

A **Ferramentas das Propriedades de Hora e Data** permite ao usuário alterar a data e a hora do sistema, configurar o fuso horário usado pelo sistema e configurar o daemon do Protocolo de Horário da Rede (Network Time Protocol - NTP) a fim de sincronizar o relógio do sistema com um servidor de horário.

Você deve estar rodando o Sistema X Window e ter privilégios root para usar a ferramenta. Para iniciar a aplicação pela área de trabalho, vá para o **Botão do Menu Principal => Configurações do Sistema => Data e Hora** ou digite o comando `redhat-config-date` em uma janela de comandos (em um terminal XTerm ou GNOME, por exemplo).

## 31.1. Propriedades de Data e Hora

Conforme exibido na Figura 31-1, a primeira janela com abas que aparece é para configurar a data e a hora do sistema e o daemon do NTP (`ntpd`).


**Figura 31-1. Propriedades de Data e Hora**

Para alterar a data, use as setas para a direita e para a esquerda do mês para alterá-lo, use as setas para a direita e para a esquerda ao lado do ano para alterá-lo e clique no dia da semana desejado. As alterações têm efeito após clicar no botão **OK**.

Para alterar a hora, use os botões para cima e para baixo ao lado de **Hora**, **Minuto**, and **Segundo** na seção **Time**. As alterações têm efeito após o botão **OK** ser clicado.

O daemon do Protocolo de Horário da Rede (Network Time Protocol - NTP) sincroniza o relógio do sistema com um servidor de horário remoto ou fonte de horário (como um satélite). Para habilitar esta funcionalidade, selecione **Habilitar Protocolo de Horário da Rede**. Isto habilita o menu suspenso **Servidor**. Você pode escolher um dos servidores pré-definidos ou digitar o nome do servidor no menu suspenso. Seu sistema não começa a sincronizar com o servidor NTP até que você clique em **OK**. Após clicar, a configuração é salva e o daemon do NTP é iniciado (ou reiniciado se já estiver rodando).

Clicar o botão **OK** aplica quaisquer alterações efetuadas em data e hora, na configuração do daemon do NTP e do fuso horário. Também sai do programa.

## 31.2. Configuração do Fuso Horário

Para configurar o fuso horário do sistema, clique na aba **Fuso Horário**. O fuso horário pode ser alterado através do mapa interativo ou escolhendo o fuso horário desejado na lista abaixo do mapa. Para usar o mapa, clique na cidade que representa o fuso horário desejado. Um **X** vermelho aparece e a seleção do fuso é alterada na lista abaixo do mapa. Clique em **OK** para aplicar as alterações e sair do programa.

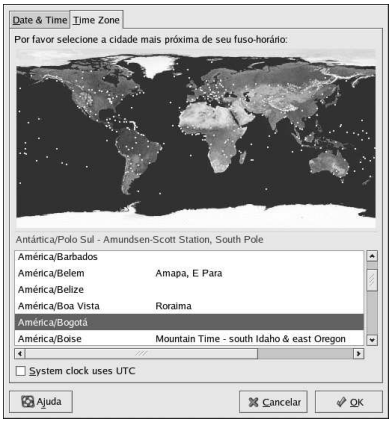


**Figura 31-2. Propriedades do Fuso Horário**

Se o relógio do seu sistema está definido para usar UTC, selecione a opção **Relógio do Sistema usa UTC**. UTC significa *Universal Time, Coordinated*, também conhecido como 'Greenwich mean time (GMT). Os outros fusos horários são determinados pela adição ou subtração do horário UTC.

# Capítulo 32.

# Configuração do Teclado

O programa de instalação permite que os usuários configurem um layout de teclado para seus sistemas. Para configurar um layout de teclado diferente após a instalação, use a **Ferramenta de Configuração do Teclado**.

Para iniciar a **Ferramenta de Configuração do Teclado**, selecione o botão do **Menu Principal** (no painel) => **Configurações do Sistema** => **Teclado**, ou digite o comando `redhat-config-keyboard` em uma janela de comandos (shell).


**Figura 32-1. Ferramenta de Configuração do Teclado**

Selecione um layout de tcaldo da lista (ex.: **U.S. English**) e clique em **OK**. Para que as tenham efeito, você deve fazer o logout da sua sessão gráfica e depois se autenticar (login) novamente.

# Capítulo 33.

# Configuração do Mouse

O programa de instalação permite aos usuários selecionar o tipo de mouse conectado ao sistema. Para configurar um tipo diferente de mouse, use a **Ferramenta de Configuração do Mouse**.

Para iniciar a **Ferramenta de Configuração do Mouse**, selecione o botão do **Menu Principal** (no Painel) => **Configurações do Sistema** => **Mouse**, ou digite o comando `redhat-config-mouse` em uma janela de comandos (em um terminal XTerm ou GNOME, por exemplo). Se o Sistema X Window não estiver rodando, a versão texto da ferramenta é iniciada.


**Figura 33-1. Selecione o Mouse**

Escolha o novo tipo de mouse para o seu sistema. Se não houver um tipo correspondente exato, escolha um que seja mais compatível com o sistema e com o mouse.

O dispositivo embutido de apontamento, como uma área de toque em um laptop, é geralmente compatível ao PS/2.

Todos os tipos de mouse têm anexos como **PS/2**, **serial**, ou **USB** entre parênteses. Isto especifica a porta do mouse.

A porta de um mouse PS/2 se parece com  .

A porta de um mouse serial se parece com  .

A porta de um mouse USB se parece com  .

Se o tipo de mouse específico não está listado, selecione um do itens **Genérico**, baseado no número de botões e interface de seu mouse.

**Dica**

Selecione a opção **Genérico - Mouse de Rolagem** com a porta apropriada para habilitar o botão de rolagem do mouse.

O botão de rolagem de um mouse pode ser usado como o botão do meio para cortar texto, colar texto e outras funções. Se o mouse tem apenas dois botões, selecione **Emular 3 botões** para usar o mouse de dois botões como se tivesse três. Quando esta opção está habilitada, clicar os dois botões do mouse simultaneamente emula a ação do clique do botão do meio.

Se um mouse de porta serial é selecionado, clique no botão **Dispositivos Seriais** para configurar o número correto do dispositivo serial, tal como `/dev/ttyS0`, para o mouse.

Clique em **OK** para salvar o novo tipo de mouse. A seleção é gravada no arquivo `/etc/sysconfig/mouse`, e então o serviço de console do mouse - `gpm` - é reiniciado. As alterações também são gravadas no arquivo de configuração do Sistema X Window - `/etc/X11/XF86Config`. No entanto, a alteração do tipo de mouse não é aplicada automaticamente para a sessão X (gráfica) atual. Para habilitar o novo tipo de mouse, faça o log out da área de trabalho gráfica e depois faça o login novamente.

**Dica**

Para alterar a ordem dos botões do mouse para uma pessoa canhota, vá para o botão do **Menu Principal** (no Painel) => **Preferências** => **Mouse**, e selecione a orientação do mouse para**Mouse para Canhoto**.

# Capítulo 34.
# Configuração do Sistema X Window

Durante a instalação, o monitor, a placa de vídeo e a tela do sistema são configuradas. Para alterar qualquer uma destas configurações, use a **Ferramenta de Configuração do X**.

Para iniciar a **Ferramenta de Configuração do X**, selecione **Botão do Menu Principal** (no Painel) => **Configurações do Sistema => Tela**, ou digite o comando `redhat-config-xfree86` em uma janela de comandos (ex.: em um XTerm ou terminal GNOME). Se o Sistema X Window não está rodando, é iniciada uma pequena versão do X para rodar o programa.

Após alterar alguma destas configurações, faça log out da área de trabalho gráfica e autentique-se novamente para habilitar as alterações.

## 34.1. Configurações da Tela

A aba **Tela** permite que usuários alterem a *resolução* e a *definição de cores*. A tela de um monitor consiste de pontos minúsculos chamados *pixels*. O número de pixels apresentados de uma vez é chamado resolução. Por exemplo: a resolução 1024x768 significa que são usados 1024 pixels na horizontal e 768 pixels na vertical. Quanto maior a resolução, mais imagens o monitor pode exibir de uma vez. Quanto maior a resolução, menor será a aparência dos ícones na área de trabalho.

A definição de cores da tela determina quantas cores possíveis são exibidas. Quanto maior a definição de cores, maior o contraste entre as cores.

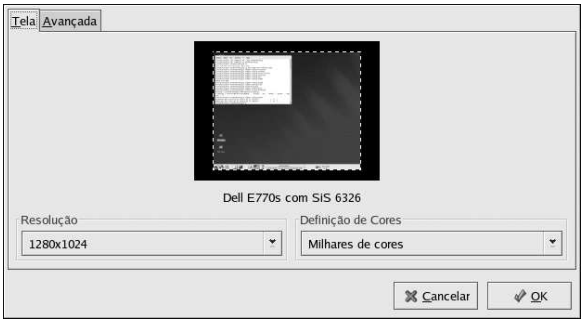


**Figura 34-1. Configurações da Tela**

## 34.2. Configurações Avançadas

Quando a aplicação é iniciada, detecta o monitor e a placa de vídeo. Se o hardware for detectado corretamente, suas informações são exibidas na aba **Avançadas**, conforme a Figura 34-2.

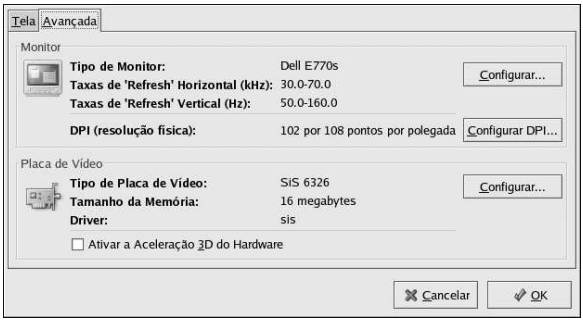


**Figura 34-2. Configurações Avançadas**

Para alterar o tipo de monitor ou outras de suas configurações, clique no botão **Configurar** correspondente. Para alterar o tipo da placa de vídeo ou outras de suas configurações, clique no botão **Configurar** ao lado de suas configurações.

# Capítulo 35.
# Configuração de Usuário e Grupo

A **Administrador de Usuários** permite a você visualizar, modificar, adicionar e apagar usuários e grupos locais.

Para usar a **Administrador de Usuários**, você deve estar rodando o Sistema X Window, ter privilégios root e ter o pacote RPM `redhat-config-users` instalado. Para iniciar a **Administrador de Usuários** pela área de trabalho, vá para o botão do **Menu Principal** (no Painel) => **Configurações do Sistema** => **Usuários e Grupos**. Ou, digite o comando `redhat-config-users` em uma janela de comandos (um terminal XTerm ou GNOME, por exemplo).

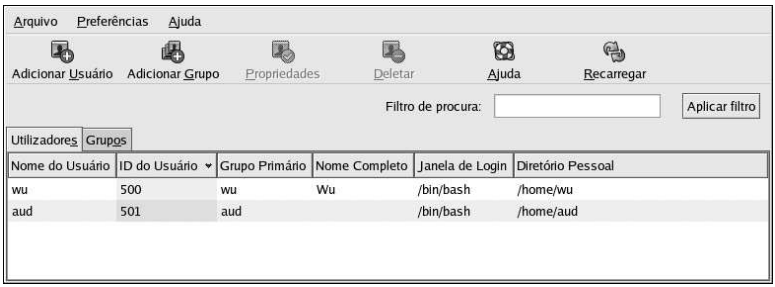


**Figura 35-1. Administrador de Usuários**

Para visualizar uma lista dos usuários locais do sistema, clique na aba **Usuários**. Para visualizar uma lista dos grupos locais do sistema, clique na aba **Grupos**.

Para encontrar um usuário ou grupo específico, digite algumas das primeiras letras do nome no campo **Filtro da Busca**. Pressione [Enter] ou clique no botão **Aplicar filtro**. A lista filtrada é então exibida.

Para escolher usuários ou grupos, clique na coluna de nomes. Os usuários ou grupos são classificados pelo valor desta coluna.

O Red Hat Enterprise Linux reserva os IDs abaixo de 500 para usuários do sistema. Por default, a **Administrador de Usuários** não exibe os usuários do sistema. Para visualizar todos os usuários, inclusive os do sistema, desselecione a opção **Preferências** => **Filtrar usuários e grupos do sistema** a partir do menu suspenso.

## 35.1. Adicionando um Novo Usuário

Para adicionar um novo usuário, clique no botão **Adicionar Usuário**. Aparece uma janela, conforme exibido na Figura 35-2. Digite o nome e nome completo do novo usuário nos respectivos campos. Digite a senha do usuário nos campos **Senha** e **Confirmar Senha**. A senha deve ter no mínimo seis caracteres.

**Dica**

Quanto mais longa é a senha do usuário, mais difícil é para alguém adivinhá-la e se autenticar na conta do usuário sem sua permissão. Também é recomendável que a senha não seja baseada em uma palavra do dicionário, e que seja composta de uma combinação de letras, números e caracteres especiais.

Selecione uma shell de login. Se você não está certo sobre sua escolha, aceite o valor default `/bin/bash`. O diretório home default é `/home/`*`nome_do_usuário`*`/`. Você pode alterar o diretório home que foi criado para o usuário ou pode optar por não criar um diretório home desselecionando **Criar diretório home**.

Se você optar por criar um diretório home, os arquivos de configuração default são copiados do diretório `/etc/skel/` para o novo diretório home.

O Red Hat Enterprise Linux usa um esquema de *grupo privado do usuário* (user private group - UPG). O esquema UPG não altera em nada a maneira como o padrão UNIX lida com grupos; apenas oferece uma nova convenção. Sempre que você criar um novo usuário, um grupo único com o mesmo nome é criado, por default. Se você não quer criar este grupo, desselecione **Criar um grupo privado para o usuário**.

Para especificar um ID para o usuário, selecione **Especificar o ID do usuário manualmente**. Se a opção não estiver selecionada, o próximo ID disponível começando pelo número 500 será atribuído ao novo usuário. O Red Hat Enterprise Linux reserva os IDs abaixo de 500 para usuários do sistema.

Clique em **OK** para criar o usuário.


**Figura 35-2. Novo Usuário**

Para configurar propriedades mais avançadas do usuário, como expiração da senha, ou para modificar as propriedades após adicionar o usuário, consulte a Seção 35.2 para mais informações.

Para adicionar o usuário em mais grupos, clique na aba **Usuário**, selecione o usuário e clique em **Propriedades**. Na janela **Propriedades do Usuário**, selecione a aba **Grupos**. Selecione os grupos nos quais você deseja adicionar o usuário, selecione também o grupo principal deste usuário e clique em **OK**.

## 35.2. Modificando as Propriedades do Usuário

Para visualizar as propriedades de um usuário existente, clique na aba **Usuários**, selecione o usuário na lista e clique em **Propriedades** no menu de botões (ou vá para **Arquivo => Propriedades** no menu suspenso). Aparece uma janela similar à Figura 35-3.

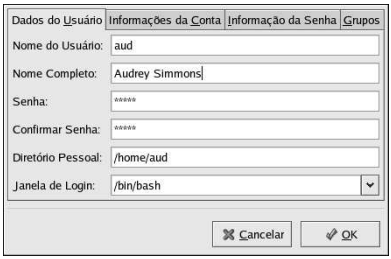


**Figura 35-3. Propriedades do Usuário**

A janela **Propriedades do Usuário** é dividida em diversas abas:

- **Dados do Usuário** — Exibe as informações básicas do usuário configuradas quando você o adicionou. Use esta aba para alterar o nome completo, a senha, o diretório home ou a shell de login do usuário.
- **Informações da Conta** — Selecione **Habilitar expiração da conta** se você quer que a conta expire em uma determinada data. Insira a data nos campos providos. Selecione **Conta do usuário está bloqueada** para bloquear a conta do usuário de modo que ele não possa efetuar o login no sistema.
- **Informações da Senha** — Esta aba exibe a data em que a senha do usuário foi alterada pela última vez. Para forçar o usuário a alterar a senha após um certo número de dias, selecione **Habilitar expiração da senha**. É possível alterar o número de dias antes da expiração da senha, o número de dias antes de avisar o usuário a alterar senhas e número de dias antes da conta se tornar inativa.
- **Grupos** — Selecione os grupos aos quais você deseja adicionar o usuário e seu grupo principal.

## 35.3. Adicionando um Novo Grupo

Para adicionar um novo grupo de usuários, clique no botão **Adicionar Grupo**. Aparece uma janela similar à Figura 35-4. Digite o nome do grupo a ser criado. Para especificar um ID para o grupo novo, selecione **Especificar ID do grupo manualmente** e então selecione o GID ('group ID'). O Red Hat Enterprise Linux reserva os IDs abaixo de 500 para grupos do sistema.

Clique em **OK** para criar o grupo. Ele aparece na lista de grupos.


**Figura 35-4. Novo Grupo**

Para adicionar usuários ao grupo, consulte a Seção 35.4.

## 35.4. Alterando as Propriedades do Grupo

Para visualizar as propriedades de um grupo existente, selecione-o a partir da lista e clique no botão **Propriedades** (ou selecione **Arquivo => Propriedades** no menu suspenso). Aparece uma janela similar à Figura 35-5 appears.


**Figura 35-5. Propriedades do Grupo**

A aba **Usuários do Grupo** exibe quais usuários são membros do grupo. Selecione usuários para serem adicionados ao grupo, ou desselecione usuários a serem removidos. Clique em **OK** para modificar os usuários no grupo.

## 35.5. Configuração da Linha de Comando

Se você prefere trabalhar com ferramentas de linha de comando ou não tem o Sistema X Window instalado, use esta seção para configurar usuários e grupos.

### 35.5.1. Adicionando um Usuário

Para adicionar um usuário ao sistema:

1. Submeta o comando `useradd` para criar uma conta de usuário bloqueada:
   `useradd <username>`
2. Desbloqueie a conta com o comando `passwd` para atribuir uma senha e definir suas regras de validade.
   `passwd <username>`

As opções de linha de comando para `useradd` estão detalhadas na Tabela 35-1.

| Opção | Descrição |
|---|---|
| `-c comentário` | Comentário para o usuário |
| `-d home-dir` | Diretório home a ser usado ao invés do default `/home/nome_do_usuário/` |
| `-e data` | A data para a desabilitação da conta no formato YYYY-MM-DD |
| `-f dias` | Número de dias entre a expiração da senha e a desabilitação da conta. (Se **0** é especificado, a conta é desabilitada imediatamente após a expiração da senha. Se **-1** é especificado, a conta não é desabilitada após a senha expirar.) |
| `-g nome-do-grupo` | O nome ou número do grupo default do usuário (o grupo deve existir antes de ser espcificado aqui.) |
| `-G lista-de-grupos` | Lista de nomes ou números dos grupos adicionais (além do default), separados por vírgulas, dos quais o usuário faz parte. (Os grupos devem existir antes de serem especificados aqui.) |

| Opção | Descrição |
|---|---|
| `-m` | Criar o diretório home se ainda não houver um |
| `-M` | Não criar o diretório home |
| `-n` | Não criar um grupo privado para o usuário |
| `-r` | Crie uma conta do sistema com ID de usuário abaixo de 500 e sem diretório home |
| `-p` *`senha`* | A senha criptografada com `crypt` |
| `-s` | A shell de login do usuário, cujo default é `/bin/bash` |
| `-u` *`id-do-usuário`* | ID do usuário, que deve ser único e maior que 499 |

**Tabela 35-1. Opções de linha de comando do `useradd`**

### 35.5.2. Adicionando um Grupo

Para adicionar um grupo ao sistema, use o comando `groupadd`:

`groupadd <`*`group-name`*`>`

As opções de linha de comando do `groupadd` estão detalhadas na Tabela 35-2.

| Opção | Descrição |
|---|---|
| `-g` *`id-do-grupo`* | ID do grupo, que deve ser único e maior que 499 |
| `-r` | Crie um grupo do sistema com ID menor que 500 |
| `-f` | Saia com um erro se o grupo já existe (o grupo não é alterado). Se as opções `-g` e `-f` são especificaddas, mas o grupo já existe, a opção `-g` é ignorada. |

**Tabela 35-2. Opções de Linha de Comando do `groupadd`**

### 35.5.3. Validade da Senha

Por motivos de segurança, é recomendado requerer aos usuários mudar suas senhas periodicamente. Isto pode ser feito ao adicionar ou editar um usuário na aba **Informações da Senha** da **Administrador de Usuários**.

Para configurar a expiração da senha de um usuário na janela de comandos, use o comando `chage` seguido de uma das opções contidas na Tabela 35-3, seguida do nome do usuário.

**Importante**

Senhas shadow devem ser habilitadas para usar o comando `chage`

| Opção | Descrição |
|---|---|

| Opção | Descrição |
|---|---|
| `-m` *dias* | Especifique o número mínimo de dias para o usuário alterar a senha. Se o valor é 0, a senha não expira. |
| `-M` *dias* | Especifique o número máximo de dias para a validade da senha. Quando o número de dias especificado nesta opção mais o número de dias especificado na opção `-d` é menor que a data atual, o usuário deve mudar a senha antes de usar a conta. |
| `-d` *dias* | Especifique o número de dias em que a senha foi alterada pela última vez, desde 1o de Janeiro de 1970. |
| `-I` *dias* | Especifique o número de dias inativos entre a expiração da senha e o bloqueio da conta. Se o valor é 0, a conta não é bloqueada após a senha expirar. |
| `-E` *data* | Especifique a data na qual a conta é bloqueada, no formato YYYY-MM-DD. Também é possível usar o número de dias desde 1o de Janeiro de 1970, ao invés da data. |
| `-W` *dias* | Especifique o número de dias antes da expiração da senha para avisar o usuário. |

**Tabela 35-3. Opções de Linha de Comando do `chage`**

**Dica**

Se o comando `chage` é seguido diretamente pelo nome do usuário (sem opções), traz os valores atuais para a validade da senha e permite que eles sejam alterados.

