Material disponível em: www.ProjetodeRedes.com.br

Guia do Servidor Linux

Editado por

Conectiva S.A.

www.ProjetodeRedes.kit.net

Guia do Servidor

Editado por Conectiva S.A.

2.0 Edição

Publicado em novembro de 2000

Coordenação: Márcia Gawlak

Autores: Roberto Teixeira; Carlos Daniel Mercer;

Imagens: Artur T. Hara

Revisão Gramatical: Fernando Cardoso Nascimento

Desenvolvimento/Diagramação: Jorge Luiz Godoy Filho

Os autores gostariam de ser avisados sobre modificações, traduções e versões impressas.

Agradecemos a todos aqueles que têm participado ativamente no desenvolvimento dos trabalhos de tradução, internacionalização, divulgação e adaptação do Linux à realidade latinoamericana, pois muito de nosso esforço está calcado no esforço participativo desta comunidade.

Esperamos que este guia seja de utilidade para todos aqueles que busquem uma ferramenta de auxílio às suas atividades diárias, e que possa enriquecer e facilitar os seus conhecimentos.

Dados Internacionais de Catalogação na Publicação (CIP)

(Câmara Brasileira do Livro, SP, Brasil)

ISBN 85-87118-29-3

1. Linux (Sistema operacional de computador)

2. Equipe Conectiva.

Conectiva S.A.

Rua Tocantins, 89 - Cristo Rei - Curitiba - PR

CEP 80.050.430

http://www.conectiva.com.br

Índice

Lista de Tabelas

Lista de Figuras

Lista de Exemplos

Prefácio

A filosofia básica deste guia é apresentar os serviços mais importantes e essenciais, como as novidades que o Conectiva Linux traz para os administradores de rede e de sistemas. Numa linguagem rápida e fácil, o administrador pode ter uma visão geral de cada serviço, bem como uma explanação da teoria e conceitos dos programas que estão disponíveis no produto. O guia não visa ensinar cada programa ou pacote, pois na teoria poderia-se criar um novo livro para cada assunto. Além da descrição geral dos principais pacotes, o usuário pode observar exemplos da sua instalação e configuração.

O Linuxconf foi classificado como essencial ou importante em uma rede, porque já é um padrão da distribuição Conectiva Linux. Mas o que queremos salientar nessa versão do servidor são os novos módulos que foram desenvolvidos para ele. Antes de falar dos módulos vamos dar um pequeno conceito do Linuxconf que é um programa que centraliza as configurações de administração de sistema e de redes. Uma de suas vantagens é a interface bastante amigável, que satisfaz a maioria dos usuários; ele pode ser usado em modo gráfico, texto e até pode ser chamado via web. A Conectiva procurou implementar novos módulos no programa, como também melhorar os já existentes, deixando o Linuxconf ainda mais estável. Com uma equipe especializada e trabalhando somente neste projeto, foi implementado um módulo para a configuração da solução de *Boot* Remoto, Wine, um aumento de funcionalidades na configuração do Samba, DNS, NFS e muitos outros módulos que o próprio programa apresenta. Para fechar, a grande vantagem do Linuxconf é a implementação constante realizada pela equipe da Conectiva e também pela própria comunidade Linux. Acompanhe em

nosso site (http://www.conectiva.com.br/atualizacoes/) sua evolução e tenha sempre em sua máquina a última versão. O Linuxconf está descrito com mais detalhes no primeiro capítulo deste guia.

Dando continuidade ao guia, é apresentado o conceito e funcionamento de um servidor de LDAP. Este serviço é um protocolo cliente-servidor, utilizado para acessar um serviço de Diretório - uma base de dados que se assemelha a uma lista telefônica - que guarda toda a base de informações dos seus usuários. Uma facilidade interessante é que, usando o cliente Netscape® o usuário pode acessar todas as configurações de seu navegador remotamente.

É descrito o funcionamento do RAID, que é uma poderosa ferramenta para criar um subsistema de unidades de disco, rápido e confiável, através de unidades individuais. Sua função é proteger falhas no disco e não ser utilizado como um substituto para fazer *backup*. RAID é um serviço complexo que deve ser utilizado com cautela e por administradores experientes.