Se um administrador de sistema deseja que o usuário defina a senha na primeira vez que se autenticar, uma senha inicial ou vazia para o usuário pode ser definida para expirar imediatamente após a primeira autenticação.

Para forçar o usuário a configurar sua senha na primeira autenticação (login) no console, siga estes passos. Note que este processo não funciona se o usuário se autenticar usando o protocolo SSH.

1. *Bloquear a senha do usuário* — Se o usuário não existe, use o comando `useradd` para criar a conta do usuário, mas não atribua uma senha para que continue bloqueada.

   Se a senha já está habilitada, bloqueie-a com o comando:
   `usermod -L username`

2. *Forçar expiração imediata da senha* — Digite o seguinte comando:
   `chage -d 0 username`

   Este comando define o valor da data em que a senha foi alterada pela última vez em relação ao período (1o de Janeiro de 1970). Este valor força a expiração imediata da senha independente das regras de validade, caso existam.

3. *Desbloqueie a conta* — Há duas maneiras de executar este passo. O administrador pode atribuir uma senha inicial ou uma senha vazia.

   

   **Aviso**

   Não use o comando `passwd` para definir a senha, pois desabilita a expiração imediata da senha configurada recentemente.

Para atribuir uma senha inicial, siga estes passos:

- Inicie o interpretador Python da linha de comando com `python`. Este exibe o seguinte:
```
Python 2.2.2 (#1, Dec 10 2002, 09:57:09)
[GCC 3.2.1 20021207 (Red Hat Enterprise Linux 3 3.2.1-2)] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>>
```
- Na janela de comandos, digite o seguinte (substituindo *`password`* pela senha a ser criptografada e *`salt`* pela combinação exata de 2 cacateres alfabéticos em caixa alta ou baixa, de 2 dígitos, o caracter ponto (.), ou a barra (/), como por exemplo: `ab` ou `12`:
```
import crypt; print crypt.crypt("password","salt")
```
  O output é a senha criptografada, similar a `12CsGd8FRcMSM`.
- Digite [Ctrl]-[D] para sair do interpretador Python.
- Corte e cole o output exato da senha criptografada, sem espaços em branco iniciais ou no meio, para o seguinte comando:
```
usermod -p "encrypted-password" username
```

Ao invés de atribuir uma senha inicial, pode-se atribuir uma senha vazia com o seguinte comando:
```
usermod -p "" username
```

**Cuidado**

Apesar de usar uma senha vazia ser conveniente para ambos, usuário e administrador, há um pequeno risco de uma terceira pessoa fazer o login primeiro e acessar o sistema. Para minimizar esta ameaça, é recomendado que o administrador verifique se o usuário está pronto para fazer o login quando a conta está desbloqueada.

Em qualquer um dos casos, a senha será requisitada ao usuário na autenticação (login) inicial.

## 35.6. Explicando o Processo

Os passos a seguir ilustram o que acontece se o comando `useradd juan` é submetido em um sistema no qual as senhas shadow estão habilitadas:

1. É criada uma nova linha para `juan` em `/etc/passwd`. A linha tem as seguintes características:
   - Começa com o nome do usuário `juan`.
   - Há um `x` no campo da senha indicando que o sistema está usando senhas shadow.
   - É criado um ID maior ou igual a 500 para o usuário. (No Red Hat Enterprise Linux, IDs de usuários e de grupos abaixo de 500 são reservados para uso do sistema.)
   - É criado um ID do grupo maior ou igual a 500.
   - A informação opcional GECOS é deixada em branco.
   - O diretório home de `juan` é definido como `/home/juan/`.
   - A shell default é definida em `/bin/bash`.

2. É criada uma nova linha para `juan` em `/etc/shadow`. A linha tem as seguintes características:
   - Começa com o nome do usuário `juan`.
   - Dois pontos de exclamação (`!!`) aparecem no campo da senha do arquivo `/etc/shadow`, o que bloqueia a conta.

**Nota**

Se uma senha criptografada é passada usando a opção `-p`, é inserida no arquivo `/etc/shadow` na nova linha do usuário.

- A senha é definida para nunca expirar.

3. É criada uma nova linha `juan` para o grupo em `/etc/group`. Um grupo com o mesmo nome do usuário é chamado *grupo privado do usuário*. Para mais informações sobre grupos privados de usuário, consulte a Seção 35.1.

   A linha criada no `/etc/group` tem as seguintes características:

   - Começa com o nome do grupo `juan`.
   - Aparece um `x` no campo da senha indicando que o sistema está usando senhas shadow.
   - O ID do grupo coincide com o ID do usuário `juan` iem `/etc/passwd`.

4. É criada uma nova linha `juan` para o grupo em `/etc/gshadow`. A linha tem as seguintes características:

   - Começa com o nome do grupo `juan`.
   - Aparece um ponto de exclamação (`!`) no campo da senha do arquivo `/etc/gshadow`, que bloqueia o grupo.
   - Todos os outros campos estão em branco.

5. É criado um diretório para o usuário `juan` em `/home/`. Esse diretório pertence ao usuário `juan` e ao grupo `juan`. No entanto, tem permissões para ler, escrever e executar *apenas* para o usuário `juan`. Todas as outras permissões são negadas.
6. Os arquivos do diretório `/etc/skel/` (que contém configurações default do usuário) são copiados para o novo diretório `/home/juan/`.

Neste ponto, uma conta bloqueada chamada `juan` existe no sistema. Para ativá-la, o administrador deve imediatamente atribuí-la com uma senha, usando o comando `passwd` e, opcionalmente, definir as regras de validade da senha.

## 35.7. Informações Adicionais

Consulte estas referências para mais informações sobre o gerenciamento de grupos e usuários.

### 35.7.1. Documentação Instalada

- As páginas man do `useradd`, `passwd`, `groupadd` e do `chage`.

### 35.7.2. Livros Relacionados

- *Guia de Referência do Red Hat Enterprise Linux* — Este manual oferece uma lista dos usuários e grupos padrão, aborda a questão dos grupos privados de usuários e traz uma visão geral das senhas shadow.

- *Introdução à Administração de Sistemas Red Hat Enterprise Linux* — Este manual complementar contém mais informações sobre o gerenciamento de grupos e usuários, e também sobre o gerenciamento de recursos do usuário.

Capítulo 36.

# Configuração da Impressora

The **Ferramenta de Configuração da Impressora** allows users to configure a printer. This tool helps maintain the printer configuration file, print spool directories, and print filters.

Red Hat Enterprise Linux 3 uses the CUPS printing system. If a system was upgraded from a previous Red Hat Enterprise Linux version that used CUPS, the upgrade process preserved the configured queues.

Using the **Ferramenta de Configuração da Impressora** requires root privileges. To start the application, select **Main Menu Button** (on the Panel) **=> System Settings => Printing**, or type the command `redhat-config-printer`. This command automatically determines whether to run the graphical or text-based version depending on whether the command is executed in the graphical desktop environment or from a text-based console.

To force the **Ferramenta de Configuração da Impressora** to run as a text-based application, execute the command `redhat-config-printer-tui` from a shell prompt.

**Important**

Do not edit the `/etc/printcap` file or the files in the `/etc/cups/` directory. Each time the printer daemon (`cups`) is started or restarted, new configuration files are dynamically created. The files are dynamically created when changes are applied with the **Ferramenta de Configuração da Impressora** as well.

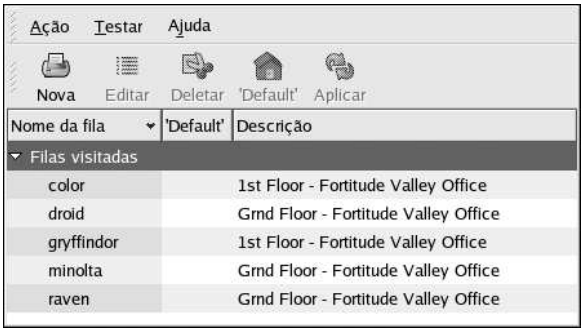


**Figura 36-1. Ferramenta de Configuração da Impressora**

The following types of print queues can be configured:

- **Locally-connected** — a printer attached directly to the computer through a parallel or USB port.
- **Networked CUPS (IPP)** — a printer that can be accessed over a TCP/IP network via the Internet Printing Protocol, also known as IPP (for example, a printer attached to another Red Hat Enterprise Linux system running CUPS on the network).

- **Networked UNIX (LPD)** — a printer attached to a different UNIX system that can be accessed over a TCP/IP network (for example, a printer attached to another Red Hat Enterprise Linux system running LPD on the network).
- **Networked Windows (SMB)** — a printer attached to a different system which is sharing a printer over a SMB network (for example, a printer attached to a Microsoft Windows™ machine).
- **Networked Novell (NCP)** — a printer attached to a different system which uses Novell's NetWare network technology.
- **Networked JetDirect** — a printer connected directly to the network through HP JetDirect instead of to a computer.

**Important**

If you add a new print queue or modify an existing one, you must apply the changes to them to take effect.

Clicking the **Apply** button saves any changes that you have made and restarts the printer daemon. The changes are not written to the configuration file until the printer daemon is restarted. Alternatively, you can choose **Action => Apply**.

## 36.1. Adding a Local Printer

To add a local printer, such as one attached through a parallel port or USB port on your computer, click the **New** button in the main **Ferramenta de Configuração da Impressora** window to display the window in Figura 36-2. Click **Forward** to proceed.

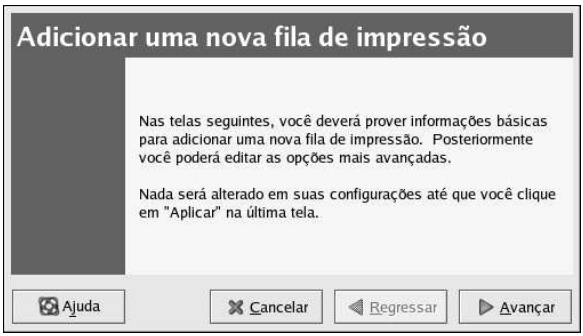


**Figura 36-2. Adding a Printer**

Na janela exibida na Figura 36-3, indique um nome único para a impressora no campo **Nome**. O nome de uma impressora não pode conter espaços e deve começar por uma letra. Este nome pode conter letras, números, hífens (-) e underscores (_). Opcionalmente, indique uma breve descrição da impressora, que pode conter espaços.

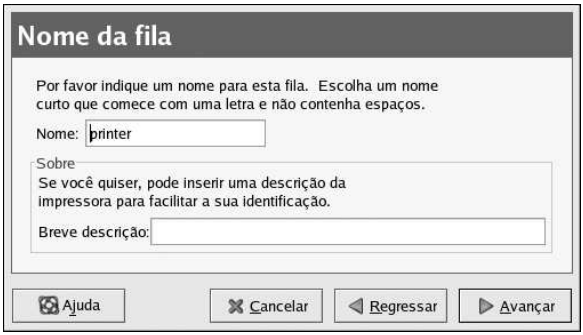


**Figura 36-3. Selecting a Queue Name**

After clicking **Forward**, Figura 36-4 appears. Select **Locally-connected** from the **Select a queue type** menu, and select the device. The device is usually `/dev/lp0` for a parallel printer or `/dev/usb/lp0` for a USB printer. If no devices appear in the list, click **Rescan devices** to rescan the computer or click **Custom device** to specify it manually. Click **Forward** to continue.

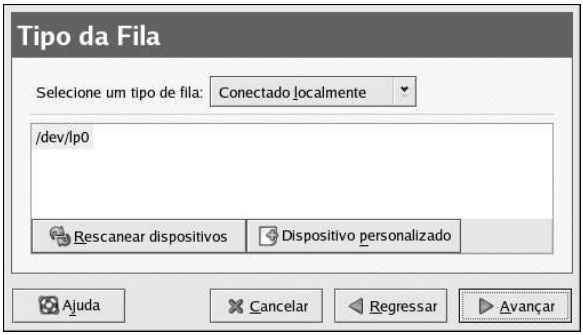


**Figura 36-4. Adding a Local Printer**

Em seguida, selecione o tipo de impressora. Consulte a Seção 36.7 para mais detalhes.

## 36.2. Adding an IPP Printer

An IPP printer is a printer attached to a different Linux system on the same network running CUPS or a printer configured on another operating system to use IPP. By default, the **Ferramenta de Configuração da Impressora** browses the network for any shared IPP printers. (This option can be changed by selecting **Action => Sharing** from the pulldown menu.) Any networked IPP printer found via CUPS browsing appears in the main window under the **Browsed queues** category.

If you have a firewall configured on the print server, it must be able to send and receive connections on the incoming UDP port, 631. If you have a firewall configured on the client (the computer sending the print request), it must be allowed to send and accept connections on port 631.

If you disable the automatic browsing feature, you can still add a networked IPP printer by clicking the **New** button in the main **Ferramenta de Configuração da Impressora** window to display the window in Figura 36-2. Click **Forward** to proceed.

Na janela exibida na Figura 36-3, indique um nome único para a impressora no campo **Nome**. O nome de uma impressora não pode conter espaços e deve começar por uma letra. Este nome pode conter letras, números, hífens (-) e underscores (_). Opcionalmente, indique uma breve descrição da impressora, que pode conter espaços.

After clicking **Forward**, Figura 36-5 appears. Select **Networked CUPS (IPP)** from the **Select a queue type** menu.

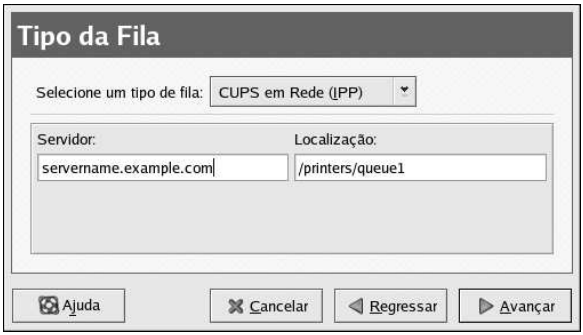


**Figura 36-5. Adding an IPP Printer**

Text fields for the following options appear:

- **Server** — The hostname or IP address of the remote machine to which the printer is attached.
- **Path** — The path to the print queue on the remote machine.

Click **Forward** to continue.

Em seguida, selecione o tipo de impressora. Consulte a Seção 36.7 para mais detalhes.

**Important**

The networked IPP print server must allow connections from the local system. Refer to Seção 36.13 for more information.

## 36.3. Adding a Remote UNIX (LPD) Printer

To add a remote UNIX printer, such as one attached to a different Linux system on the same network, click the **New** button in the main **Ferramenta de Configuração da Impressora** window. The window shown in Figura 36-2 will appear. Click **Forward** to proceed.

Na janela exibida na Figura 36-3, indique um nome único para a impressora no campo **Nome**. O nome de uma impressora não pode conter espaços e deve começar por uma letra. Este nome pode conter letras, números, hífens (-) e underscores (_). Opcionalmente, indique uma breve descrição da impressora, que pode conter espaços.

Select **Networked UNIX (LPD)** from the **Select a queue type** menu, and click **Forward**.

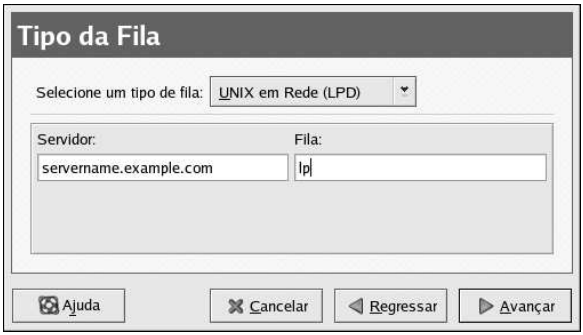


**Figura 36-6. Adding a Remote LPD Printer**

Text fields for the following options appear:

- **Server** — The hostname or IP address of the remote machine to which the printer is attached.
- **Queue** — The remote printer queue. The default printer queue is usually `lp`.

Click **Forward** to continue.

Em seguida, selecione o tipo de impressora. Consulte a Seção 36.7 para mais detalhes.

**Important**

The remote print server must accept print jobs from the local system.

## 36.4. Adding a Samba (SMB) Printer

To add a printer which is accessed using the SMB protocol (such as a printer attached to a Microsoft Windows system), click the **New** button in the main **Ferramenta de Configuração da Impressora** window. The window shown in Figura 36-2 will appear. Click **Forward** to proceed.

Na janela exibida na Figura 36-3, indique um nome único para a impressora no campo **Nome**. O nome de uma impressora não pode conter espaços e deve começar por uma letra. Este nome pode conter letras, números, hífens (-) e underscores (_). Opcionalmente, indique uma breve descrição da impressora, que pode conter espaços.

Select **Networked Windows (SMB)** from the **Select a queue type** menu, and click **Forward**. If the printer is attached to a Microsoft Windows system, choose this queue type.

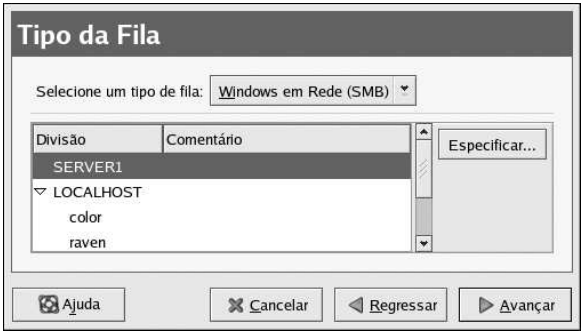


**Figura 36-7. Adding a SMB Printer**

As shown in Figura 36-7, SMB shares are automatically detected and listed. Click the arrow beside each share name to expand the list. From the expanded list, select a printer.

If the printer you are looking for does not appear in the list, click the **Specify** button on the right. Text fields for the following options appear:

- **Workgroup** — The name of the Samba workgroup for the shared printer.
- **Server** — The name of the server sharing the printer.
- **Share** — The name of the shared printer on which you want to print. This name must be the same name defined as the Samba printer on the remote Windows machine.
- **User name** — The name of the user you must log in as to access the printer. This user must exist on the Windows system, and the user must have permission to access the printer. The default user name is typically **`guest`** for Windows servers, or **`nobody`** for Samba servers.
- **Password** — The password (if required) for the user specified in the **User name** field.

Click **Forward** to continue. The **Ferramenta de Configuração da Impressora** then attempts to connect to the shared printer. If the shared printer requires a username and password, a dialog window appears prompting you to provide a valid username and password for the shared printer. If an incorrect share name is specified, you can change it here as well. If a workgroup name is required to connect to the share, it can be specified in this dialog box. This dialog window is the same as the one shown when the **Specify** button is clicked.

Em seguida, selecione o tipo de impressora. Consulte a Seção 36.7 para mais detalhes.

**Atenção**

Se você requer um nome de usuário e senha, estes são armazenados descriptogafados em arquivos que podem ser acessados somente por root e lpd. Sendo assim, é possível que outras pessoas saibam o nome e senha se tiverem acesso root. Para evitar isso, o nome de usuário e senha de acesso à impressora devem ser diferentes daqueles usados para a conta do usuário no sistema Red Hat Enterprise Linux local. Se forem diferentes, então o único comprometimento possível da segurança será o uso não-autorizado da impressora. Se há arquivos compartilhados pelo servidor, é recomendado que também utilizem uma senha diferente daquela usada na fila de impressão.

## 36.5. Adding a Novell NetWare (NCP) Printer

To add a Novell NetWare (NCP) printer, click the **New** button in the main **Ferramenta de Configuração da Impressora** window. The window shown in Figura 36-1 will appear. Click **Forward** to proceed.

Na janela exibida na Figura 36-3, indique um nome único para a impressora no campo **Nome**. O nome de uma impressora não pode conter espaços e deve começar por uma letra. Este nome pode conter letras, números, hífens (-) e underscores (_). Opcionalmente, indique uma breve descrição da impressora, que pode conter espaços.

Select **Networked Novell (NCP)** from the **Select a queue type** menu.

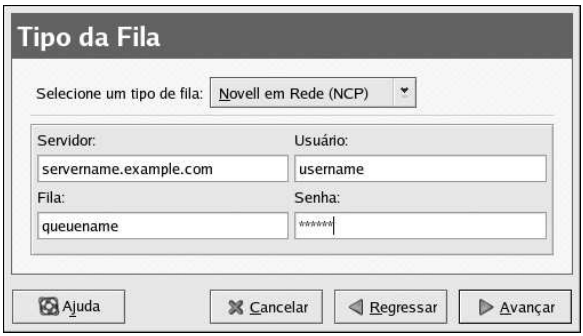


**Figura 36-8. Adding an NCP Printer**

Text fields for the following options appear:

- **Server** — The hostname or IP address of the NCP system to which the printer is attached.
- **Queue** — The remote queue for the printer on the NCP system.
- **User** — The name of the user you must log in as to access the printer.
- **Password** — The password for the user specified in the **User** field above.

Em seguida, selecione o tipo de impressora. Consulte a Seção 36.7 para mais detalhes.

**Atenção**

Se você requer um nome de usuário e senha, estes são armazenados descriptogafados em arquivos que podem ser acessados somente por root e lpd. Sendo assim, é possível que outras pessoas saibam o nome e senha se tiverem acesso root. Para evitar isso, o nome de usuário e senha de acesso à impressora devem ser diferentes daqueles usados para a conta do usuário no sistema Red Hat Enterprise Linux local. Se forem diferentes, então o único comprometimento possível da segurança será o uso não-autorizado da impressora. Se há arquivos compartilhados pelo servidor, é recomendado que também utilizem uma senha diferente daquela usada na fila de impressão.