Apresentamos o bom e "velho" DNS. Este serviço, além de ser conhecido por muitos, é de suma importância para a configuração de uma rede. Neste capítulo é apresentada uma introdução do seu conceito básico e configuração.

Em Redes Mistas, é demonstrado o NFS e mais dois protocolos para o Linux trabalhar com outros sistemas operacionais - Samba e Mars-NWE. O NFS é um protocolo importante, dentro do Linux, para se fazer o compartilhamento de arquivos; já o Samba permite que máquinas Linux "conversem" com máquinas Windows e o Mars-NWE possibilita a comunicação de máquinas ou redes Linux com máquinas ou redes Novell. Esta parte do guia é bastante importante e interessante para aqueles que estão migrando para o Linux e ainda não podem abandonar definitivamente outros sistemas operacionais. O Linux vem mostrar aqui

que pode conviver amigavelmente com todos.

Buscamos criar uma seqüência de serviços para o administrador montar um servidor básico de Internet. Apresentamos o Apache para um servidor web, o WU-FTPD para um servidor de FTP e o Squid para um servidor de proxy. Com estes três serviços você já monta um servidor base para seu provedor Internet, por exemplo.

Dando continuidade, no capítulo - Correio Eletrônico - apresentamos o funcionamento do Sendmail para a configuração de um servidor de e-mail. Utilize esse capítulo para incrementar seu servidor.

Falamos de Segurança no Servidor, apresentando algumas regras para aumentar a segurança em sua rede e também descrevendo de uma maneira bem clara e objetiva o que um administrador deve fazer para desabilitar os serviços não utilizados. Este é o primeiro passo que um bom administrador deve dar, desabilitar o que não está sendo usado. Saber, conhecer a rede é um dos fatores mais importantes para oferecer um mínimo de segurança para sua rede; mesmo que o administrador não conheça conceitos de segurança, conhecer a rede já é um grande passo. Leia com atenção este capítulo para dar seu primeiro salto.

Para fechar a seção de capítulos, temos Alta Disponibilidade. Este capítulo objetiva a apresentação de conceitos e aplicações que possibilitam aumentar a disponibilidade de servidores Linux. Alta Disponibilidade vem mostrar que não é apenas mais um programa dentro de um produto, e sim, uma característica de um sistema computacional. O Conectiva Linux também vem abrindo as portas para essa filosofia.

No apêndice, temos um assunto importante: o *Appletalk*. Este apêndice do descreve o pacote *Netatalk* que vem no Conectiva Linux. Com ele você pode criar

redes mistas usando máquinas Macintosh® e Linux.

Para finalizar este guia, são apresentadas as licenças de uso gerais, a GPL e a licença de uso do produto.

Aproveite ao máximo seus conceitos e exemplos.

Convenções Tipográficas

Durante a confecção deste guia, procuramos descrever e formatar com uniformidade os vários termos utilizados. Segue abaixo as principais convenções utilizadas.

Tabela 1. Convenções deste Guia

Convenção	Descrição
Itálico	Palavras em inglês.
Opções de Menus e Submenus	Letra em tamanho maior que o corpo de texto; os submenus estão separados por setas.
Letra `courier (mais fina e espaçada)`	Definida para nomes de arquivos ou extensões de arquivos.

A *Conectiva* espera, com este material, fornecer uma base para aqueles que desejam implantar soluções avançadas em um servidor, utilizando uma plataforma Linux.

Se for encontrado algum erro ortográfico ou conceitual, por favor acesse o site (http://www.conectiva.com.br/doc/errata) e preencha o formulário adequado.

A *Conectiva* agradece o seu interesse neste produto e deseja boa sorte em seu empreendimento!

Capítulo 1. Linuxconf

Apresentaremos agora o Linuxconf para entender melhor o que acontece quando efetuamos qualquer alteração através dele, ou quando entramos e saímos do aplicativo. Em vez de explicar cada um dos módulos, examinaremos a habilitação e desabilitação deles e também conheceremos quais são os arquivos monitorados pelo Linuxconf.