## 36.6. Adding a JetDirect Printer

To add a JetDirect printer, click the **New** button in the main **Ferramenta de Configuração da Impressora** window. The window shown in Figura 36-1 will appear. Click **Forward** to proceed.

Na janela exibida na Figura 36-3, indique um nome único para a impressora no campo **Nome**. O nome de uma impressora não pode conter espaços e deve começar por uma letra. Este nome pode conter letras, números, hífens (-) e underscores (_). Opcionalmente, indique uma breve descrição da impressora, que pode conter espaços.

Select **Networked JetDirect** from the **Select a queue type** menu, and click **Forward**.


**Figura 36-9. Adding a JetDirect Printer**

Text fields for the following options appear:

- **Printer** — The hostname or IP address of the JetDirect printer.
- **Port** — The port on the JetDirect printer that is listening for print jobs. The default port is 9100.

Em seguida, selecione o tipo de impressora. Consulte a Seção 36.7 para mais detalhes.

## 36.7. Selecting the Printer Model and Finishing

After selecting the queue type of the printer, the next step is to select the printer model.

You will see a window similar to Figura 36-10. If it was not auto-detected, select the model from the list. The printers are divided by manufacturers. Select the name of the printer manufacturer from the pulldown menu. The printer models are updated each time a different manufacturer is selected. Select the printer model from the list.


**Figura 36-10. Selecting a Printer Model**

The recommended print driver is selected based on the printer model selected. The print driver processes the data that you want to print into a format the printer can understand. Since a local printer is attached directly to your computer, you need a print driver to process the data that is sent to the printer.

If you are configuring a remote printer (IPP, LPD, SMB, or NCP), the remote print server usually has its own print driver. If you select an additional print driver on your local computer, the data is filtered multiple times and is converted to a format that the printer can not understand.

To make sure the data is not filtered more than once, first try selecting **Generic** as the manufacturer and **Raw Print Queue** or **Postscript Printer** as the printer model. After applying the changes, print a test page to try out this new configuration. If the test fails, the remote print server might not have a print driver configured. Try selecting a print driver according to the manufacturer and model of the remote printer, applying the changes, and printing a test page.

**Tip**

You can select a different print driver after adding a printer by starting the **Ferramenta de Configuração da Impressora**, selecting the printer from the list, clicking **Edit**, clicking the **Driver** tab, selecting a different print driver, and then applying the changes.

### 36.7.1. Confirming Printer Configuration

The last step is to confirm your printer configuration. Click **Apply** to add the print queue if the settings are correct. Click **Back** to modify the printer configuration.

Click the **Apply** button in the main window to save your changes and restart the printer daemon. After applying the changes, print a test page to ensure the configuration is correct. Refer to Seção 36.8 for details.

If you need to print characters beyond the basic ASCII set (including those used for languages such as Japanese), you must review your driver options and select **Prerender Postscript**. Refer to Seção 36.9 for details. You can also configure options such as paper size if you edit the print queue after adding it.

## 36.8. Printing a Test Page

After you have configured your printer, you should print a test page to make sure the printer is functioning properly. To print a test page, select the printer that you want to try out from the printer list, then select the appropriate test page from the **Test** pulldown menu.

If you change the print driver or modify the driver options, you should print a test page to test the different configuration.

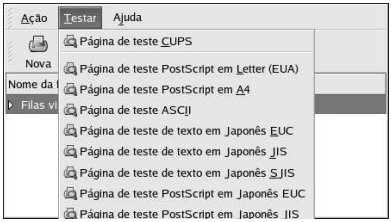


**Figura 36-11. Test Page Options**

## 36.9. Modifying Existing Printers

To delete an existing printer, select the printer and click the **Delete** button on the toolbar. The printer is removed from the printer list. Click **Apply** to save the changes and restart the printer daemon.

To set the default printer, select the printer from the printer list and click the **Default** button on the toolbar. The default printer icon ✔ appears in the **Default** column of the default printer in the list. A IPP browsed queue printer can not be set as the default printer in the **Ferramenta de Configuração da Impressora**. To make an IPP printer the default, either add it as described in Seção 36.2 and make it the default or use the **GNOME Print Manager** to set it as the default. To start the **GNOME Printer Manager**, select **Main Menu => System Tools => Print Manager**. Right-click on the queue name, and select **Set as Default**. Setting the default printer in the **GNOME Print Manager** only changes the default printer for the user who configures it; it is not a system-wide setting.

After adding the printer(s), the settings can be edited by selecting the printer from the printer list and clicking the **Edit** button. The tabbed window shown in Figura 36-12 is displayed. The window contains the current values for the selected printer. Make any necessary changes, and click **OK**. Click **Apply** in the main **Ferramenta de Configuração da Impressora** window to save the changes and restart the printer daemon.

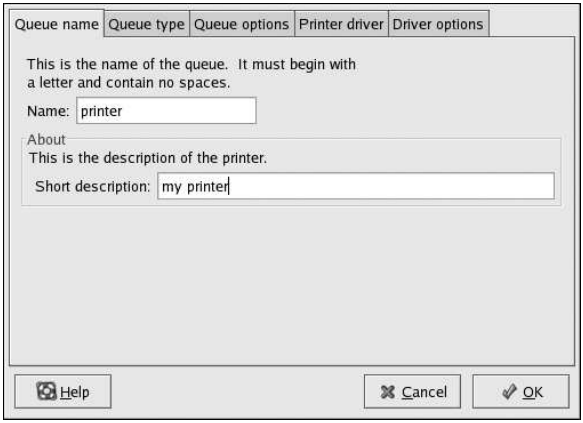


**Figura 36-12. Editing a Printer**

### 36.9.1. Queue Name

To rename a printer or change its short description, change the value in the **Queue name** tab. Click **OK** to return to the main window. The name of the printer should change in the printer list. Click **Apply** to save the change and restart the printer daemon.

### 36.9.2. Queue Type

The **Queue type** tab shows the queue type that was selected when adding the printer and its settings. The queue type of the printer can be changed or just the settings. After making modifications, click **OK** to return to the main window. Click **Apply** to save the changes and restart the printer daemon.

Depending on which queue type is chosen, different options are displayed. Refer to the appropriate section on adding a printer for a description of the options.

### 36.9.3. Printer Driver

The **Printer driver** tab shows which print driver is currently being used. If it is changed, click **OK** to return to the main window. Click **Apply** to save the change and restart the printer daemon.

### 36.9.4. Driver Options

The **Driver Options** tab displays advanced printer options. Options vary for each print driver. Common options include:

- **Prerender Postscript** should be selected if characters beyond the basic ASCII set are being sent to the printer but they are not printing correctly (such as Japanese characters). This option prerenders non-standard PostScript fonts so that they are printed correctly.

  If the printer does not support the fonts you are trying to print, try selecting this option. For example, select this option to print Japanese fonts to a non-Japanese printer.

  Extra time is required to perform this action. Do not choose it unless problems printing the correct fonts exist.

Also select this option if the printer can not handle PostScript level 3. This option converts it to PostScript level 1.

- **GhostScript pre-filtering** — allows you to select **No pre-filtering**, **Convert to PS level 1**, or **Convert to PS level 2** in case the printer can not handle certain PostScript levels. This option is only available if the PostScript driver is used.
- **Page Size** allows the paper size to be selected. The options include US Letter, US Legal, A3, and A4.
- **Effective Filter Locale** defaults to **C**. If Japanese characters are being printed, select **ja_JP**. Otherwise, accept the default of **C**.
- **Media Source** defaults to **Printer default**. Change this option to use paper from a different tray.

To modify the driver options, click **OK** to return to the main window. Click **Apply** to save the change and restart the printer daemon.

## 36.10. Saving the Configuration File

When the printer configuration is saved using the **Ferramenta de Configuração da Impressora**, the application creates its own configuration file that is used to create the files in the `/etc/cups` directory. You can use the command line options to save or restore the **Ferramenta de Configuração da Impressora** file. If the `/etc/cups/` directory is saved and restored to the same locations, the printer configuration is not restored because each time the printer daemon is restarted, it creates a new `/etc/printcap` file from the **Ferramenta de Configuração da Impressora** configuration file. When creating a backup of the system's configuration files, use the following method to save the printer configuration files.

To save your printer configuration, type this command as root:

```
/usr/sbin/redhat-config-printer-tui --Xexport > settings.xml
```

Your configuration is saved to the file `settings.xml`.

If this file is saved, it can be used to restore the printer settings. This is useful if the printer configuration is deleted, if Red Hat Enterprise Linux is reinstalled, or if the same printer configuration is needed on multiple systems. The file should be saved on a different system before reinstalling. To restore the configuration, type this command as root:

```
/usr/sbin/redhat-config-printer-tui --Ximport < settings.xml
```

If you already have a configuration file (you have configured one or more printers on the system already) and you try to import another configuration file, the existing configuration file will be overwritten. If you want to keep your existing configuration and add the configuration in the saved file, you can merge the files with the following command (as root):

```
/usr/sbin/redhat-config-printer-tui --Ximport --merge < settings.xml
```

Your printer list will then consist of the printers you configured on the system as well as the printers you imported from the saved configuration file. If the imported configuration file has a print queue with the same name as an existing print queue on the system, the print queue from the imported file will override the existing printer.

After importing the configuration file (with or without the `merge` command), you must restart the printer daemon. Issue the command:

```
/sbin/service cups restart
```

## 36.11. Command Line Configuration

If you do not have X installed and you do not want to use the text-based version, you can add a printer via the command line. This method is useful if you want to add a printer from a script or in the %post section of a kickstart installation.

### 36.11.1. Adding a Local Printer

To add a printer:

```
redhat-config-printer-tui --Xadd-local options
```

Options:

--device=*node*

(Required) The device node to use. For example, `/dev/lp0`.

--make=*make*

(Required) The IEEE 1284 MANUFACTURER string or the printer manufacturer's name as in the foomatic database if the manufacturer string is not available.

--model=*model*

(Required) The IEEE 1284 MODEL string or the printer model listed in the foomatic database if the model string is not available.

--name=*name*

(Optional) The name to be given to the new queue. If one is not given, a name based on the device node (such as "lp0") will be used.

--as-default

(Optional) Set this as the default queue.

After adding the printer, use the following command to start/restart the printer daemon:

```
service cups restart
```

### 36.11.2. Removing a Local Printer

A printer queue can also be removed via the command line.

As root, to remove a printer queue:

```
redhat-config-printer-tui --Xremove-local options
```

Options:

--device=*node*

(Required) The device node used such as `/dev/lp0`.

--make=*make*

(Required) The IEEE 1284 MANUFACTURER string, or (if none is available) the printer manufacturer's name as in the foomatic database.

--model=*model*

(Required) The IEEE 1284 MODEL string, or (if none is available) the printer model as listed in the foomatic database.

After removing the printer from the **Ferramenta de Configuração da Impressora** configuration, restart the printer daemon for the changes to take effect:

```
service cups restart
```

If all printers have been removed, and you do not want to run the printer daemon anymore, execute the following command:

```
service cups stop
```

### 36.11.3. Setting the Default Printer

To set the default printer, use the following command, and specify the *queuename*:

```
redhat-config-printer-tui --Xdefault --queue=queuename
```

## 36.12. Managing Print Jobs

When you send a print job to the printer daemon, such as printing text file from **Emacs** or printing an image from **The GIMP**, the print job is added to the print spool queue. The print spool queue is a list of print jobs that have been sent to the printer and information about each print request, such as the status of the request, the username of the person who sent the request, the hostname of the system that sent the request, the job number, and more.

If you are running a graphical desktop environment, click the **Printer Manager** icon on the panel to start the **GNOME Print Manager** as shown in Figura 36-13.

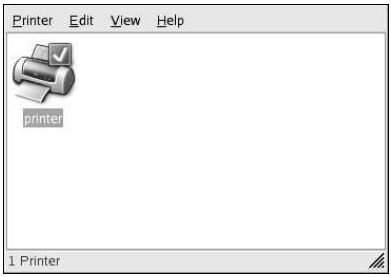


**Figura 36-13. GNOME Print Manager**

It can also be started by selecting **Main Menu Button** (on the Panel) => **System Tools** => **Print Manager**.

To change the printer settings, right-click on the icon for the printer and select **Properties**. The **Ferramenta de Configuração da Impressora** is then started.

Double-click on a configured printer to view the print spool queue as shown in Figura 36-14.

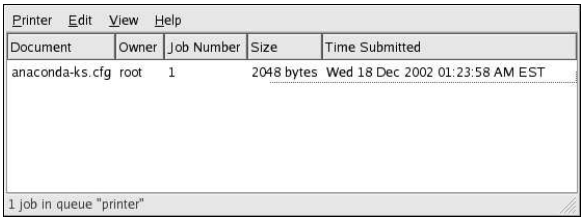


**Figura 36-14. List of Print Jobs**

To cancel a specific print job listed in the **GNOME Print Manager**, select it from the list and select **Edit => Cancel Documents** from the pulldown menu.

If there are active print jobs in the print spool, a printer notification icon might appears in the **Panel Notification Area** of the desktop panel as shown in Figura 36-15. Because it probes for active print jobs every five seconds, the icon might not be displayed for short print jobs.


**Figura 36-15. Printer Notification Icon**

Clicking on the printer notification icon starts the **GNOME Print Manager** to display a list of current print jobs.

Also located on the Panel is a **Print Manager** icon. To print a file from **Nautilus**, browse to the location of the file and drag and drop it on to the **Print Manager** icon on the Panel. The window shown in Figura 36-16 is displayed. Click **OK** to start printing the file.

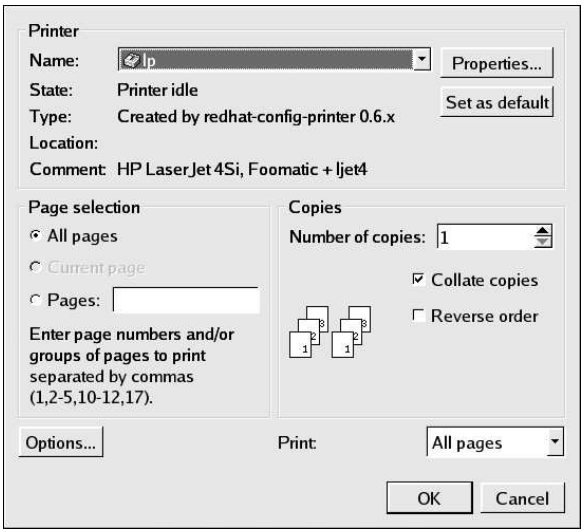


**Figura 36-16. Print Verification Window**

To view the list of print jobs in the print spool from a shell prompt, type the command `lpq`. The last few lines will look similar to the following:

```
Rank    Owner/ID            Class  Job Files       Size Time
active user@localhost+902     A    902 sample.txt  2050 01:20:46
```

**Exemplo 36-1. Example of `lpq` output**

If you want to cancel a print job, find the job number of the request with the command `lpq` and then use the command `lprm` *`job number`*. For example, `lprm 902` would cancel the print job in Exemplo 36-1. You must have proper permissions to cancel a print job. You can not cancel print jobs that were started by other users unless you are logged in as root on the machine to which the printer is attached.

You can also print a file directly from a shell prompt. For example, the command `lpr sample.txt` will print the text file `sample.txt`. The print filter determines what type of file it is and converts it into a format the printer can understand.

## 36.13. Sharing a Printer

The **Ferramenta de Configuração da Impressora**'s ability to share configuration options can only be used if you are using the CUPS printing system.

Allowing users on a different computer on the network to print to a printer configured for your system is called *sharing* the printer. By default, printers configured with the **Ferramenta de Configuração da Impressora** are not shared.

To share a configured printer, start the **Ferramenta de Configuração da Impressora** and select a printer from the list. Then select **Action => Sharing** from the pulldown menu.

**Note**

If a printer is not selected, **Action** => **Sharing** only shows the system-wide sharing options normally shown under the **General** tab.

On the **Queue** tab, select the option to make the queue available to other users.

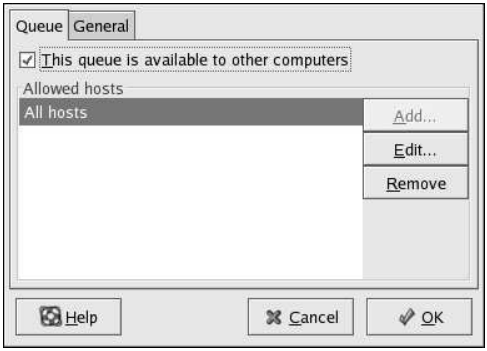


**Figura 36-17. Queue Options**

After selecting to share the queue, by default, *all* hosts are allowed to print to the shared printer. Allowing all systems on the network to print to the queue can be dangerous, especially if the system is directly connected to the Internet. It is recommended that this option be changed by selecting the **All hosts** entry and clicking the **Edit** button to display the window shown in Figura 36-18.

If you have a firewall configured on the print server, it must be able to send and receive connections on the incoming UDP port, 631. If you have a firewall configured on the client (the computer sending the print request), it must be allowed to send and accept connections on port 631.

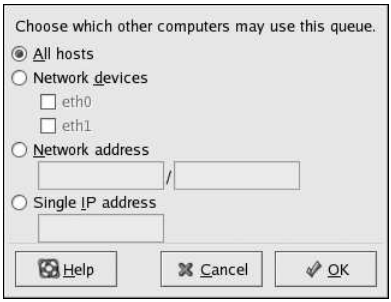


**Figura 36-18. Allowed Hosts**

The **General** tab configures settings for all printers, including those not viewable with the **Ferramenta de Configuração da Impressora**. There are two options:

- **Automatically find remote shared queues** — Selected by default, this option enables IPP browsing, which means that when other machines on the network broadcast the queues that they have, the queues are automatically added to the list of printers available to the system; no additional configuration is required for a printer found from IPP browsing. This option does not automatically share the printers configured on the local system.
- **Enable LPD protocol** — This option allows the printer to receive print jobs from clients configured to use the LPD protocol using the `cups-lpd` service, which is an `xinetd` service.

**Warning**

If this option is enabled, all print jobs are accepted from all hosts if they are received from an LPD client.

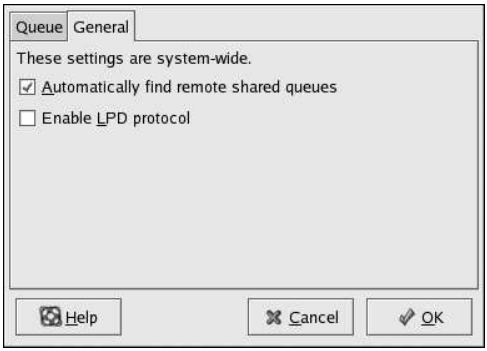


**Figura 36-19. System-wide Sharing Options**

## 36.14. Additional Resources

To learn more about printing on Red Hat Enterprise Linux, refer to the following resources.

### 36.14.1. Installed Documentation

- `map lpr` — The manual page for the `lpr` command that allows you to print files from the command line.
- `man lprm` — The manual page for the command line utility to remove print jobs from the print queue.
- `man mpage` — The manual page for the command line utility to print multiple pages on one sheet of paper.
- `man cupsd` — The manual page for the CUPS printer daemon.
- `man cupsd.conf` — The manual page for the CUPS printer daemon configuration file.
- `man classes.conf` — The manual page for the class configuration file for CUPS.

### 36.14.2. Useful Websites

- http://www.linuxprinting.org — *GNU/Linux Printing* contains a large amount of information about printing in Linux.
- http://www.cups.org/ — Documentation, FAQs, and newsgroups about CUPS.

redhat.

Capítulo 37.

# Tarefas Automatizadas

No Linux, as tarefas podem ser configuradas para serem executadas automaticamente dentro de um determinado período de tempo, em uma data específica ou quando a média de carga do sistema estiver abaixo de um número especificado. O Red Hat Enterprise Linux vem pré-configurado para executar tarefas importantes do sistema a fim de mantê-lo atualizado. Por exemplo: o banco de dados slocate usado pelo comando `locate` é atualizado diariamente. Um administrador de sistemas pode usar tarefas automatizadas para executar backups periódicos, monitorar o sistema e rodar scipts personalizados, dentre outras tarefas.

O Red Hat Enterprise Linux vem com diversos utilitários de tarefas automatizados: `cron`, `at` e `batch`.

## 37.1. Cron

O Cron é um daemon que pode ser utilizado para agendar a execução de tarefas recorrentes de acordo com uma combinação de hora, dia do mês, mês, dia da semana e semana.

O cron assume que o sistema está continuamante ligado. Se o sistema não estiver ligado no momento para o qual a tarefa foi agendada, esta não será executada. Para agendar tarefas de uma ocorrência, consulte a Seção 37.2.

Para usar o serviço cron, é necessário instalar o pacote RPM `vixie-cron` e o serviço `crond` deve estar rodando. Para determinar se o pacote está instalado, use o comando `rpm -q vixie-cron`. Para determinar se o serviço está rodando, use o `/sbin/service crond status`.

### 37.1.1. Configurando Tarefas no Cron

O principal arquivo de configuração do cron, `/etc/crontab`, contém as seguintes linhas:

```
SHELL=/bin/bash
PATH=/sbin:/bin:/usr/sbin:/usr/bin
MAILTO=root
HOME=/

# run-parts
01 * * * * root run-parts /etc/cron.hourly
02 4 * * * root run-parts /etc/cron.daily
22 4 * * 0 root run-parts /etc/cron.weekly
42 4 1 * * root run-parts /etc/cron.monthly
```

As primeiras quatro linhas são variáveis utilizadas para configurar o ambiente no qual as atividades do cron são executadas. O valor da variável `SHELL` diz ao sistema qual ambiente shell deve usar (neste exemplo, a shell bash), e a variável `PATH` define a localidade usada para executar comandos. O output das tarefas do cron é enviado por e-mail ao nome do usuário definido na variável `MAILTO`. Se a variável `MAILTO` for definida com um campo vazio (`MAILTO=""`), o e-mail não será enviado. A variável `HOME` pode ser usada para definir o diretório raíz a ser usado ao executar comandos ou scripts.

Cada linha do arquivo `/etc/crontab` representa uma tarefa e tem o formato:

```
minute   hour   day   month   dayofweek   command
```

- `minute` — qualquer número inteiro de 0 a 59

- `hour` — qualquer número inteiro de 0 a 23
- `day` — qualquer número inteiro de 1 a 31 (deve ser um dia válido se o mês for especificado)
- `month` — qualquer número inteiro de 1 a 12 (ou a abreviação do mês em inglês, como jan ou feb)
- `dayofweek` — qualquer número inteiro de 0 a 7, onde 0 ou 7 representa o Domingo (ou a abreviação do dia da semana em inglês, como sun ou mon)
- `command` — o comando a executar (pode ser um comando como `ls /proc >> /tmp/proc` ou o comando para executar um script personalizado)

Para qualquer um dos valores acima, pode ser usado um asterisco (*) para especificar todos os valores válidos. Por exemplo: um asterisco no valor mês significa que o comando deve ser executado todo mês segundo as restrições dos outros valores.

Um hífen (-) entre números inteiros especifica um intervalo de números inteiros. Por exemplo: **`1-4`** significa os números inteiros 1, 2, 3 e 4.

Uma lista de valores separados por vírgulas (,) especifica uma lista. Por exemplo: **`3, 4, 6, 8`** indica estes quatro números inteiros específicos.

A barra (/) pode ser usada para especificar valores fásicos. O valor de um número inteiro pode ser pulado dentro de um período, inserindo **`/`**<***`inteiro`***> após o intervalo. Por exemplo: **`0-59/2`** pode ser usado para definir todo o segundo minuto no campo dos minutos. Valores fásicos também podem ser usados com um asterisco. Por exemplo: o valor **`*/3`** pode ser usado no campo do mês para executar a tarefa a cada três meses.

Quaisquer linhas que iniciem com o jogo da velha (#) são comentários e não são processados.

Conforme mostrado no arquivo `/etc/crontab`, o cron usa o script `run-parts` para executar os scripts nos diretórios `/etc/cron.hourly`, `/etc/cron.daily`, `/etc/cron.weekly` e `/etc/cron.monthly` com uma frequência horária, diária, semanal ou mensal, respectivamente. Os arquivos destes diretórios devem ser scripts de linha de comando (shell).

Se uma tarefa cron precisa ser executada com uma frequência que não seja horária, diária, semanal ou mensal, ela pode ser adicionada ao diretório `/etc/cron.d`. Todos os arquivos deste diretório usam a mesma sintaxe que o `/etc/crontab`. Consulte o Exemplo 37-1 para ver exemplos.

```
# record the memory usage of the system every monday
# at 3:30AM in the file /tmp/meminfo
30 3 * * mon cat /proc/meminfo >> /tmp/meminfo
# run custom script the first day of every month at 4:10AM
10 4 1 * * /root/scripts/backup.sh
```

**Exemplo 37-1. Exemplos de crontab**

Usuários além do root podem configurar tarefas no cron usando a funcionalidade `crontab`. Todos os crontabs definidos pelo usuário são armazenados no diretório `/var/spool/cron` e executados usando o nome do usuário que os criou. Para criar um crontab como um determinado usuário, logue-se como este usuário e digite o comando `crontab -e` para editar o crontab do usuário usando o editor especificado pelas variáveis de ambiente `VISUAL` ou `EDITOR`. O arquivo usa o mesmo formato do `/etc/crontab`. Ao salvar as alterações do crontab, este é armazenado de acordo com o nome do usuário e gravada no arquivo `/var/spool/cron/`*`nome_do_usuário`*.

O daemon do cron checa quaisquer alterações no arquivo `/etc/crontab`, no diretório `/etc/cron.d/` e no diretório `/var/spool/cron` a cada minuto. Se qualquer alteração for encontrada, esta será carregada para a memória. Portanto, o daemon não precisa ser reiniciado se um arquivo crontab for alterado.

### 37.1.2. Controlando Acesso ao Cron

Os arquivos `/etc/cron.allow` e `/etc/cron.deny` são usados para restringir acesso ao cron. O formato de ambos arquivos de controle de acesso consiste em um nome de usuário por linha. Espaços em branco não são permitidos em nenhum destes arquivos. O daemon do cron (`crond`) não precisa ser reiniciado se os arquivos de controle de acesso forem modificados. Os arquivos de controle de acesso são lidos a cada vez que o usuário tentar adicionar ou apagar uma tarefa do cron.

O usuário root pode usar o cron sempre, independentemente dos nomes de usuário listados nos arquivos de controle de acesso.

Se o arquivo `cron.allow` existe, somente os usuários listados neste poderão usar o cron, e então o arquivo `cron.deny` será ignorado.

Se o arquivo `cron.allow` não existe, os usuários listados no `cron.deny` não poderão usar o cron.

### 37.1.3. Iniciando e Parando o Serviço

Para iniciar o serviço cron, use o comando `/sbin/service crond start`. Para parar o serviço, use o comando `/sbin/service crond stop`. É recomendado iniciar o serviço no momento da inicialização da máquina (boot time). Consulte o Capítulo 21 para obter detalhes sobre o início automático do serviço cron na hora da inicialização.

## 37.2. At e Batch

Enquanto o cron é usado para agendar tarefas recorrentes, o comando `at` é usado para agendar tarefas únicas em uma hora específica. O comando `batch` é usado para agendar uma tarefa única a ser executada quando a média de carga dos sistemas cai abaixo de 0,8.

Para usar o `at` ou o `batch`, o pacote RPM `at` deve ser instalado e o serviço `atd` deve estar rodando. Para verificar se o pacote está instalado, use o comando `rpm -q at`. Para verificar se o serviço está rodando, use o comando `/sbin/service atd status`.

### 37.2.1. Configurando Trabalhos com At

Para agendar um trabalho único em uma hora específica, digite o comando `at` *`hora`*, onde *`hora`* é a hora para executar o comando.

O argumento *`hora`* pode ser um dos seguintes:

- Formato HH:MM — Por exemplo: 04:00 especifica 4:00AM. Se a hora já passou, será executado na hora especificada no dia seguinte.
- midnight — Especifica 12:00AM.
- noon — Especifica 12:00PM.
- teatime — Especifica 4:00PM.
- Formato nome-do-mês dia ano — Por exemplo: January 15 2004 especifica o 15o dia de Janeiro no ano 2004. O ano é opcional.
- Formatos MMDDYY, MM/DD/YY, ou MM.DD.YY — Por exemplo: 011504 para o 15o dia de Janeiro no ano 2004.
- now + time — hora em minutos, horas, dias ou semanas. Por exemplo: 'now + 5 days' especifica que o comando deve ser executado na mesma hora daqui cinco dias.

A hora deve ser especificada primeiro, seguida da data opcional. Para mais informações sobre o formato hora, leia o arquivo texto `/usr/share/doc/at-`*`<version>`*`/timespec`.

Após digitar o comando `at` com o argumento da hora, será exibida uma janela de comandos `at>`. Digite o comando a ser executado, pressione [Enter] e pressione Ctrl-D. Mais de um comando pode ser especificado digitando cada comando seguido da tecla [Enter]. Após digitar todos os comandos, pressione [Enter] para ir para uma linha em branco e pressione Ctrl-D. Alternativamente, um script shell pode ser inserido na janela de comandos, pressionando [Enter] após cada linha do script e pressionando Ctrl-D em uma linha em branco para sair. Se um script for inserido, a shell usada é aquela definida no ambiente SHELL do usuário, ou a shell de login do usuário ou `/bin/sh` (a que for encontrada primeiro).

Se o conjunto de comandos ou script tentar exibir informações para a saída default (satandard out), o output é enviado por e-mail ao usuário.

Use o comando `atq` para visualizar trabalhos pendentes. Consulte a Seção 37.2.3 para mais informações.

O uso do comando `at` pode ser restrito. Consulte a Seção 37.2.5 para ver detalhes.

### 37.2.2. Configurando Trabalhos com o Batch

Para executar uma tarefa única quando a média de carga estiver abaixo de 0,8, use o comando `batch`.

Após digitar o comando `batch`, será exibida uma janela de comandos `at>`. Digite o comando a executar, pressione [Enter] e então Ctrl-D. Mais de um comando pode ser especificado digitando cada um deles seguido da tecla [Enter]. Após digitar todos os comandos, pressione [Enter] para ir para uma linha em branco e então pressione Ctrl-D. Alternativamente, um script shell pode ser inserido na janela de comandos, pressionando [Enter] após cada linha do script e pressionando Ctrl-D em uma linha em branco para sair. Se um script for inserido, a shell usada é aquela definida no ambiente SHELL do usuário, ou a shell de login do usuário ou `/bin/sh` (a que for encontrada primeiro). Assim que a média de carga estiver abaixo de 0,8, o conjunto de comandos ou script será executado.

Se o conjunto de comandos ou script tentar exibir informações para a saída default (satandard out), o output é enviado por e-mail ao usuário.

Use o comando `atq` para visualizar trabalhos pendentes. Consulte a Seção 37.2.3 para mais informações.

O uso do comando `batch` pode ser restrito. Consulte a Seção 37.2.5 para detalhes.

### 37.2.3. Visualizando Trabalhos Pendentes

Para visualizar os trabalhos pendentes do `at` e do `batch`, use o comando `atq`. Este exibe uma lista dos trabalhos pendentes; cada trabalho em uma linha. Cada linha segue o formato número do trabalho, data, hora, classe do trabalho e nome do usuário. Os usuários podem visualizar apenas seus próprios trabalhos. Se o usuário root executar o comando `atq`, serão exibidos todos os trabalhos de todos os usuários.

### 37.2.4. Opções Adicionais de Linha de Comando

Opções adicionais de linha de comando para o `at` e `batch` incluem:

| Opção | Descrição |
|---|---|
| `-f` | Lê os comandos ou script a partir de um arquivo ao invés de especificá-los na janela de comandos. |
| `-m` | Envia e-mail ao usuário quando o trabalho estiver completo. |

| Opção | Descrição |
|---|---|
| `-v` | Exibe a hora em que o trabalho será executado. |

**Tabela 37-1. Opções de Linha de Comando para `at` e `batch`**

### 37.2.5. Controlando o Acesso a At e Batch

Os arquivos `/etc/at.allow` e `/etc/at.deny` podem ser usados para restringir o acesso aos comandos `at` e `batch`. O formato de ambos arquivos de controle de acesso consiste em um nome de usuário em cada linha. Espaços em branco não são permitidos em nenhum destes arquivos. O daemon do `at` (o `atd`) não precisa ser reiniciado se os arquivos de controle de acesso forem modificados. Os arquivos de controle de acesso são lidos cada vez que o usuário tentar executar os comandos `at` ou `batch`.

O usuário root sempre pode executar os comandos `at` e `batch`, independentemente dos arquivos de controle de acesso.

Se o arquivo `at.allow` existir, somente os usuários listados neste poderão usar `at` ou `batch`, e o arquivo `at.deny` será ignorado.

Se `at.allow` não existir, os usuários listados em `at.deny` não poderão usar `at` ou `batch`.

### 37.2.6. Iniciando e Parando o Serviço

Para iniciar o serviço `at`, use o comando `/sbin/service atd start`. Para parar o serviço, use o comando `/sbin/service atd stop`. É recomendado inciar o serviço no momento da inicialização da máquina (boot time). Consulte o Capítulo 21 para obter detalhes sobre o início automático do serviço cron na hora da inicialização.

## 37.3. Recursos Adicionais

Para aprender mais sobre a configuração de tarefas automatizadas, consulte os seguintes recursos.

### 37.3.1. Documentação Instalada

- Página man do `cron` — visão geral do cron.
- Páginas man do `crontab` nas seções 1 e 5 — A página man na seção 1 contém uma visão geral do arquivo `crontab`. A página man da seção 5 contém o formato do arquivo e alguns exemplos de entradas.
- `/usr/share/doc/at-<version>/timespec` contém informações mais detalhadas sobre os horários que podem ser especificados para trabalhos do cron.
- Página man do `at` — descrição do `at` e `batch` e suas opções de linha de comando.

# Capítulo 38.
# Arquivos de Registro

*Arquivos de registro* são arquivos que contêm mensagens sobre o sistema, incluindo o kernel, os serviços e as aplicações rodando nele. Há arquivos de registro diferentes para informações diferentes. Por exemplo: há um arquivo de registro default do sistema, um arquivo de registro para mensagens de segurança e um outro para tarefas do cron.

Arquivos de registro podem ser muito úteis ao tentar solucionar um problema no sistema, como o carregamento de um driver do kernel ou ao procurar por tentativas de autenticação não-autorizadas no sistema. Este capítulo aponta onde encontrar os arquivos de registro, como visualizá-los e o que procurar nestes arquivos.

Alguns arquivos de registro são controlados por um daemon chamado `syslogd`. Uma lista das mensagens de registro mantidas pelo `syslogd` pode ser encontrada no arquivo de configuração `/etc/syslog.conf`.

## 38.1. Localizando Arquivos de Registro

A maioria dos arquivos de registro são localizados no diretório `/var/log/`. Algumas aplicações como `httpd` e `samba` têm um diretório dentro de `/var/log/` para seus arquivos de registro.

Note os diversos arquiivos no diretório de arquivos de registros com números após seus nomes. Estes são criados quando os arquivos de registro são rotacionados. Os arquivos são rotacionados para que não fiquem muito grandes. O pacote `logrotate` contém uma tarefa cron que rotaciona automaticamente os arquivos de registro de acordo com o arquivo de configuração `/etc/logrotate.conf` e com os arquivos de configuração no diretório `/etc/logrotate.d/`. Por default, são configurados para rotacionar toda semana, e manter quatro semanas de registro dos arquivos anteriores.

## 38.2. Visualizando Arquivos de Registro

A maioria dos arquivos de registro tem formato somente texto. Você pode visualizá-los com qualquer editor de texto, como `Vi` ou **Emacs**. Alguns arquivos de registro são legíveis por todos os usuários do sistema; entretanto, são necessários privilégios root para ler a maioria deles.

Para visualizar arquivos de registro através de uma aplicação interativa, e em tempo real, use a **Visualizador de Registro**. Para iniciar a aplicação, vá para **botão do Menu Principal** (no Painel) => **Ferramentas do Sistema** => **Registros do Sistema**, ou digite o comando `redhat-logviewer` em uma janela de comandos.

A aplicação exibe somente os arquivos de registro que existem; portanto, a lista pode diferir daquela exibida em Figura 38-1.

Para filtrar o conteúdo do arquivo de registro por palavras-chave, digite uma ou mais no campo de texto **Filtrar por**, e então clique em **Filtrar**. Clique em **Restaurar** para restaurar os conteúdos.

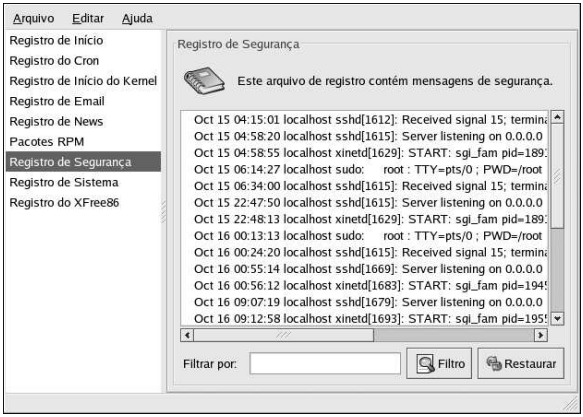


**Figura 38-1. Visualizador de Registro**

Por default, o arquivo de registro atualmente visível é atualizado a cada 30 segundos. Para alterar a taxa de atualização, selecione **Editar => Preferências** no menu suspenso. Aparece a janela exibida na Figura 38-2. Na aba **Arquivos de Registro**, clique nas setas para cima e para baixo ao lado da taxa de atualização para alterá-la. Clique em **Fechar** para retornar à janela principal. A taxa de atualização é alterada imediatamente. Para atualizar manualmente o arquivo sendo visualizado no momento, selecione **Arquivo => Atualizar Agora** ou pressione [Ctrl]-[R].

Na aba **Arquivos de Registro** em Preferências, é possível modificar as localizações dos arquivos de registro. Selecione o arquivo de registro da lista e clique no botão **Editar**. Digite a nova localização ou clique no botão **Navegar** para alocar o arquivo usando um diálogo de seleção de arquivos. Clique em **OK** para retornar às preferências, e então clique em **Fechar** para retornar à janela principal.

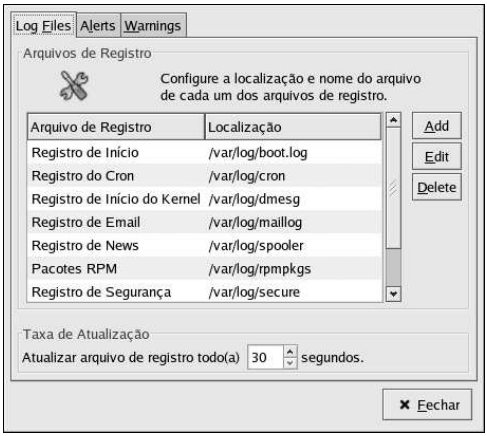


**Figura 38-2. Localizações dos Arquivos de Registro**

## 38.3. Adicionando um Arquivo de Registro

Para adicionar um arquivo de registro à lista, selecione **Editar => Preferências** e clique no botão **Adicionar** na aba **Arquivos de Registro**.

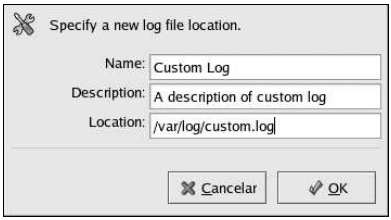


**Figura 38-3. Adicionando um Arquivo de Registro**

Dê um nome, uma descrição e a localização do arquivo a adicionar. Após clicar em **OK**, o arquivo é adicionado imediatamente à área de visualização (caso exista).

## 38.4. Examinando Arquivos de Registro

A **Visualizador de Registro** pode ser configurada para exibir um ícone de alerta ao lado das linhas que contêm palavras-chave de alerta, e um ícone de aviso ao lado das linhas com palavras-chave de aviso.

Para adicionar palavras de alerta, selecione **Editar => Preferências** no menu suspenso e então clique na aba **Alertas**. Clique no botão **Adicionar** para incluir uma palavra de alerta. Para apagar uma palavra de alerta, selecione-a da lista e clique em **Apagar**.

O ícone de alerta  é exibido à esquerda das linhas que contêm quaisquer palavras de alerta.

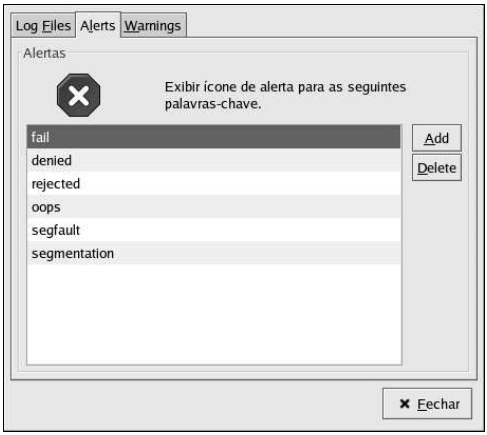


**Figura 38-4. Alertas**

Para adicionar palavras de aviso, selecione **Editar => Preferências** no menu suspenso e clique na aba **Avisos**. Clique no botão **Adicionar** para incluir uma palavra de aviso. Para apagar uma palavra de aviso, selecione-a da lista e então clique em **Apagar**.

O ícone de aviso  é exibido à esquerda das linhas que contêm quaisquer palavras de aviso.


**Figura 38-5. Aviso**

redhat.

Capítulo 39.

# Atualizando (upgrade) o kernel

O kernel do Red Hat Enterprise Linux é especialmente desenvolvido pela equipe do kernel da Red Hat para garantir sua integridade e compatibilidade aos componentes de hardware suportados. Antes da Red Hat lançar um kernel, este passa primeiro por uma série de testes de qualidade rigorosos.

Os kernels do Red Hat Enterprise Linux são empacotados no formato RPM para que sejam fáceis de atualizar e verificar. Por exemplo: quando o pacote RPM `kernel`, distribuído pela Red Hat, Inc., é instalado, uma imagem `initrd` é criada. Consequentemente, não é necessário usar o comando `mkinitrd` após instalar um kernel diferente. Também modifica o arquivo de configuração do gestor de início para incluir o novo kernel.

**Atenção**

O desenvolvimento de um kernel personalizado não é suportado pela Equipe de Suporte à Instalação da Red Hat. Para mais informações sobre o desenvolvimento de um kernel personalizado a partir do código fonte, conslute o Apêndice A.

## 39.1. Visão Geral dos Pacotes do Kernel

O Red Hat Enterprise Linux contém os seguintes pacotes do kernel (alguns talvez não se apliquem à arquitetura de sua máquina):

- `kernel` — contém o kernel e as seguintes funcionalidades-chave:
  - Suporte ao monoprocessador para sistemas x86 e Athlon (pode rodar em um sistema multi-processador, mas apenas um processdor é utilizado)
  - Suporte multi-processador para todas as outras arquiteturas
  - Em sistemas x86, somente os primeiros 4 GB de RAM são usados; use o pacote `kernel-hugemem` para sistemas x86 com mais de 4 GB de RAM.