Visão Geral

O Linuxconf é um sistema avançado de administração para o Linux. Ele centraliza tarefas como configuração do sistema e monitoração dos serviços existentes na máquina. Na verdade, o Linuxconf é um gerenciador de módulos, cada qual responsável por executar uma tarefa específica. Por exemplo, entre vários outros, existem módulos para:

- configuração do servidor Apache;
- configuração de conexões PPP;
- configuração de regras para o filtro de pacotes do kernel.

Tendo em vista a maneira como o Linuxconf foi projetado, para adicionar uma funcionalidade basta que alguém escreva um novo módulo para executar a tarefa. Com isto, temos uma ferramenta que pode centralizar a configuração de todo o sistema.

Uma das características de grande parte dos programas para Linux é que eles são muito flexíveis e têm dezenas (ou centenas) de opções de configuração. O Linuxconf facilita a configuração destes programas, apresentando as opções de configuração existentes de maneira organizada, muitas vezes fazendo também a validação dos dados informados, diminuindo a ocorrência de erros mais sérios.

> Quando você faz uma alteração através de um módulo e o finaliza, as modificações no sistema são efetuadas. Quando você sair do Linuxconf, serão feitas checagens para verificar se o estado atual do sistema corresponde com a configurações do Linuxconf.

Interfaces do Linuxconf

Ao contrário de várias outras ferramentas de administração, o Linuxconf tem várias interfaces de usuário:

Interface texto

Interface indispensável, pois pode ser utilizada a qualquer momento, seja via console ou via acesso remoto (telnet ou ssh). Esta interface elimina a necessidade de manter instalado um servidor gráfico X apenas para configurar a máquina. A Tabela 1-1 mostra alguns atalhos de teclado úteis para este modo do Linuxconf.

Tabela 1-1. Atalhos de Teclado para o Linuxconf

Teclas	Descrição
F1	abre tela de ajuda
F3	sai de uma seção/tela
Ctrl-X	mostra lista pop-up da opção
Ctrl-A	vai para o início da linha (**Home)**
Ctrl-B	volta à página anterior (**PageUp)**
Ctrl-D	apaga o caractere corrente (**Delete)**
Ctrl-E	vai para o final da linha (**End)**
Ctrl-F	vai para a página posterior (**PageDown)**
Ctrl-K	apaga o texto, do cursor ao final da linha

Interface *web*

A possibilidade de configurar uma máquina através de uma interface *web* é cômoda, pois basta ter acesso a um navegador. Com isto, é possível configurar uma máquina através de praticamente qualquer plataforma de *hardware* e *software*, bastando utilizar um navegador.

Interfaces gráficas

Interfaces amigáveis para usuários que preferem configurar o sistema através de uma interface gráfica, tendo à sua disposição janelas, caixas de diálogo, botões, etc. Estas interfaces devem ser executadas em um servidor gráfico X, como o XFree86 (servidor gráfico padrão do Linux).

Interface de linha de comando

Alguns módulos do Linuxconf podem ser utilizados via linha de comando, o que, entre outras possibilidades, permite a sua utilização em *scripts*.

Você poderá utilizar qualquer uma destas interfaces, dependendo apenas da sua necessidade ou do que há disponível na máquina que está sendo administrada.

Utilização do Linuxconf

O Linuxconf pode ser executado a qualquer momento, através da linha de comando. Para iniciá-lo, basta digitar **linuxconf** na linha de comando, ou clicar no ícone do ambiente gráfico do superusuário.

A configuração padrão do Conectiva Linux permite que apenas o superusuário acesse o Linuxconf. Esta política foi escolhida por questões de segurança. Para que outros usuários possam executá-lo é necessário que o programa tenha o bit *suid* habilitado.

Quando o Linuxconf é executado pela primeira vez ele exibe uma tela de apresentação, com algumas instruções de utilização do programa.

Ao ser iniciado, o Linuxconf verifica se a variável DISPLAY está configurada. Caso afirmativo, ele inicia sua interface gráfica, conforme mostra a Figura 1-1.