- `kernel-hugemem` — (somente para sistemas i686) Além das opções habilitadas para o pacote `kernel`. As principais opções de configuração são:
  - Suporte para mais de 4 GB de RAM (até 16 GB para sistemas x86)
  - Extensão de Endereço Físico (PAE - Physical Address Extension), ou paging de 3 níveis em processadores x86 que suportam PAE
  - Suporte para processadores múltiplos
  - 4GB/4GB dividido — 4GB de espaço para o endereço virtual do kernel e quase 4GB para cada processo de usuário em sistemas x86

- `kernel-BOOT` — usado somente durante a instalação.
- `kernel-pcmcia-cs` — contém suporte para placas PCMCIA.
- `kernel-smp` — contém o kernel para sistemas com multi-processadores. Veja a seguir as principais características:

- Suporte a multi-processadores
- Suporte para mais de 4 GB de RAM (até 64 GB para sistemas x86)
- Extensão de Endereço Físico (PAE - Physical Address Extension), ou paging de 3 níveis em processadores x86 que suportam PAE

- `kernel-source` — Contém os arquivos do código-fonte para o kernel do Linux
- `kernel-utils` — Contém utilitários que podem ser usados para controlar o kernel ou hardware do sistema.
- `kernel-unsupported` — existe am algumas arquiteturas

  Como não é possível o Red Hat Enterprise Linux conter suporte para todos os componentes de hardware existentes, este pacote contém módulos que não são suportados pela Red Hat, Inc. durante ou depois da instalação. O pacote não é instalado durante o processo de instalação; mas deve ser instalado após a instalação. Os drivers do pacote não-suportado são providos através de nossos melhores esforços — atualizações e consertos podem ou não ser incorporados ao longo do tempo.

## 39.2. Preparando para o Upgrade

Antes de atualizar (upgrade) o kernel, tome algumas precauções. Se o sistema tiver um drive de disquete, o primeiro passo é garantir que você tenha um disquete boot funcionando no caso de algum problema. Se o gestor de início não está configurado corretamente para iniciar o novo kernel, o sistema não pode ser inicializado no Red Hat Enterprise Linux sem um disquete boot operante.

Para criar o disquete boot, autentique-se como root e digite o seguinte em uma janela de comandos:

```
/sbin/mkbootdisk `uname -r`
```

**Dica**

Consulte a página man do `mkbootdisk` para mais opções.

Reinicialize a máquina com o disquete boot e verifique se este funciona antes de continuar.

Provavelmente, o disquete não será necessário, mas guarde-o em um lugar seguro por precaução.

Para determinar quais pacotes do kernel são instalados, execute o seguinte comando em uma janela de comandos:

```
rpm -qa | grep kernel
```

O output contém alguns dos ou todos os pacotes a seguir, dependendo da arquitetura do sistema (os números da versão e pacotes podem ser diferentes):

```
kernel-2.4.21-1.1931.2.399.ent
kernel-source-2.4.21-1.1931.2.399.ent
kernel-utils-2.4.21-1.1931.2.399.ent
kernel-pcmcia-cs-3.1.31-13
kernel-smp-2.4.21-1.1931.2.399.ent
```

A partir do output, determine quais pacotes precisam ser baixados (download) para a atualização do kernel. Para sistemas com apenas um processador, o único pacote necessário é o `kernel`. Consulte a Seção 39.1 para obter descrições dos diversos pacotes.

No nome do arquivo, cada pacote do kernel contém a arquitetura para a qual o pacote foi criado. O formato é kernel-<*variante*>-<*versão*>.<*arquitetura*>.rpm, onde a <*variante*> é `smp`, `utils`, etc. A <*arquitetura*> é uma das seguintes:

1. `x86_64` para a arquitetura AMD64.
2. `ia64` para a arquitetura Intel® Itanium™.
3. `ppc64pseries` para a arquitetura IBM® eServer™ pSeries™.
4. `ppc64iseries` para a arquitetura IBM® eServer™ iSeries™.
5. `s390` para a arquitetura IBM® S/390®.
6. `s390x` para a arquitetura IBM® eServer™ zSeries®.
7. Variante da x86: Os kernels da x86 são otimizados para versões diferentes da x86. As opções são as seguintes:
   - `athlon` para sistemas AMD Athlon® e AMD Duron®
   - `i686` para sistemas Intel® Pentium® II, Intel® Pentium® III e Intel® Pentium® 4

## 39.3. Baixando (download) o Kernel Atualizado

Há diversas maneiras de determinar se há um kernel atualizado disponível para o sistema.

- Errata de Segurança. Veja a localidade seguinte para informações sobre erratas de segurança, incluindo atualizações do kernel que consertam questões de segurança.
  `http://www.redhat.com/apps/support/errata/`
- Através de Atualizações Quadrimestrais. Consulte a localidade seguinte para mais detalhes:
  `http://www.redhat.com/apps/support/errata/rhlas_errata_policy.html`
- Use a Red Hat Network para baixar e instalar os pacotes RPM do kernel. A Red Hat Network pode baixar o kernel mais atualizado, atualizar o kernel no sistema, criar uma imagem de disco RAM inicial se necessário e configurar o gestor de início para inicializar o kernel novo. Para mais informações, consulte http://www.redhat.com/docs/manuals/RHNetwork/.

Se a Red Hat Network for usada para baixar e instalar o kernel atualizado, siga as instruções da Seção 39.5 e da Seção 39.6, mas não especifique que o kernel seja inicializado por default, porque a Red Hat Network altera automaticamente o kernel default para a última versão. Para instalar o kernel manualmente, vá para a Seção 39.4.

## 39.4. Executando a Atualização

Após recuperar todos os pacotes necessários, é hora de atualizar o kernel existente. Em uma janela de comandos, como root, vá para o diretório que contém os pacotes RPM do kernel e siga estes passos.

**Importante**

É altamente recomendado que o kernel antigo seja guardado, caso ocorra probelmas com o novo.

Use o argumento `-i` com o comando `rpm` para guardar o kernel antigo. Se a opção `-U` for usada para atualizar o pacote do `kernel`, sobrescreverá o kernel atualmente instalado. (a versão do kernel pode variar):

```
rpm -ivh kernel-2.4.21-1.1931.2.399.ent.<arch>.rpm
```

Se o sistema tem multi-processadores, instale também os pacotes `kernel-smp` (a versão do kernel pode variar):

```
rpm -ivh kernel-smp-2.4.21-1.1931.2.399.ent.<arch>.rpm
```

Se o sistema é baseado na `i686` e contém mais de 4 gigabytes de RAM, instale o pacote `kernel-hugemem`, também criado para a arquitetura `i686` (a versão do kernel pode variar):

```
rpm -ivh kernel-hugemem-2.4.21-1.1931.2.399.ent.i686.rpm
```

Se os pacotes `kernel-source` ou `kernel-utils` devem ser atualizados, as versões antigas provavelmente não são necessárias. Use os seguintes comandos para atualizar estes pacotes (as versões podem variar):

```
rpm -Uvh kernel-source-2.4.21-1.1931.2.399.ent.<arch>.rpm
rpm -Uvh kernel-utils-2.4.21-1.1931.2.399.ent.<arch>.rpm
```

O próximo passo é verificar se a imagem de disco RAM inicial foi criada. Consulte a Seção 39.5 para mais detalhes.

## 39.5. Verificando a Imagem de Disco RAM Inicial

Se o sistema usa o sistema de arquivo ext3, um controlador SCSI ou se usa etiquetas para referenciar partições no `/etc/fstab`, é necessário um disco RAM inicial. O disco RAM inicial permite que um kernel modular tenha acesso aos módulos dos quais pode precisar para ser inicializado, antes que o kernel tenha acesso ao dispositivo onde os módulos normalmente residem.

Nas arquiteturas Red Hat Enterprise Linux, além da IBM eServer iSeres, o disco RAM inicial pode ser criado com o comando `mkinitrd`. No entanto, este passo é executado automaticamente se o kernel e seus pacotes associados são instalados ou atualizados através dos pacotes RPM distribuídos pela Red Hat, Inc.. Consequentemente, não precisa ser executado manualmente. Para verificar se o disco foi criado, use o comando `ls -l /boot`, para garantir que o arquivo `initrd-<versão>.img` foi criado (a versão deve coincidir com a versão do kernel recém-instalado).

Em sistemas iSeries, o arquivo do disco RAM inicial e o arquivo vmlinux são combinados em um só arquivo, criado com o comando `addRamDisk`. Este passo é executado automaticamente se o kernel e seus pacotes associados são instalados ou atualizados através dos pacotes RPM distribuídos pela Red Hat, Inc.. Consequentemente, não precisa ser executado manualmente. Para verificar se o disco foi criado, use o comando `ls -l /boot`, para garantir que o arquivo `/boot/vmlinitrd-<kernel-versão>` foi criado (a versão deve coincidir com a versão do kernel recém-instalado).

O próximo passo é verificar se o gestor de início foi configurado para incializar o kernel novo. Consulte a Seção 39.6 para detalhes.

## 39.6. Verificando o Gestor de Início

O pacote RPM `kernel` configura o gestor de início para inicializar o kernel recém-instalado (exceto em sistemas IBM eServer iSeries). No entanto, não configura o gestor de início para inicializar o novo kernel por default.

É sempre bom confirmar se o gestor de início foi configurado corretamente. Este passo é crucial. Se o gestor de início for configurado incorretamente, o sistema não será inicializado apropriadamante no Red Hat Enterprise Linux. Se isto ocorrer, inicialize o sistema com o disquete boot criado anteriormente e tente configurar o gestor de início novamente.

### 39.6.1. Sistemas x86

Os sistemas x86 têm a opção de usar o GRUB ou o LILO como gestor de início, com uma exceção — os sistemas AMD64 não têm a opção de usar o LILO. Para todos os sistemas x86, o GRUB é o default.

#### 39.6.1.1. GRUB

Se usar o GRUB como gestor de início, confirme se o arquivo `/boot/grub/grub.conf` contém uma seção `title` com a mesma versão do pacote do `kernel` recém-instalado (se o `kernel-smp` ou o `kernel-hugemem` também foi instalado, existirá uma seção para este também):

```
# Note that you do not have to rerun grub after making changes to this file
# NOTICE:  You have a /boot partition.  This means that
#          all kernel and initrd paths are relative to /boot/, eg.
#          root (hd0,0)
#          kernel /vmlinuz-version ro root=/dev/hda2
#          initrd /initrd-version.img
#boot=/dev/hda
default=1
timeout=10
splashimage=(hd0,0)/grub/splash.xpm.gz
title Red Hat Enterprise Linux (2.4.21-1.1931.2.399.ent)
        root (hd0,0)
        kernel /vmlinuz-2.4.21-1.1931.2.399.ent ro root=LABEL=/
        initrd /initrd-2.4.21-1.1931.2.399.ent.img
title Red Hat Enterprise Linux (2.4.20-2.30.ent)
        root (hd0,0)
        kernel /vmlinuz-2.4.20-2.30.ent ro root=LABEL=/
        initrd /initrd-2.4.20-2.30.ent.img
```

Se uma partição `/boot/` separada foi criada, as localidades do kernel e da imagem initrd são relativas a `/boot/`.

Note que o default não está configurado para o kernel novo. Para configurar o GRUB a inicializar o kernel novo por default, altere o valor da variável `default` para o número da seção title que contém o kernel novo. A contagem começa pelo 0. Por exemplo: se o kernel novo está na primeira seção title, defina `default` para **0**.

Comece a testar o kernel novo reinicializando o computador e monitorando as mensagens para garantir que o hardware seja detectado apropriadamente.

#### 39.6.1.2. LILO

Se o LILO for usado como o gestor de início, confirme se o arquivo `/etc/lilo.conf` contém uma seção `image` com a mesma versão que o pacote do `kernel` recém-instalado (se o pacote `kernel-smp` ou o `kernel-hugemem` foi instalado, existirá uma seção para este também):

Note que o default não está configurado para o kernel novo. Para configurar o LILO a inicializar o kernel novo por default, defina o valor da variável `default` para o valor da `label` na seção image. Execute o comando `/sbin/lilo` como root para ativar as alterações. Após executá-lo, o output será similar ao seguinte:

```
Added 2.4.21-1.1931.2.399.ent *
Added linux
```

O `*` após `2.4.21-1.1931.2.399.ent` significa que o kernel desta seção é o kernel default que o LILO inicializará.

Comece a testar o kernel novo reinicializando o computador e monitorando as mensagens para garantir que o hardware seja detectado apropriadamente.

### 39.6.2. Sistemas Itanium

Os sistemas Itanium usam o ELILO como gestor de início, que usa o `/boot/efi/EFI/redhat/elilo.conf` como arquivo de configuração. Confirme se este arquivo contém uma seção `image` com a mesma versão que o pacote do `kernel` recém-instalado:

```
prompt
timeout=50
default=old

image=vmlinuz-2.4.21-1.1931.2.399.ent
        label=linux
        initrd=initrd-2.4.21-1.1931.2.399.ent.img
        read-only
        append="root=LABEL=/"
image=vmlinuz-2.4.20-2.30.ent
        label=old
        initrd=initrd-2.4.20-2.30.ent.img
        read-only
        append="root=LABEL=/"
```

Note que o default não está configurado para o kernel novo. Para configurar o ELILO a inicializar o kernel novo por default, altere o valor da variável `default` para o valor `label` da seção `image` que contém o kernel novo.

Comece a testar o kernel novo reinicializando o computador e monitorando as mensagens para garantir que o hardware seja detectado apropriadamente.

### 39.6.3. Sistemas IBM S/390 e IBM eServer zSeries

Os sistemas IBM S/390 and IBM eServer zSeries usam o z/IPL como gestor de início, que usa o `/etc/zipl.conf` como arquivo de configuração. Confirme se este arquivo contém uma seção com a mesma versão que o pacote do kernel recém-instalado:

```
[defaultboot]
default=old
target=/boot/
[linux]
        image=/boot/vmlinuz-2.4.21-1.1931.2.399.ent
        ramdisk=/boot/initrd-2.4.21-1.1931.2.399.ent.img
        parameters="root=LABEL=/"
[old]
        image=/boot/vmlinuz-2.4.20-2.30.ent
        ramdisk=/boot/initrd-2.4.20-2.30.ent.img
        parameters="root=LABEL=/"
```

Note que o default não está configurado para o kernel novo. Para configurar o z/IPL a inicializar o kernel novo por default, altere o valor da variável `default` para o nome da seção que contém o kernel novo. A primeira linha de cada seção contém o nome entre parênteses.

Após modificar o arquivo de configuração, execute o seguinte comando como root para ativar as alterações:

```
/sbin/zipl
```

Comece a testar o kernel novo reinicializando o computador e monitorando as mensagens para garantir que o hardware seja detectado apropriadamente.

### 39.6.4. Sistemas IBM eServer iSeries

O arquivo `/boot/vmlinitrd-<versão-do-kernel>` é instalado quando você atualiza o kernel. Entretanto, você deve usar o comando `dd` para configurar o sistema a inicializar o kernel novo:

1. Como root, submeta o comando `cat /proc/iSeries/mf/side` para determinar o lado default (A, B ou C).
2. Como root, submeta o seguinte comando, onde *<versão-do-kernel>* é a versão do kernel novo e *<lado>* é o lado do comando anterior:
   `dd if=/boot/vmlinitrd-<kernel-version> of=/proc/iSeries/mf/<side>/vmlinux bs=8k`

Comece a testar o kernel novo reinicializando o computador e monitorando as mensagens para garantir que o hardware seja detectado apropriadamente.

### 39.6.5. Sistemas IBM eServer pSeries

Os sistemas IBM eServer pSeries usam o YABOOT como gestor de início, que usa o `/etc/aboot.conf` como arquivo de configuração. Confirme se o arquivo contém uma seção `image` com a mesma versão que o pacote do `kernel` recém-instalado:

```
boot=/dev/sda1
init-message=Welcome to Red Hat Enterprise Linux!
Hit <TAB> for boot options

partition=2
timeout=30
install=/usr/lib/yaboot/yaboot
delay=10
nonvram

image=/vmlinux--2.4.20-2.30.ent
        label=old
        read-only
        initrd=/initrd--2.4.20-2.30.ent.img
        append="root=LABEL=/"

image=/vmlinux-2.4.21-1.1931.2.399.ent
        label=linux
        read-only
        initrd=/initrd-2.4.21-1.1931.2.399.ent.img
        append="root=LABEL=/"
```

Note que o default não está configurado para o kernel novo. O kernel da primeira imagem é inicializado por default. Para alterar o kernel default a inicializar, mova sua estrofe de imagem para que seja a primeira listada ou adicione a diretiva `default` e defina-a para a `label` da estrofe da imagem que contém o kernel novo.

Comece a testar o kernel novo reinicializando o computador e monitorando as mensagens para garantir que o hardware seja detectado apropriadamente.

# Capítulo 40.

# Módulos do Kernel

O kernel do Linux tem um design modular. No momento da inicialização, somente um kernel residente mínimo é carregado na memória. Depois disso, sempre que um usuário requisitar uma funcionalidade que não está presente no kernel residente, um *módulo do kernel*, por vezes referido como um *driver*, é dinamicamente carregado na memória.

Durante a instalação, o sistema detecta o hardware. Baseado nesta detecção e nas informações providas pelo usuário, o programa de instalação decide quais módulos precisam ser carregados no momento da inicialização. O programa de instalação configura o mecanismo de carregamento dinâmico para funcionar transparentemente.

Se hardware novo for adicionado após a instalação e este requer um módulo do kernel, o sistema deve ser configurado para carregar o módulo do kernel apropriado para o hardware novo. Quando o sistema é inicializado com o hardware novo, o programa **Kudzu** roda, detecta o hardware novo se for suportado e configura o módulo para ele. O módulo também pode ser especificado manualmente editando o arquivo de configuração do módulo, `/etc/modules.conf`.

**Nota**

Os módulos da placa de vídeo costumavam exibir a interface do Sistema X Window como parte do pacote `XFree86` e não do kernel; portanto, este capítulo não se aplica a eles.

Por exemplo: se um sistema inclui um adaptador de rede SMC EtherPower 10 PCI, o arquivo de configuração do módulo contém a seguinte linha:

```
alias eth0 tulip
```

Se uma segunda placa de rede, idêntica à primeira, for adicionada ao sistema, adicione a seguinte linha ao `/etc/modules.conf`:

```
alias eth1 tulip
```

Consulte o *Guia de Referência do Red Hat Enterprise Linux* para uma lista alfabética dos módulos do kernel e hardware suportados pelos módulos.

## 40.1. Utilitários do Módulo do Kernel

Um grupo de comandos para administrar módulos do kernel é disponibilizado se o pacote `modutils` está instalado. Use estes comandos ao determinar se um módulo foi carregado com sucesso ou ao tentar módulos diferentes para um novo componente de hardware.

O comando `/sbin/lsmod` exibe uma lista dos módulos carregados no momento. Por exemplo:

```
Module                  Size  Used by    Not tainted
iptable_filter          2412   0 (autoclean) (unused)
ip_tables              15864   1 [iptable_filter]
nfs                    84632   1 (autoclean)
lockd                  59536   1 (autoclean) [nfs]
sunrpc                 87452   1 (autoclean) [nfs lockd]
soundcore               7044   0 (autoclean)
```

```
ide-cd                  35836   0 (autoclean)
cdrom                   34144   0 (autoclean) [ide-cd]
parport_pc              19204   1 (autoclean)
lp                       9188   0 (autoclean)
parport                 39072   1 (autoclean) [parport_pc lp]
autofs                  13692   0 (autoclean) (unused)
e100                    62148   1
microcode                5184   0 (autoclean)
keybdev                  2976   0 (unused)
mousedev                 5656   1
hid                     22308   0 (unused)
input                    6208   0 [keybdev mousedev hid]
usb-uhci                27468   0 (unused)
usbcore                 82752   1 [hid usb-uhci]
ext3                    91464   2
jbd                     56336   2 [ext3]
```

Para cada linha, a primeira coluna é o nome do módulo; a segunda coluna é o tamanho do módulo e a terceira é a contagem de uso.

As informações após a contagem de uso variam ligeiramente por módulo. Se `(unused)` está listado na linha do módulo, este não está em uso. Se `(autoclean)` está na linha do módulo, este pode ser limpo automaticamente pelo comando `rmmod -a`. Quando este comando é executado, quaisquer módulos marcados com 'autoclean' que não foram usados desde a última ação de auto-limpeza, são descarregados. O Red Hat Enterprise Linux não executa a ação de auto-limpeza por default.

Se há um nome de módulo listado no fim da linha entre parênteses, este módulo é dependente do módulo listado na primeira coluna da linha. Por exemplo: na linha

```
usbcore                 82752   1 [hid usb-uhci]
```

os módulos `hid` e `usb-uhci` do kernel dependem do módulo usbcore.

O output do `/sbin/lsmod` é o mesmo que o output da visualização `/proc/modules`.

Para carregar um módulo do kernel, use o comando `/sbin/modprobe` seguido do nome do módulo do kernel. Por default, `modprobe` tenta carregar o módulo dos sub-diretórios `/lib/modules/<kernel-version>/kernel/drivers/`. Há um sub-diretório para cada tipo de módulo, como o sub-diretório`net/` para drivers de interface de rede. Alguns módulos do kernel têm dependências de módulo; ou seja, outros módulos devem ser carregados primeiro para que estes sejam carregados. O comando `/sbin/modprobe` verifica estas dependências e as carrega antes de carregar o módulo especificado.

Por exemplo: o comando

```
/sbin/modprobe hid
```

carrega quaisquer dependências de módulo e então o módulo `hid`.

Para exibir todos os comandos na tela, enquanto `/sbin/modprobe` os executa, use a opção `-v`. Por exemplo:

```
/sbin/modprobe -v hid
```

Aparece um output similar ao seguinte:

```
/sbin/insmod /lib/modules/2.4.21-1.1931.2.399.ent/kernel/drivers/usb/hid.o
Using /lib/modules/2.4.21-1.1931.2.399.ent/kernel/drivers/usb/hid.o
Symbol version prefix 'smp_'
```

O comando `/sbin/insmod` também serve para carregar oo mdulo do kernel; no entanto, não resolve as dependências. Sendo assim, é recomendado usar o comando `/sbin/modprobe`.

Para descarregar os módulos do kernel, use o comando `/sbin/rmmod` seguido do nome do módulo do kernel. O utilitário `rmmod` descarrega somente os módulos que não estão em uso e não são uma dependência de outros módulos em uso.

Por exemplo: o comando

```
/sbin/rmmod hid
```

descarrega o módulo `hid` do kernel.

Um outro utilitário útil para módulos do kernel é o `modinfo`. Use o comando `/sbin/modinfo` para exibir informações sobre um módulo do kernel. A sintaxe geral lé:

```
/sbin/modinfo [options] <module>
```

As opções incluem `-d` para exibir uma breve descrição do módulo e `-p` para listar os parâmetros suportados pelo módulo. Para obter uma lista completa das opções, consulte a página man do `modinfo` (`man modinfo`).

## 40.2. Recursos Adicionais

Para mais informações sobre os módulos do kernel e seus utilitários, consulte os seguintes recursos:

### 40.2.1. Documentação Instalada

- Página man do `lsmod` — descrição e explicação de seu output.
- Página man do `insmod` — descrição e listagem das opções de linha do comando.
- Página man do `modprobe` — descrição e listagem das opções de linha do comando.
- Página man do `rmmod` — descrição e listagem das opções de linha do comando.
- Página man do `modinfo` — descrição e listagem das opções de linha do comando.
- `/usr/src/linux-2.4/Documentation/modules.txt` — como compilar e usar os módulos do kernel. Este arquivo é parte do pacote `kernel-source`.

### 40.2.2. Sites Úteis

- http://www.redhat.com/mirrors/LDP/HOWTO/Module-HOWTO/index.html — *Linux Loadable Kernel Module HOWTO* do Projeto de Documentação do Linux.

Capítulo 41.

# Configuração do Agente de Transporte de Correio (MTA - Mail Transport Agent)

Um *Agente de Transporte de Correio* (MTA) é essencial para o envio de e-mail. Um *Agente de Usuário de Correio* (MUA) como o **Evolution**, **Mozilla Mail** e o **Mutt**, é usado para ler e compôr e-mails. Quando um usuário envia um e-mail de um MUA, as mensagens são passadas ao MTA, que envia a mensagem para uma série de MTAs até que chegue ao seu destino.

Mesmo que um usuário não planeje enviar e-mails de seu sistema, algumas tarefas automatizadas ou programas do sistema talvez usem o comando `/bin/mail` para enviar e-mail contendo mensagens de registro ao usuário root do sistema local.

O Red Hat Enterprise Linux 3 oferece dois MTAs: Sendmail e Postfix. Se ambos estão instalados, o `sendmail` é o MTA default. A **Comutador do Agente de Transporte de Correio** permite a seleção do `sendmail` ou do `postfix` como o MTA default do sistema.

O pacote RPM `redhat-switch-mail` deve estar instalado para usar a versão texto do programa **Comutador do Agente de Transporte de Correio**. Se você quer usar a versão gráfica, o pacote `redhat-switch-mail-gnome` também deve estar instalado. >>>>>> 1.1.2.4 Para mais informações sobre a instalação dos pacotes RPM, consulte a Parte III.

Para iniciar a **Comutador do Agente de Transporte de Correio**, selecione **Botão do Menu Principal** (no Painel) => **Ferramentas do Sistema => Mais Ferramentas do Sistema => Comutador do Agente de Transporte de Correio**, ou digite o comando `redhat-switch-mail` em uma janela de comandos (ex.: em um terminal GNOME ou XTerm).

O programa detecta automaticamente se o Sistema X Window está rodando. Se estiver, o programa inicia em modo gráfico, conforme mostra a Figura 41-1. Se o X não for detectado, inicia em modo texto. Para forçar a **Comutador do Agente de Transporte de Correio** a rodar no modo texto, use o comando `redhat-switch-mail-nox`.

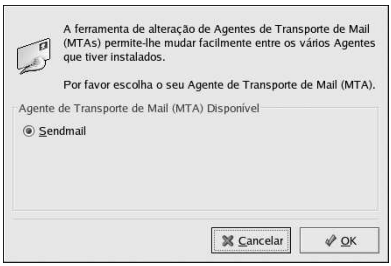


**Figura 41-1. Comutador do Agente de Transporte de Correio**

Se você selecionar **OK** para alterar o MTA, o daemon de correio selecionado é habilitado para iniciar no momento da inicialização, e o daemon de correio desselecionado é desabilitado, pois assim este não inicia no momento da inicialização da máquina. O daemon de correio selecionado é iniciado e o outro é parado, portanto as alterações têm efeito imediato.

Para mais informações sobre protocolos de e-mail e MTAs, consulte o *Guia de Referência do Red Hat Enterprise Linux;*.

# VI. Monitoramento do Sistema

Os administradores de sistema também monitoram o desempenho do sistema. O Red Hat Enterprise Linux contém ferramentas para auxiliar os administradores nestas tarefas.

## Índice

# Capítulo 42.

# Coletando Informações do Sistema

Antes de aprender como configurar seu sistema, você deve aprender a coletar informações essenciais do sistema. Por exemplo: você deve saber como encontrar a quantidade de memória livre, a quantidade de espaço disponível no disco rígido, como o disco rígido foi particionado e quais processos estão sendo executados. Este capítulo aborda como recuperar este tipo de informação de seu sistema Red Hat Enterprise Linux usando alguns comandos e programas simples.

## 42.1. Processos do Sistema

O comando `ps ax` exibe uma lista dos processos correntes do sistema, incluindo aqueles que pertencem a outros usuários. Para exibir os donos dos processos junto a estes use o comando `ps aux`. Esta é uma lista estática; em outras palavras, não é um retrato do que está rodando quando o comando foi submetido. Se você quer uma lista dos processos correntes atualizada constantemente, use o `top` conforme descrito abaixo.

O output do `ps` pode ser longo. Para evitar a rolagem pela página, você pode inserir um pipe com less:

```
ps aux | less
```

Você pode usar o comando `ps` combinado com o `grep` para checar se um processo está rodando. Por exemplo: para determinar se a **Emacs** está rodando, use o seguinte comando:

```
ps ax | grep emacs
```

O comando `top` exibe os processos correntes e também informações importantes sobre eles, inclusive sua memória e uso da CPU. A lista está em tempo real e é interativa. Veja abaixo um exemplo do output do comando `top`:

```
 19:11:04  up  7:25,  9 users,  load average: 0.00, 0.05, 0.12
89 processes: 88 sleeping, 1 running, 0 zombie, 0 stopped
CPU states:  cpu    user    nice  system    irq  softirq  iowait    idle
           total    6.6%    0.0%    0.0%   0.0%     0.0%    0.0%  192.8%
           cpu00    6.7%    0.0%    0.1%   0.1%     0.0%    0.0%   92.8%
           cpu01    0.0%    0.0%    0.0%   0.0%     0.0%    0.0%  100.0%
Mem:  1028556k av,  241972k used,  786584k free,       0k shrd,   37712k buff
       162316k active,               18076k inactive
Swap: 1020116k av,       0k used, 1020116k free                   99340k cached

  PID USER     PRI  NI  SIZE  RSS SHARE STAT %CPU %MEM   TIME CPU COMMAND
 1899 root      15   0 17728  12M  4172 S     6.5  1.2 111:20   0 X
 6380 root      15   0  1144 1144   884 R     0.3  0.1   0:00   0 top
    1 root      15   0   488  488   432 S     0.0  0.0   0:05   1 init
    2 root      RT   0     0    0     0 SW    0.0  0.0   0:00   0 migration/0
    3 root      RT   0     0    0     0 SW    0.0  0.0   0:00   1 migration/1
    4 root      15   0     0    0     0 SW    0.0  0.0   0:00   0 keventd
    5 root      34  19     0    0     0 SWN   0.0  0.0   0:00   0 ksoftirqd/0
    6 root      34  19     0    0     0 SWN   0.0  0.0   0:00   1 ksoftirqd/1
    9 root      25   0     0    0     0 SW    0.0  0.0   0:00   0 bdflush
    7 root      15   0     0    0     0 SW    0.0  0.0   0:00   1 kswapd
    8 root      15   0     0    0     0 SW    0.0  0.0   0:00   1 kscand
   10 root      15   0     0    0     0 SW    0.0  0.0   0:01   1 kupdated
   11 root      25   0     0    0     0 SW    0.0  0.0   0:00   0 mdrecoveryd
```

Para sair do `top`, pressione a tecla [q].

Veja a seguir comandos interativos úteis que você pode usar com o `top`:

| Comando | Descrição |
|---|---|
| [Space] | Atualizar a tela imediatamente |
| [h] | Exibir uma tela de ajuda |
| [k] | Matar (kill) um processo. Você deverá indicar o ID do processo e o sinal a ser enviado para ele. |
| [n] | Alterar o número de processos exibidos. Você deverá indicar o número. |
| [u] | Ordenar por usuário. |
| [M] | Ordenar por uso da memória. |
| [P] | Ordenar por uso da CPU. |

**Tabela 42-1. Comandos `top` interativos**

**Dica**

Aplicações como o **Mozilla** e o **Nautilus** são *thread-aware* — são criados threads múltiplos para lidar com usuários múltiplos ou pedidos múltiplos, e cada thread recebe um ID de processo. Por default, o `ps` e o `top` exibem somente o thread principal (inicial). Para visualizar todos os threads, use o comando `ps -m` ou pressione [Shift]-[H] no `top`.

Se você prefere uma interface gráfica do `top`, pode usar a **GNOME System Monitor**. Para iniciá-la pela área de trabalho, selecione **Botão do Menu Principal** (no Painel) => **Ferramentas do Sistema** => **Monitor do Sistema** ou digite `gnome-system-monitor` em uma janela de comandos no Sistema X Window. Então, selecione a aba **Listagem de Processos**.

O **Monitor do Sistema GNOME** permite que você procure processos na lista de processos correntes e também visualize todos os processos, os seu processos ou os processos ativos.

Para saber mais sobre um processo, selecione-o e clique no botão **Mais Informações**. Os detalhes do processo serão exibidos no rodapé da janela.

Para parar um processo, selecione-o e clique em **Finalizar Processo**. Esta função é útil para processos interrompidos em respota ao input do usuário.

Para ordenar pelas informações de uma coluna específica, clique no nome da coluna. A coluna que contém as informações através das quais a lista é ordenada, aparece em cinza escuro.

Por default, o **Monitor do Sistema GNOME** não exibe threads. Para alterar estas preferências, selecione **Editar => Preferências**, clique na aba **Listagem de Processos** e selecione **Exibir Threads**. As preferências também permitem configurar o intervalo de atualização, o tipo de informações exibidas por default sobre cada processo e as cores dos gráficos de monitoramento do sistema.

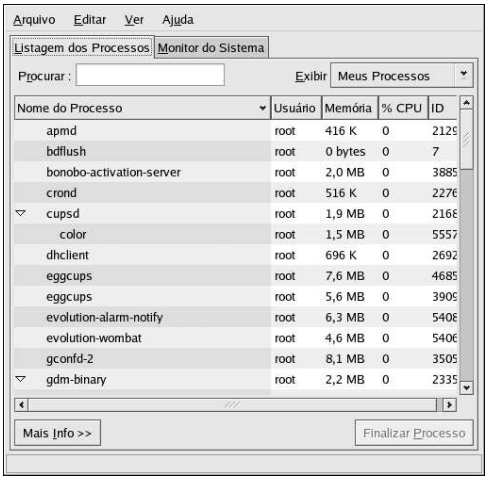


**Figura 42-1. GNOME System Monitor**

## 42.2. Uso da Memória

O comando `free` exibe a quantidade total de memória física e espaço swap do sistema, assim como a quantidade de memória usada, disponível, compartilhada, nos buffers do kernel e memória cacheada.

```
             total       used       free     shared    buffers     cached
Mem:        256812     240668      16144     105176      50520      81848
-/+ buffers/cache:     108300     148512
Swap:       265032        780     264252
```

O comando command `free -m` exibe as mesmas informações em megabytes, que têm uma leitura mais fácil.

```
             total       used       free     shared    buffers     cached
Mem:           250        235         15        102         49         79
-/+ buffers/cache:        105        145
Swap:          258          0        258
```

Se preferir uma interface gráfica do `free`, você pode usar o **Monitor do Sistema GNOME**. Para iniciá-lo pela área de trabalho, vá para o **Botão do Menu Principal** (no Painel) => **Ferramentas do Sistema** => **Monitor do Sistema** ou digite `gnome-system-monitor` em uma janela de comandos no Sistema X Window. E então feche a aba **Monitor do Sistema**.

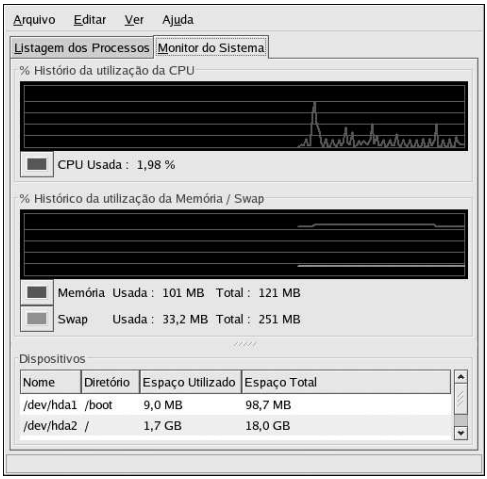


**Figura 42-2. GNOME System Monitor**

## 42.3. Sistemas de Arquivo

O comando `df` reporta o uso do espaço em disco do sistema. Se você digitar o comando `df` em uma janela de comandos, o output se parecerá com o seguinte:

```
Filesystem           1k-blocks      Used Available Use% Mounted on
/dev/hda2             10325716   2902060   6899140  30% /
/dev/hda1                15554      8656      6095  59% /boot
/dev/hda3             20722644   2664256  17005732  14% /home
none                    256796         0    256796   0% /dev/shm
```

Por default, este utilitário mostra o tamanho da partição em blocos de 1 kilobyte, e a quantidade de espaço usado e disponível no disco em kilobytes. Para visualizar as informações em megabytes e gigabytes, use o comando `df -h`. O argumento `-h` pede um formato 'human-readable'. O output se parece com o seguinte:

```
Filesystem            Size  Used Avail Use% Mounted on
/dev/hda2             9.8G  2.8G  6.5G  30% /
/dev/hda1              15M  8.5M  5.9M  59% /boot
/dev/hda3              20G  2.6G   16G  14% /home
none                  251M     0  250M   0% /dev/shm
```

Na lista de partições, há uma entrada `/dev/shm`. Esta representa o sistema de arquivo da memória virtual do sistema.

O comando `du` representa o espaço estimado em disco sendo usado por arquivos de um diretório. Se você digitar `du` em uma janela de comandos, verá o uso do disco de cada sub-diretório na lista. O total geral do diretório corrente e de seus sub-diretórios também será exibido na última linha da lista. Se você não deseja visualizar os totais de todos os sub-diretórios, use o comando `du -hs` para ver somente o total geral do diretório em formato legível. Use o comando `du --help` para ver mais opções.

Para visualizar as partições e uso do espaço do disco do sistema em formato gráfico, use a aba **Monitor do Sistema** conforme mostrado na parte inferior da Figura 42-2.

## 42.4. Hardware

Se você está tendo problemas ao configurar seu hardware ou deseja somente saber quais componentes de hardware estão presentes no sistema, pode usar a aplicação **Visualizador de Hardware** para exibir o hardware que pode ser detectado. Para iniciar o programa pela área de trabalho, selecione **Botão do Menu Principal => Ferramentas do Sistema => Visualizador de Hardware** ou digite `hwbrowser` em uma janela de comandos. Conforme a Figura 42-3, o programa exibe seus dispositivos de CD-ROM, disquetes, discos rígidos e suas partições, dispositivos de rede, dispositivos de apontamento (mouse), dispositivos do sistema e placas de vídeo. Clique no nome da categoria no menu esquerdo e a informação será exibida.

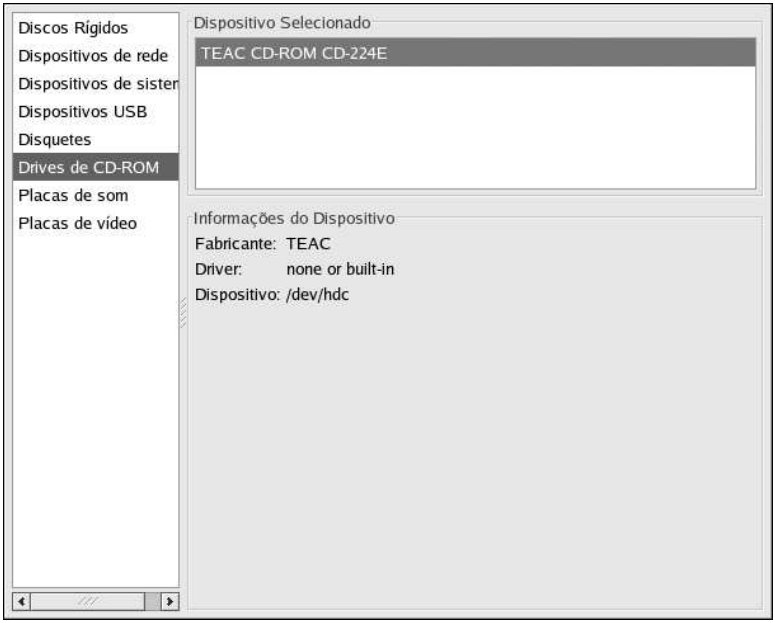


**Figura 42-3. Visualizador de Hardware**

Você também pode usar o comando `lspci` para listar todos os dispositivos PCI. Use o comando `lspci -v` para informações mais verbalisadas ou `lspci -vv` para um output bastante verbalisado.

Por exemplo: o `lspci` pode ser usado para determinar o fabricante, modelo e quantidade de memória de uma placa de vídeo do sistema:

```
01:00.0 VGA compatible controller: Matrox Graphics, Inc. MGA G400 AGP (rev 04) \
(prog-if 00 [VGA])
Subsystem: Matrox Graphics, Inc. Millennium G400 Dual Head Max
Flags: medium devsel, IRQ 16
Memory at f4000000 (32-bit, prefetchable) [size=32M]
Memory at fcffc000 (32-bit, non-prefetchable) [size=16K]
Memory at fc000000 (32-bit, non-prefetchable) [size=8M]
Expansion ROM at 80000000 [disabled] [size=64K]
Capabilities: [dc] Power Management version 2
Capabilities: [f0] AGP version 2.0
```

O `lspci` também é útil para determinar a placa de rede do seu sistema, caso você não saiba o fabricante ou número do modelo.

## 42.5. Recursos Adicionais

Para aprender mais sobre a coleta de informações do sistema, consulte os seguintes recursos.

### 42.5.1. Documentação Instalada

- `ps --help` — Exibe uma lista de opções que podem ser usadas com o `ps`.
- Página man do `top` — Digite `man top` para aprender mais sobre o `top` e suas diversas opções.
- Página man do `free` — digite `man free` para aprender mais sobre o `free` e suas diversas opções.
- Página man do `df` — Digite `man df` para aprender mais sobre o comando `df` e suas diversas opções.
- Página man do `du` — Digite `man du` para aprender mais sobre o comando `du` e suas diversas opções.
- Página man do `lspci` — Digite `man lspci` para aprender mais sobre o comando `lspci` e suas diversas opções.
- Diretório `/proc/` — O conteúdo do diretório `/proc` também pode ser usado para coletar informações mais detalhadas do sistema. Consulte o *Guia de Referência do Red Hat Enterprise Linux* para informações adicionais sobre o diretório `/proc/`.

### 42.5.2. Livros Relacionados

- *Introdução à Administração de Sistemas Red Hat Enterprise Linux*; Red Hat, Inc. — Inclui um capítulo sobre o monitoramento de recursos.

# Capítulo 43.

# OProfile

OProfile é uma ferramenta de monitoramento de desempenho do sistema, com baixa sobrecarga. Utiliza o hardware de monitoramento de desempenho no processador para recuperar informações sobre o kernel e executáveis do sistema. Por exemplo: quando a memória é referenciada, o número de pedidos do cache L2 e o número de interrupções de hardware recebidas. Em um sistema Red Hat Enterprise Linux, o pacote RPM `oprofile` deve estar instalado para usar esta ferramenta.

Muitos processadores incluem hardware de monitoramento do desempenho. Este hardware possibilita detectar quando determinados eventos ocorrem (como quando os dados requisitados não estão no cache). O hardware normalmente toma a forma de um ou mais *contadores* que são incrementados cada vez que ocorre um evento. Quando o valor do contador "adia," é gerada uma interrupção, possibilitando controlar a quantidade de detalhes (e consequentemente de sobrecarga) produzida pelo monitoramento do desempenho.

O OProfile usa este hardware (ou um substituto baseado em timer nos casos em que não há hardware de monitoramento de desempenho) para coletar *amostras* de dados relacionados ao desempenho cada vez que um contador gera uma interrupção. Estas amostras são gravadas periodicamente no disco; posteriormente, os dados contidos nestas amostras podem então ser usados para gerar relatórios de desempenho dos sistemas e aplicações.