Figura 1-1. Interface Gráfica do Linuxconf

Como pode ser observado na Figura 1-1, o Linuxconf tem três seções: Configura-

ção, Controle e Estado. A seção *Configuração* trata basicamente de configurações do sistema e a seção *Estado* permite a visualização de *logs* e informações gerais do sistema. Como o objetivo deste capítulo é entender o funcionamento do Linuxconf, nos deteremos na seção *Controle*, a qual nos permite visualizar e modificar os padrões do Linuxconf.

Para utilizar a interface texto do Linuxconf, basta executá-lo no modo texto, ou então adicionar a opção `--text` na linha de comando: **linuxconf --text**.

A Figura 1-2 ilustra o Linuxconf sendo executado num XTerm.

Figura 1-2. Executando o Linuxconf em um XTerm

Note que as informações apresentadas na interface texto são as mesmas apresentadas na interface gráfica, sendo que apenas a forma de apresentação difere entre as duas interfaces.

A interface *web* pode ser acessada através da URL *http://sua_maquina:98/*, mas para isto você deve primeiramente configurar o Linuxconf para que ele aceite conexões via rede.

Habilitando o Acesso ao Linuxconf Via Rede

O primeiro passo para habilitar o acesso ao Linuxconf através da rede é ir até o menu Configuração→Ambiente de Rede → Diversos → Acesso ao Configurador Linux via rede e marcar a opção *ativa acesso via rede*.

Além desta opção é útil marcar também a opção *Acesso de registro* no arquivo `/var/log/htmlaccess.log`, para que os acessos fiquem registrados neste arquivo. Logo abaixo destas opções, você encontra alguns campos para definir quais máquinas podem acessar o Linuxconf via rede. Se estes não forem preenchidos, o Linuxconf aceitará apenas conexões da rede local da primeira placa de rede detectado pelo sistema, o que é considerado um funcionamento razoavelmente seguro.

Se você prefere ser mais específico, informe uma máquina ou uma rede e opcionalmente uma máscara de rede. Suas opções para especificar uma máquina ou uma rede são:

- um nome de máquina;
- um endereço IP;
- um par de endereço IP e máscara de rede;
- um nome de dispositivo (*eth0*, *eth1*, etc).

Observe o exemplo da Figura 1-3:

Figura 1-3. Configuração do Acesso ao Linuxconf Via Rede

Com esta configuração será possível acessar a interface *web* do Linuxconf através da interface *loopback* (127.0.0.1), da rede *192.168.0.0/255.255.255.0* e da máquina *host.qwerty.com*. Quando é especificado um endereço IP ou um nome de máquina, sem especificar uma máscara de rede, é assumida por padrão a seguinte máscara: *255.255.255.255*.

Como esta interface do Linuxconf roda através do inetd, é necessário verificar se ele está habilitado. Este procedimento pode ser efetuado através da caixa de diálogo Controle → Painel de Controle → Controle de atividade dos serviços. Nesta caixa de diálogo procure pelo serviço *linuxconf*, o qual deverá estar marcado como Inativo, como ilustrado na Figura 1-4.

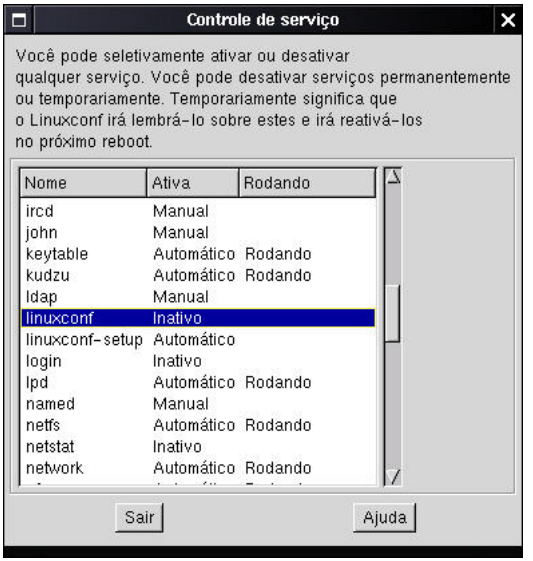


Figura 1-4. Listagem dos Serviços

Ao selecionar esta opção, será apresentada uma caixa de diálogo de configuração do serviço. Por enquanto preocupe-se apenas em ativar o serviço, marcando *Estado* como *Ativo* (veja Figura 1-5).