**Importante**

O suporte ao kernel do OProfile no Red Hat Enterprise Linux 3 é baseado no código do kernel 2.5 em desenvolvimento. Quando nos referimos à documentação do OProfile, as funcionalidades específicas da versão 2.5 se aplicam ao OProfile do Red Hat Enterprise Linux 3, apesar da versão do kernel ser 2.4. Do mesmo modo, as funcionalidades do OProfile específicas do kernel 2.4 *não* se apicam ao Red Hat Enterprise Linux 3.

O OProfile é uma ferramenta útil, mas mas saiba de algumas limitações ao utilizá-lo:

- *Uso de bibliotecas compartilhadas* — Amostras de código em bibliotecas compartilhadas não são atribuídos a uma determinada aplicação a não ser que a opção `--separate=library` seja usada.
- *As amostras de monitoramento do desempenho são imprecisas* — Quando o registro do monitoramento de desempenho ativa uma amostra, a resolução da interrupção não é precisa como uma exceção 'divide by zero'. Devido à execução fora de ordem das instruções pelo processador, a amostra pode ser gravada em uma instrução próxima.
- `oprofpp` *não associa amostras apropriadamante para funções em linha* — o `oprofpp` usa um mecanismo de intervalo de endereço simples para determinar em qual função um endereço se encontra. As amostras de função em linha não são atribuídas à função em linha, mas sim à função na qual a função em linha estava inserida.
- *OProfile acumula dados de diversas execuções (runs)* — O OProfile é um perfilador do sistema e espera que os processos liguem e desliguem diversas vezes. Portanto, as amostras de diversas execuções são acumuladas. Use o comando `opcontrol --reset` para limpar as amostras de execuções anteriores.
- *Problemas de desempenho não são limitados à CPU* — O OProfile é orientado para encontrar problemas com processos limitados à CPU. OProfile não identifica processos adormecidos (asleep) porque estes aguardam bloqueios (locks) ou a ocorrência de algum outro evento (como o dispositivo I/O finanlizar uma operação).

No Red Hat Enterprise Linux, somente os kernels de multi-processador (multi-processor, SMP) têm o suporte ao OProfile habilitado. Para determinar qual kernel está rodando, invoque o seguinte comando:

```
uname -r
```

Se a versão do kernel retornada termina em `.entsmp`, o kernel do multi-processador está rodando. Caso contrário, instale-o via Red Hat Network ou pelos CDs da distribuição, mesmo se o sistema não for multi-processador. O kernel multi-processador pode rodar em um sistema de processador simples.

## 43.1. Visão Geral das Ferramentas

A Tabela 43-1 traz uma visão geral das ferramentas oferecidas com o pacote `oprofile`.

| Comando | Decrição |
|---|---|
| `opcontrol` | Configura quais dados são coletados. Consulte a Seção 43.2 para mais detalhes. |
| `op_help` | Exibe eventos disponíveis do processador do sistema junto a uma breve descrição de cada. |
| `op_merge` | Mistura diversas amostras do mesmo executável. Consulte a Seção 43.5.4 para mais detalhes. |
| `op_time` | Oferece uma visão geral de todos os executáveis perfilados. Consulte a Seção 43.5.1 para mais detalhes. |
| `op_to_source` | Cria uma fonte anotada para um executável se a aplicação foi compilada com símbolos de depuração. Consulte a Seção 43.5.3 para mais detalhes. |
| `oprofiled` | Roda como um daemon para gravar dados da amostra no disco periodicamente. |
| `oprofpp` | Recupera dados do perfil. Consulte a Seção 43.5.2 para mais detalhes. |
| `op_import` | Converte o arquivo do banco de dados de amostras de um formato diferente para o formato nativo do sistema. Use esta opção somente ao analisar um banco de dados de amostras de uma arquitetura diferente. |

**Tabela 43-1. Comandos do OProfile**

## 43.2. Configurando o OProfile

Antes de rodar o OProfile é necessário configurá-lo. Você deve, no mínimo, selecionar monitorar o kernel (ou selecionar não monitorar o kernel). As seções seguintes descrevem como usar o utilitário `opcontrol` para configurar o OProfile. Conforme os comandos `opcontrol` são executados, as opções de configurações são salvas no arquivo `/root/.oprofile/daemonrc`.

### 43.2.1. Especificando o Kernel

Primeiro, configure se o OProfile deve monitorar o kernel. Esta é a única opção de configuração requisitada antes de iniciar o OProfile. Todas as outras são opcionais.

Para monitorar o kernel, execute o seguinte comando como root:

```
opcontrol --vmlinux=/boot/vmlinux-`uname -r`
```

Para configurar o OProfile para não monitorar o kernel, execute o seguinte comand como root:

```
opcontrol --no-vmlinux
```

Este comando também carrega o módulo `oprofile` do kernel (se já não estiver carregado) e cria o diretório `/dev/oprofile/` se já não existe. Consulte a Seção 43.6 para obter detalhes sobre este diretório.

**Nota**

Mesmo se o OProfile está configurado para não perfilar o kernel, o kernel SMP ainda deve rodar para que o módulo `oprofile` possa ser carregado a partir dele.

Determinar se as amostras devem ser coletadas dentro do kernel, altera somente quais dados são coletados e não como ou onde os dados coletados são armazenados. Para gerar arquivos de amostra diferentes para as aplicações e bibliotecas do kernel, consulte a Seção 43.2.3.

### 43.2.2. Determinando os Eventos a Monitorar

A maioria dos processadores contém *contadores*, que são usados pelo OProfile para monitorar eventos específicos. Conforme observa-se na Tabela 43-2, o número de contadores disponíveis depende do processador.

| Processador | `cpu_type` | Número de Contadores |
|---|---|---|
| Pentium Pro | i386/ppro | 2 |
| Pentium II | i386/pii | 2 |
| Pentium III | i386/piii | 2 |
| Pentium 4 (não-hyper-threaded) | i386/p4 | 8 |
| Pentium 4 (hyper-threaded) | i386/p4-ht | 4 |
| Athlon | i386/athlon | 4 |
| AMD64 | x86-64/hammer | 4 |
| Itanium | ia64/itanium | 4 |
| Itanium 2 | ia64/itanium2 | 4 |
| TIMER_INT | timer | 1 |
| IBM eServer iSeries | timer | 1 |
| IBM eServer pSeries | timer | 1 |
| IBM eServer S/390 | timer | 1 |
| IBM eServer zSeries | timer | 1 |

**Tabela 43-2. Processadores e Contadores do OProfile**

Use a Tabela 43-2 para verificar se o tipo correto de processador foi detectado e para determinar o número de eventos que pode ser monitorado simultaneamente. O `timer` é usado como o tipo de processador se o processador não tiver hardware de monioramento de desempenho.

Se o `timer` é usado, os eventos não podem ser determinados para nenhum processador porque o hardware não suporta contadores de desempenho de hardware. Ao invés disso, a interrupção do timer é usada para o perfilamento.

Se o `timer` não é usado como o tipo processador, os eventos monitorados podem ser alterados, e o contador 0 do processador é determinado para um evento baseado na hora, por default. Se há mais de um contador no processador, os contadores além do contador 0 não são determinados para um evento, por default. Os eventos monitorados por default são apresentados na Tabela 43-3.

| Processador | Evento Default para o Contador 0 | Decrição |
|---|---|---|
| Pentium Pro, Pentium II, Pentium III, Athlon, AMD64 | CPU_CLK_UNHALTED | O relógio do processador não é desligado (halted) |
| Pentium 4 (HT e não-HT) | GLOBAL_POWER_EVENTS | O tempo durante o qual o processador não é parado |
| Itanium 2 | CPU_CYCLES | Ciclos da CPU |
| TIMER_INT | (nenhum) | Amostra de cada interrupção do timer |

**Tabela 43-3. Eventos Default**

O número de eventos que podem ser monitorados de uma vez é determinado pelo número de contadores do processador. Entretanto, esta não é uma correlação um-pra-um; em alguns processadores, determinados eventos devem ser mapeados para contadores específicos. Para determinar o número de contadores disponíveis, execute o seguinte comando:

```
cat /dev/oprofile/cpu_type
```

Os eventos disponíveis variam de acordo com o tipo de processador. Para determinar os eventos disponíveis para perfilamento, execute o seguinte comando como root (a lista é específica ao tipo de processador do sistema):

```
op_help
```

Os eventos de cada contador podem ser configurados através da linha de comando ou com uma interface gráfica. Se o contador não puder ser configurado para um evento específico, aparece uma mensagem de erro.

Para determinar o evento para cada contador configurável através da linha de comando, use o `opcontrol`:

```
opcontrol --ctrlN-event=<event-name>
```

Substitua *N* pelo número do contador (começando por 0) e substitua *<event-name>* pelo nome exato do evento, encontrado no `op_help`.

#### 43.2.2.1. Taxa de Amostragem

Por default, é selecionado um conjunto de eventos baseados na hora. São criadas aproximadamente 2000 amostras por segundo por processador. Se a interrupção do timer for usada, é definido um timer igual à taxa instantânea (jiffy rate), que não pode ser definido pelo usuário. Se o `cpu_type` não é

`timer`, cada evento pode ter uma *taxa de amostragem* definida. A taxa de amostragem é o número de eventos entre cada amostra instantânea.

Ao definir o evento para o contador, também é possível especificar uma taxa de amostragem:

```
opcontrol --ctrN-event=<event-name> --ctrN-count=<sample-rate>
```

Substitua <*sample-rate*> pelo número de eventos a aguardar antes de fazer o 'sampling' novamente. Quanto menor a contagem, mais frequentes as amostras. Para eventos que ocorrem esporadicamente, pode-se precisar de uma contagem menor para capturar as instâncias do evento.

**Atenção**

Seja muito cuidadoso ao determinar as taxas de amostragem. A amostragem muito frequente pode sobrecarregar o sistema, fazendo com que ele pareça estar congelado (frozen) ou fazendo com que realmente congele.

#### 43.2.2.2. Máscaras de Unidade (Unit Masks)

Se o `cpu_type` não é `timer`, as *máscaras de unidade* também podem ser necessárias para definir o evento posteriormente.

As máscaras de unidade de cada evento estão listadas no comando `op_help`. Os vores de cada máscara de unidade estão listadas no formato hexadecimal. Para especificar mais de uma máscara de unidade, os valores hexadecimais devem ser combinados usando uma operação 'bitwise', ou *bit-a-bit*.

```
opcontrol --ctrN-event=<event-name> --ctrN-count=<sample-rate> --ctrN-unit-mask=<value>
```

### 43.2.3. Separando os Perfis do Kernel e do Espaço do Usuário

Por default, as informações do modo kernel e do modo usuário são coletadas para cada evento. Para configurar o OProfile a não contar os eventos no modo kernel em um contador específico, execute o seguinte comando (onde *N* é o número do contador):

```
opcontrol --ctrN-kernel=0
```

Execute o segunte comando para iniciar novamente o perfilamento do modo do kernel para o contador:

```
opcontrol --ctrN-kernel=1
```

Para configurar o OProfile a não contar os eventos no modo usuário para um contador específico, execute o seguinte comando (onde *N* é o número do contador):

```
opcontrol --ctrN-user=0
```

Execute o seguinte comando para iniciar novamente o perfilamento do modo usuário para o contador:

```
opcontrol --ctrN-user=1
```

Quando o daemon do OProfile grava os dados do perfil nos arquivos de amostra, pode separar os dados do perfil da biblioteca e do kernel em arquivos de amostra separados. Para configurar como o daemon grava os arquivos de amostra, execute o seguinte comando como root:

```
opcontrol --separate=<choice>
```

<*choice*> pode ser uma das seguintes:

- `none` — não separa os perfis (default)
- `library` — gera perfis por aplicação para as bibliotecas
- `kernel` — gera perfis por aplicação para o kernel e seus módulos
- `all` — gera perfis por aplicação para as bibliotecas e perfis por aplicação para o kernel e seus módulos

Se `--separate=library` é usada, o nome do arquivo de amostras inclui os nomes dos executáveis, assim como o nome da biblioteca.

## 43.3. Iniciando e Parando o OProfile

Para começar a monitorar o sistema com o OProfile, execute o seguinte comando como root:

```
opcontrol --start
```

Aparece um output similar ao seguinte:

```
Using log file /var/lib/oprofile/oprofiled.log
Daemon started.
Profiler running.
```

A configuração contida no `/root/.oprofile/daemonrc` é usada.

O daemon do OProfile, `oprofiled`, é iniciado; ele grava periodicamente os dados da amostra no diretório `/var/lib/oprofile/samples/`. O arquivo de registro do daemon está localizado em `/var/lib/oprofile/oprofiled.log`.

Se o OProfile é reiniciado com opções de configuração diferentes, os arquivos de amostra da sessão anterior são automaticamente copiados (backed up) no diretório `/var/lib/oprofile/samples/session-`*N*, onde *N* é o número da sessão copiada previamente mais 1.

```
Backing up samples file to directory /var/lib/oprofile/samples//session-1
Using log file /var/lib/oprofile/oprofiled.log
Daemon started.
Profiler running.
```

Para parar o perfilador, execute o seguinte comando como root:

```
opcontrol --shutdown
```

## 43.4. Salvando Dados

Às vezes é útil salvar amostras numa hora específica. Por exemplo: quando perfilar um executável, é possível coletar amostras diferentes baseados em conjuntos de dados de input diferentes. Se o número de eventos a ser monitorado excede o número de contadores disponíveis no processador, é possível rodar o OProfile diversas vezes para coletar dados, salvando os dados da amostra cada vez em um arquivo diferente.

Para salvar o conjunto corrente de arquivos de amostra, execute o seguinte comando, substituindo <*name*> por um nome descritivo único para a sessão corrente:

```
opcontrol --save=<name>
```

O diretório `/var/lib/oprofile/samples/name/` é criado e os arquivos de amostra correntes são copiados neste.

## 43.5. Analisando os Dados

Periodicamente, o daemon do OProfile, `oprofiled`, coleta as amostras e as grava no diretório `/var/lib/oprofile/samples/`. Antes de ler, certifique-se de que todos os dados estão salvos neste diretório, executando seguinte comando como root:

```
opcontrol --dump
```

Cada nome de arquivo de amostra é baseado no nome do executável, com uma chave fechando (`}`) substituindo cada barra (`/`). O nome do arquivo termina com o jogo da velha (`#`), seguido pelo número do contador deste arquivo de amostra. Por exemplo: o arquivo a seguir inclui os dados de amostra do executável `/sbin/syslogd` coletado com o contador 0:

```
}sbin}syslogd#0
```

As seguintes ferramentas estão disponíveis para perfilar os dados de amostra após terem sido coletados:

- `op_time`
- `oprofpp`
- `op_to_source`
- `op_merge`

Use estas ferramentas, juntamente aos binários perfilados, para gerar relatórios que podem ser analisados futuramente.

**Atenção**

O executável sendo perfilado deve ser usado com estas ferramentas para analisar os dados. Se este deve mudar após a coleta dos dados, faça backup do executável usado para criar as amotras assim como dos arquivos de amostra.

As amostars de cada executável são gravadas em um único arquivo de amostra. As amostras de cada biblioteca ligada dinamicamente também são gravados em um arquivo único de amostra. Enquanto o OProfile está rodando, se o executável sendo monitorado alterar e existir um arquivo de amostra do executável, o arquivo de amostra existente é apagado automaticamente. Sendo assim, se precisar do arquivo de amostra existente, deve-se fazer backup junto ao executável usado para criá-lo, antes de substituir o executável por uma versão mais nova. Consulte a Seção 43.4 para detalhes sobre o backup do arquivo de amostra.

### 43.5.1. Usando o `op_time`

A ferramenta `op_time` oferece uma visão geral de todos os executáveis sendo perfilados.

Veja a seguir uma parte do exemplo de output:

```
581         0.2949  0.0000 /usr/bin/oprofiled
966         0.4904  0.0000 /usr/sbin/cupsd
1028        0.5218  0.0000 /usr/sbin/irqbalance
1187        0.6026  0.0000 /bin/bash
1480        0.7513  0.0000 /usr/bin/slocate
2039        1.0351  0.0000 /usr/lib/rpm/rpmq
6249        3.1722  0.0000 /usr/X11R6/bin/XFree86
8842        4.4885  0.0000 /bin/sed
31342      15.9103  0.0000 /usr/bin/gdmgreeter
58283      29.5865  0.0000 /no-vmlinux
82853      42.0591  0.0000 /usr/bin/perl
```

Cada executavel é listado em sua própria linha. A primeira coluna é o número de amostras gravadas para o executável. A segunda coluna é a porcentagem das amostras relativa ao número total de amostras. A terceira coluna não é usada e a quarta é o nome do executável.

Consulte a página man do `op_time` para obter uma lista das opções de linha de comandos, como a `-r`, usada para ordenar o output do executável, daquele com o maior número de amostras para o que tiver o menor número de amostras. A opção `-c` também é útil para especificar um número de contador.

### 43.5.2. Usando o `oprofpp`

Para recuperar informações detalhadas sobre um determinado executável, use o `oprofpp`:

```
oprofpp <mode> <executable>
```

*<executable>* deve ser a localidade completa do executável a ser analisado. O *<mode>* deve ser um dos seguintes:

`-l`

Lista os dados da amostra por símbolos. Por exemplo: veja a seguir uma parte do output da execução do comando `oprofpp -l /usr/X11R6/bin/XFree86`:

```
vma      samples  %           symbol name
...
08195d10 4        3.0303      miComputeCompositeClip
080b9180 5        3.78788     Dispatch
080cdce0 5        3.78788     FreeResource
080ce4a0 5        3.78788     LegalNewID
080ce640 5        3.78788     SecurityLookupIDByClass
080dd470 9        6.81818     WaitForSomething
080e1360 12       9.09091     StandardReadRequestFromClient
...
```

A primeira coluna é o endereço inicial da memória virtual (virtual memory address, vma). A segunda coluna é o número de amostras do símbolo. A terceira coluna é a porcentagem de amostras deste símbolo relativa ao número total de amostras do executável, e a quarta coluna é o nome do símbolo.

Para ordenar o output do maior número de amostras para o menor (ordem inversa), use `-r` em conjunto com a opção `-l`.

`-s <symbol-name>`

Lista os dados da amostra específicos a um nome de símbolo. Por exemplo: o seguinte output é do comando `oprofpp -s StandardReadRequestFromClient /usr/X11R6/bin/XFree86`:

```
vma      samples  %           symbol name
080e1360 12       100         StandardReadRequestFromClient
080e1360 1        8.33333
080e137f 1        8.33333
080e13bb 1        8.33333
080e13f4 1        8.33333
080e13fb 1        8.33333
080e144a 1        8.33333
080e15aa 1        8.33333
080e1668 1        8.33333
080e1803 1        8.33333
080e1873 1        8.33333
080e190a 2        16.6667
```

A primeira linha é um resumo da combinação símbolo/executável.

A primeira coluna consiste dos endereços da memória virtual amostrados. A segunda coluna é o número de amostras do endereço da memória. A terceira coluna é a porcentagem das amostras do endereço da memória relativa ao número total de amostras do símbolo.

`-L`

Lista os dados da amostra por símbolos, com mais detalhes que a `-l`. Exemplo:

```
vma      samples  %           symbol name
08083630 2        1.51515     xf86Wakeup
 08083641 1        50
 080836a1 1        50
080b8150 1        0.757576    Ones
 080b8179 1        100
080b8fb0 2        1.51515     FlushClientCaches
 080b8fb9 1        50
 080b8fba 1        50
...
```

Os dados são os mesmos que da opção `-l`, exceto que, para cada símbolo, é exibido um endereço usado da memória virtual. Para cada endereço da memória virtual, são apresentados o número de amostras e a porcentagem de amostras realativa ao número total de amostras do símbolo.

`-g <file-name>`

Gera o output para um arquivo no formato `gprof`. Se o arquivo gerado tiver o nome `gmon.out`, o `gprof` pode ser usado para analisar os dados detalhadamente.. Consulte a página man do `gprof` para detalhes.

Veja a seguir outras opções para restringir os dados:

`-f <file-name>`

Usa o arquivo de amostra especificado *<file-name>*. Por default, o arquivo de amostra do `/var/lib/oprofile/samples/` é usado. Use esta opção para especificar um arquivo de amostra de uma sessão anterior.

`-i <file-name>`

Use *<file-name>* como o nome do executável para o qual recuperar dados.

`-d`

Decodifica os nomes dos símbolos C++.

`-D`

Decodifica os nomes dos símbolos C++ e simplifica os nomes decodificados da biblioteca STL.

`--counter <number>`

Coleta informações de um contador específico. Caso não seja especificado, o contador default é 0.

`-o`

Exibe o número da linha no código fonte de cada amostra. O executável deve ser compilado, com a opção `-g` do GCC. Caso contrário, esta opção não pode exibir os números das linhas. Por default, nenhum dos executáveis do Red Hat Enterprise Linux são compilados com esta opção.

```
vma      samples  %      symbol name         linear info
0806cbb0 0        0      _start              ../sysdeps/i386/elf/start.S:47
```

`-e <symbol-name>`

Exclui a lista de símbolos separada por vírgulas do output.

`-k`

Apresenta uma coluna adicional contendo a biblioteca compartilhada. Esta opção produz resultados somente se a opção `--separate=library` do `opcontrol` é especificada ao configurar o OProfile e se a opção `--dump-gprof-file` não for usada em conjunto com esta.

`-t <format>`

Apresenta o output em uma ordem específica de colunas. Esta opção não pode ser usada com a `-g`.

Use as seguintes letras para representar as colunas:

| Letra | Decrição |
|---|---|
| **v** | Endereço da memória virtual |
| **s** | Número de amostras |
| **S** | Número acumulado de amostras |
| **p** | Porcentagem de amostras relativa ao número total de amostras do executável |
| **P** | Porcentagem acumulativa de amostras relativa ao número total de amostras do executável |
| **q** | Porcentagem de amostras relativa a todos os executáveis amostrados |
| **Q** | Porcentagem acumulada das amostras relativa a todos os executáveis amostrados |
| **n** | Nome do símbolo |
| **l** | Nome do arquivo do fonte e número da linha, incluindo a localidade completa |
| **L** | Nome base do arquivo do código fonte e número da linha |
| **i** | Nome do executável, incluindo a localidade completa |
| **I** | Nome base do executável |
| **d** | Detalhes da amostra |
| **h** | Exibe os cabeçalhos das colunas |

**Tabela 43-4. Letras para a Ordem das Colunas**

`--session <name>`

Especifica a localidade completa da sessão ou de um diretório relativo ao diretório `/var/lib/oprofile/samples/`.

`-p <path-list>`

Especifica uma lista de localidades separadas por vírgulas, na qual localizam-se os executáveis a serem analisados.

### 43.5.3. Usando `op_to_source`

A ferramenta `op_to_source` tenta juntar as amostras para instruções específicas às linhas correspondentes no código fonte. Os arquivos resultantes gerados devem ter as amostras das linhas à esquerda. Também insere um comentário no começo de cada função, listando as amostras totais da função.

Para que este utilitário funcione, o executável deve ser compilado com a opção `-g` do GCC. Por default, os pacotes do Red Hat Enterprise Linux não são compilados com esta opção.

A sintaxe geral do `op_to_source` é a seguinte:

```
op_to_source --source-dir <src-dir> <executable>
```

O diretório contendo o código fonte e o executável a ser analisado deve ser especificado. Consulte a página man do `op_to_source` para ver uma lista das opções de linha de comando.

### 43.5.4. Usando o `op_merge`

Se há diversos arquivos de amostra para exatamente o mesmo executável ou biblioteca, os arquivos de amostra podem ser fundidos (merged) para facilitar a análise.

Por exemplo: para fundir arquivos da biblioteca `/usr/lib/library-1.2.3.so`, execute o seguinte comando como root:

```
op_merge /usr/lib/library-1.2.3.so
```

O arquivo resultante é `/var/lib/oprofile/samples/}usr}lib}library-1.2.3.so`.

Para limitar as amostras fundidas em um contador específico, use a opção `-c` seguida pelo número do contador.

## 43.6. Entendendo o `/dev/profile/`

O diretório `/dev/oprofile/` contém o sistema de arquivo do OProfile. Use o comando `cat` para exibir os valores dos arquivos virtuais deste sistema de arquivo. Por exemplo: o comando seguinte exibe o tipo de processador detectado pelo OProfile:

```
cat /dev/oprofile/cpu_type
```

Existe um diretório `/dev/oprofile/` para cada contador. Por exemplo: se há 2 contadores, existirão os diretórios `/dev/oprofile/0/` e `dev/oprofile/1/`.

Cada diretório de um contador contém os seguintes arquivos:

- `count` — Intervalo entre amostras
- `enabled` — Se for 0, o contador está desligado e nenhuma amostra é coletada para este diretório. Se for 1, o contador está ligado e as amostras são coletadas
- `event` — Evento a monitorar
- `kernel` — Se for 0, as amostras não são coletadas para este evento do contador quando o processador está no espaço do kernel. Se for 1, as amostras são coletadas mesmo se o processoador estiver no espaço do kernel.
- `unit_mask` — Quais máscaras de unidade são habilitadas para o contador
- `user` — Se for 0, as amostras não são coletadas para o evento do contador quando o processador está no espaço do usuário. Se for 1, as amostras são coletadas mesmo se o processador estiver no espaço do usuário

Os valores destes arquivos podem ser recuperados com o comando `cat`. Exemplo:

```
cat /dev/oprofile/0/count
```

## 43.7. Uso do Exemplo

Apesar do OProfile ser usado para desenvolvedores analisarem o desempenho de aplicações, também serve para administradores de sistemas analisarem o sistema. Por exemplo:

- *Determine quais aplicações e serviços são mais usados em um sistema* — o `op_time` pode ser usado para determinar quanto tempo do processador uma aplicação ou serviço usa. Se o sistema é usado por diversos serviços, mas está com desempenho baixo, os serviços que mais consomem tempo do processador podem ser movidos para um sistema dedicado.
- *Determine o uso do processador* — O evento `CPU_CLK_UNHALTED` pode ser monitorado para determinar a carga do processador em um determinado período de tempo. Estes dados podem ser usados para determinar se processadores adicionais ou mais rápidos podem melhorar o desempenho do sistema.

## 43.8. Interface Gráfica

Algumas preferências do OProfile podem ser definidas com a interface gráfica. Para iniciá-la, execute o comando `oprof_start` como root em uma janela de comandos.

Após alterar as opções, estas podem ser salvas ao clicar no botão **Salvar e sair** (Save and quit). As preferências são gravadas no `/root/.oprofile/daemonrc`e a aplicação é fechada. Sair da aplicação não interrompe o processo de amostragem do OProfile.

Na aba **Configurar** (Setup), usada para determinar os eventos para os contadores, conforme descrito na Seção 43.2.2, selecione o contador no menu suspenso e o evento na lista. É apresentada uma breve descrição do evento na caixa de texto abaixo da lista. Somente os eventos disponíveis para o contador e arquitetura específicos são apresentados. A interface também exibe se o perfilador está rodando ou não e algumas estatísticas sobre ele.

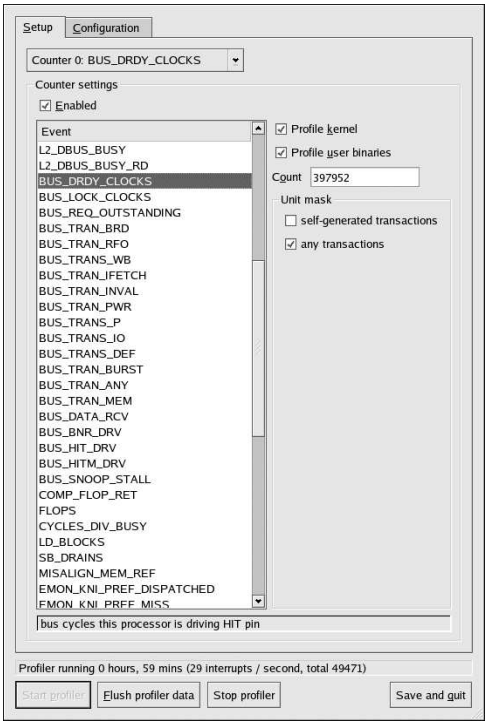


**Figura 43-1. Configuração do OProfile**

No lado direito da aba, selecione a opção **Perfilar o kernel** para contar os eventos no modo kernel do evento atualmente selecionado, conforme abordado na Seção 43.2.3. Isto é equivalente ao comando `opcontrol --ctr`*N*`-kernel=1`, onde *N* é o número do contador. Se está opção está desselecionada, é equivalente ao comando `opcontrol --ctr`*N*`-kernel=0`.

Selecione a opção **Perfilar binários do usuário** para contar os eventos no modo usuário do evento atualmente selecionado, conforme abordado na Seção 43.2.3. Isto é equivalente ao comando `opcontrol --ctr`*N*`-user=1`, onde *N* é o número do contador. Se esta opção está desselecionada, é equivalente ao comando `opcontrol --ctr`*N*`-user=0`.

Use o campo de texto **Contar** para determinar a taxa de amostragem do evento atualmente selecionado, conforme abordado na Seção 43.2.2.1.

Se há máscaras de unidade disponíveis para o evento selecionado, conforme abordado na Seção 43.2.2.2, estas são exibidas na área **Máscaras de unidade** no lado direito da aba **Configurar**. Selecione a caixa ao lado da máscara de unidade para habilitá-la para o evento.

Na aba **Configuração**, para perfilar o kernel, indique o nome e localidade do arquivo `vmlinux` do kernel a monitorar no campo **Arquivo da imagem do kernel**. Para configurar o OProfile a não monitorar o kernel, selecione **Sem imagem do kernel**.


**Figura 43-2. Configuração do OProfile**

Se a opção **Verbal** está selecionada, o registro do daemon `oprofiled` inclui mais informações.

Se **Arquivos de amostras do kernel por aplicação** está selecionada, o OProfile gera perfis por aplicação para o kernel e seus módulos, conforme abordado na Seção 43.2.3. Isto é equivalente ao comando `opcontrol --separate=kernel`. Se **Arquivos de amostras de bibliotecas compartilhadas por aplicação** está selecionada, o OProfile gera perfis por aplicação para as bibliotecas. Isto é equivalente ao comando `opcontrol --separate=library`.

Para forçar os dados a serem salvos nos arquivos de amostra (conforme abordado na Seção 43.5) clique no botão **Expor dados do perfilador**(Flush profiler data). Isto é equivalente ao comando `opcontrol --dump`.

Para iniciar o OProfile na interface gráfica, clique em **Iniciar perfilador**. Para parar o perfilador, clique em **Parar perfilador**. Sair da aplicação não interrompe a amostragem do OProfile.

## 43.9. Recursos Adicionais

Este capítulo destaca somente o OProfile, como configurá-lo e usá-lo. Para aprender mais, consulte os seguintes recursos.

### 43.9.1. Documentação Instalada

- `/usr/share/doc/oprofile-0.5.4/oprofile.html` — *OProfile Manual*
- Página man do `oprofile` — Aborda `opcontrol`, `oprofpp`, `op_to_source`, `op_time`, `op_merge` e `op_help`

### 43.9.2. Sites Úteis

- http://oprofile.sourceforge.net/ — contém a documentação mais recente, listas de discussão, canais IRC e outros.

# VII. Apêndices

Esta parte contém instruções para a criação de um kernel personalizado a partir dos arquivos fonte providos pela Red Hat, Inc..

## Índice

# Apêndice A.
# Criando um Kernel Personalizado

Muitas usuários novos do Linux perguntam: "Por que eu devo criar meu próprio kernel?" Dados os avanços no uso dos módulos do kernel, a resposta mais adequada para esta pergunta é: "Se você não sabe porque deve criar seu próprio kernel, provavelmente não é necessário fazê-lo."

O kernel distribuído junto ao Red Hat Enterprise Linux e através do sistema de Erratas do Red Hat Enterprise Linux oferece suporte para as funcionalidades mais modernas de hardware e do kernel. Para a maioria dos usuários, não é necessário recompilar o kernel. Este apêndice é oferecido como um guia para usuários que queiram recompilar seu kernel para assim aprender mais sobre ele, ou para usuários que queiram compilar uma funcionalidade experimental no kernel, dentre outros casos.

Para atualizar (upgrade) o kernel usando os pacotes do kernel distribuídos pela Red Hat, Inc., consulte o Capítulo 39.

**Aviso**

A criação de um kernel personalizado não é suportada pela Equipe de Suporte à Instalação. Para mais informações sobre a atualização de seu kernel usando os pacotes RPM distribuídos pela Red Hat, Inc., consulte o Capítulo 39.

## A.1. Preparando para Criar

Antes de criar um kernel personalizado, é extremamente importante certificar que você tenha um disquete boot de emergência funcionando, caso cometa algum erro. Para criar um disquete boot que inicializará a máquina com o kernel atual, execute o seguinte comando:

```
/sbin/mkbootdisk `uname -r`
```

Após criar o disquete, teste-o para verificar se realmente inicializa o sistema.

Para recompilar o kernel, é necessário ter o pacote `kernel-source` instalado. Invoque o comando

```
rpm -q kernel-source
```

para determinar se está instalado. Se não estiver instalado, instale-o pelos CDs do Red Hat Enterprise Linuxou pela Red Hat Network. >>>>>> 1.1.2.4 Para mais informações sobre a instalação dos pacotes RPM, consulte a Parte III.

## A.2. Criando o Kernel

Para criar um kernel personalizado (execute todos estes passos como root):

**Nota**

Este exemplo usa a 2.4.21-1.1931.2.399.ent como a versão do kernel (a versão do kernel pode variar). Para determiná-la, digite o comando `uname -r` e substitua 2.4.21-1.1931.2.399.ent pela versão do kernel retornada pelo comando.

1. Abra uma janela de comandos e vá para o diretório `/usr/src/linux-2.4/`. Todos os comandos a partir deste ponto devem ser executados neste diretório.
2. É importante que a criação do kernel comece com a árvore fonte em um estado conhecido. Consequentemente, é recomendado que o comando `make mrproper` seja executado antes de remover quaisquer arquivos de configuração de criações anteriores que talvez se encontrem dispersos na árvore fonte. Se já houver um arquivo de configuracão como o `/usr/src/linux-2.4/.config`, faça um back up em um outro diretório, antes de rodar este comando e copiar o arquivo de volta mais tarde.
3. É recomendado que a configuração do kernel default do Red Hat Enterprise Linux seja usada como um ponto de partida. Para fazer isso, copie o arquivo de configuração da arquitetura do sistema, do diretório `/usr/src/linux-2.4/configs/` para o `/usr/src/linux-2.4/.config`. Se o sistema tem mais de um processador, copie o arquivo que contém a palavra `smp`. Entretanto, se o sistema tem mais de quatro gigabytes de memória, copie o arquivo que contém a palavra `hugemem`.
4. Em seguida, personalize a configuração. O método recomendado é usar o comando `make menuconfig` para rodar o programa da **Configuração do Kernel do Linux**. O Sistema X Window não é necessário.

   Após terminar a configuração, selecione **Sair** (Exit) e selecione **Sim** (Yes) para salvar o arquivo de configuração do kernel novo (`/usr/src/linux-2.4/.config`).

   Mesmo que nenhuma alteração tenha sido feita, é necessário executar o comando `make menuconfig` (ou um dos outros métodos de configuração do kernel) antes de continuar.

   Outros métodos disponíveis para a configuração do kernel incluem:

   - `make config` — Um programa texto interativo. Os componentes são apresentados em um formato linear e respondidos um de cada vez. Este método não requer o Sistema X Window e não permite alterar as respostas de questões anteriores.
   - `make xconfig` — Este método requer o Sistema X Window e o pacote `tk`. Não é recomendado porque não analisa os arquivos de configuração de maneira confiável.
   - `make oldconfig` — Este é um script não-interativo que lê o arquivo de configuração existente (`.config`) e pergunta somente questões que não existiam anteriormente.

**Nota**

Para usar o `kmod` e os módulos do kernel, responda **`Sim`** a `kmod support` e `module version (CONFIG_MODVERSIONS) support` durante a configuração.

5. Após criar o arquivo `/usr/src/linux-2.4/.config`, use o comando `make dep` para configurar as dependências corretamente.
6. Use o comando `make clean` para preparar a árvore fonte para a criação do kernel.
7. É recomendado que o kernel personalizado tenha um número de versão modificado, para que o kernel existente não seja sobrescrito. Através do método descrito aqui, é mais fácil recuperar, no caso de um acidente. Veja os detalhes de outras possibilidades no site http://www.redhat.com/mirrors/LDP/HOWTO/Kernel-HOWTO.html ou no arquivo `Makefile` no `/usr/src/linux-2.4/`.

   Por default, o `/usr/src/linux-2.4/Makefile` inclui a palavra `custom` no fim da linha que começa com `EXTRAVERSION`. Anexar o trecho de caracteres permite que o sistema tenha o kernel antigo e o kernel novo (versão 2.4.21-1.1931.2.399.entcustom) funcionando no mesmo sistema ao mesmo tempo.

Se o sistema contém mais de um kernel personalizado, aconselhamos anexar a data no final (ou algum outro identificador).

8. Nas arquiteturas x86 e AMD64, crie o kernel com o `make bzImage`. Na arquitetura Itanium, crie o kernel com o `make compressed`. Nas arquiteturas S/390 e zSeries, crie o kernel com o `make image`. Para o iSeries e pSeries, crie o kernel com o comando `make boot`.
9. Crie todos os módulos configurados com o `make modules`.
10. Use o comando `make modules_install` para instalar os módulos do kernel (mesmo que nada tenha sido realmente criado). Atente para o underscore (_) no comando. Isto instala os módulos do kernel na localidade `/lib/modules/<KERNELVERSION>/kernel/drivers` (onde *KERNELVERSION* é a versão especificada no `Makefile`). Neste exemplo, será `/lib/modules/2.4.21-1.1931.2.399.entcustom/kernel/drivers/`.
11. Use `make install` para copiar o kernel novo e os arquivos a ele associados nos diretórios apropriados.

    Além de instalar os arquivos do kernel no diretório `/boot`, este comando também executa o script `/sbin/new-kernel-pkg` que cria uma imagem `initrd` nova e adiciona novas entradas ao arquivo de configuração do gestor de início.

    Se o sistema tem um adaptador SCSI e o driver SCSI foi compilado como um módulo, ou se o kernel foi criado com o suporte ao ext3 como um módulo (default no Red Hat Enterprise Linux), a imagem `initrd` é necessária.
12. Mesmo que sejam feitas alterações à imagem `initrd` e ao gestor de início, verifique se foram feitas corretamente e certifique-se de usar a versão do kernel personalizado, ao invés do 2.4.21-1.1931.2.399.ent. Consulte a Seção 39.5 e a Seção 39.6 para obter instruções sobre a verificação destas modificações.

## A.3. Recursos Adicionais

Para mais informações sobre o kernel do Linux, consulte os seguintes recursos.

### A.3.1. Documentação Instalada

- `/usr/src/linux-2.4/Documentation/` — Este diretório contém documentação avançada sobre o kernel do Linux e seus módulos. Estes documentos são escritos para pessoas interessadas em contribuir para o código fonte do kernel e entender como ele funciona.

### A.3.2. Sites Úteis

- http://www.redhat.com/mirrors/LDP/HOWTO/Kernel-HOWTO.html — *The Linux Kernel HOWTO* do Projeto de Documentação do Linux.
- http://www.kernel.org/pub/linux/docs/lkml/ — A lista de discussão do kernel do Linux.

# Índice Remissivo

## Símbolos



## A

## B



## C

## D

## E



## F

## G



## H



## I



## K

## L



## M



## N



## O

## P

## Q



## R

## S

## T



## U



## V



## W



## X

## Y

# Considerações finais

Os manuais são escritos no formato DocBook SGML versão 4.1. Os formatos HTML e PDF são produzidos usando stylesheets DSSSL personalizadas e scripts jade wrapper personalizados. Os arquivos SGML do DocBook são escritos em **Emacs** com o auxílio do modo PSGML.

Garrett LeSage criou as imagens de alerta (nota, dica, importante, atenção e aviso). Elas podem ser distribuídas livremente com a documentação da Red Hat.

A Equipe de Documentação de Produtos da Red Hat Linux é composto pelas seguintes pessoas:

Sandra A. Moore — Escritora / Mantenedora Principal do *Guia de Instalação para as Arquiteturas x86, Itanium™ e AMD64 do Red Hat Enterprise Linux*; Escritora / Mantenedora Principal do *Guia de Instalação para as Arquiteturas IBM® eServer™ iSeries™ e IBM® eServer™ pSeries™ do Red Hat Enterprise Linux*; Escritora contribuinte do *Guia Passo a Passo do Red Hat Enterprise Linux*

Tammy Fox — Escritora Principal/Mantenedora do *Guia de Administração do Sistema do Red Hat Enterprise Linux*; Escritora contribuinte do *Guia de Instalação para as Arquiteturas x86, Itanium™ e AMD64 do Red Hat Enterprise Linux*; Escritora contribuinte do *Guia de Segurança do Red Hat Enterprise Linux*; Escritora contribuinte do *Guia Passo a Passo do Red Hat Enterprise Linux*; Escritora Principal/Mantenedora dos scripts e stylesheets personalizados do DocBook

Edward C. Bailey — Escritor Principal/Mantenedor do *Introdução à Administração de Sistemas Red Hat Enterprise Linux*; Escritor Principal/Mantenedor das *Notas de Versão*; Escritor contribuinte do *Guia de Instalação para as Arquiteturas x86, Itanium™ e AMD64 do Red Hat Enterprise Linux*

Johnray Fuller — Escritor / Mantenedor Principal do *Guia de Referência do Red Hat Enterprise Linux*; Co-escritor e co-mantenedor do *Guia de Segurança do Red Hat Enterprise Linux*; Escritor contribuinte do *Introdução à Administração de Sistemas Red Hat Enterprise Linux*

John Ha — Escritor / Mantenedor Principal do *Configurando e Administrando um Cluster do Red Hat Cluster Suite*; Escritor / Mantenedor Principal do *Glossário da Red Hat*; Escritor / Mantenedor Principal do *Guia de Instalação para as Arquiteturas IBM® S/390® e IBM® eServer™ zSeries® do Red Hat Enterprise Linux*; Co-escritor/co-mantenedor do *Guia de Segurança do Red Hat Enterprise Linux*; Escritor contribuinte do *Introdução à Administração de Sistemas Red Hat Enterprise Linux*; Escritor contribuinte do *Guia Passo a Passo do Red Hat Enterprise Linux*

A Equipe de Internacionalização da Red Hat é composta pelas seguintes pessoas:

Jean-Paul Aubry — traduções para o Francês

David Barzilay — traduções para o Português Brasileiro

Bernd Groh — traduções para o Alemão

James Hashida — traduções para o Japonês

Michelle Ji-yeen Kim — traduções para o Coreano

Yelitza Louze — traduções para o Espanhol

Noriko Mizumoto — traduções para o Japonês

Nadine Richter — traduções para o Alemão

Audrey Simons — traduções para o Francês

Francesco Valente — traduções para o Italiano

Sarah Saiying Wang — traduções para o Chinês Simplificado

Ben Hung-Pin Wu — traduções para o Chinês Tradicional