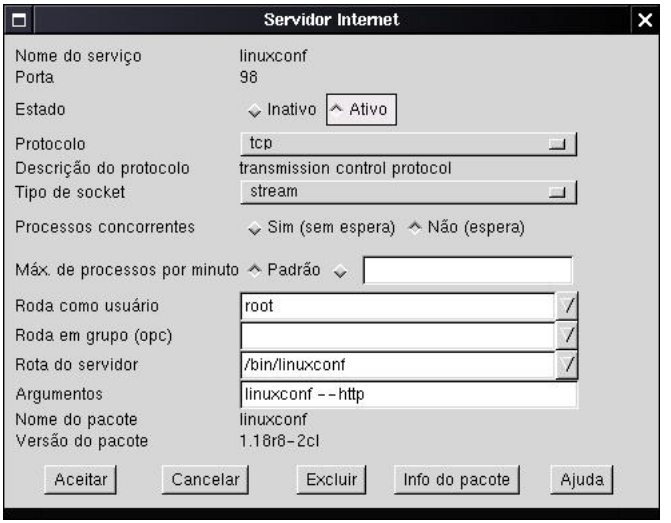


Figura 1-5. Ativando o Serviço Linuxconf

O passo seguinte é sair do Linuxconf e escolher a opção *Ativar as mudanças*, para que estas alterações sejam efetivadas.

Se o serviço inet não estiver inicializado, como superusuário inicie com os comandos:

```
# cds
atalk   functions  inet             lpd       nfs         sendmail  xfs
atd     gated      keytable         mars-nwe  nfslock     single    ypbind
```

```
crond  gpm        killall          mon       pcmcia      smb
cups   halt       kudzu            named     portmap     snmpd
dhcpd  heartbeat  ldirectord       netfs     postgresql  sshd
drbd   httpd      linuxconf-setup  network   random      syslog
# ./inet start
Iniciando os serviços INET:                                [  OK  ]
```

Finalmente, para acessar o Linuxconf através de sua interface *web*, basta apontar seu navegador para http://127.0.0.1:98/, isto é, se você estiver acessando da máquina local. Se estiver acessando da rede, substitua *127.0.0.1* pelo nome ou endereço IP da máquina.

A Figura 1-6 mostra uma página da interface *web* do Linuxconf.

Figura 1-6. Interface *Web* do Linuxconf

Ajuda do Linuxconf

O Linuxconf tem várias telas de ajuda que lhe explicam como utilizar algumas das características do programa. Para acessá-las basta selecionar a opção *Ajuda*, existente em todas as telas do programa.

> Como o Linuxconf é um projeto em andamento, algumas telas de ajuda ainda não foram traduzidas para a língua portuguesa, e outras não foram nem mesmo escritas. Portanto, não se preocupe caso apareça alguma tela de ajuda em inglês, ou se aparecer alguma mensagem dizendo que o arquivo de ajuda não existe.

Efetivar as Configurações

Um dos primeiros pontos a conhecer do Linuxconf, é que muitas das configurações realizadas através dele, somente terão efeito quando explicitamente efetivadas. Existem várias maneiras para efetivar estas mudanças. Uma delas é saindo do Linuxconf. Ao sair do programa, após ter efetuado alguma modificação em configurações, você verá uma tela semelhante à ilustrada na Figura 1-7.

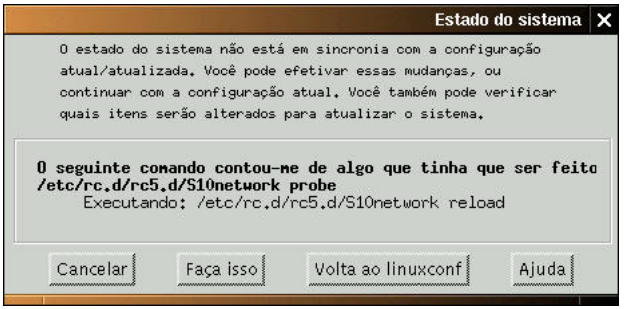


Figura 1-7. Estado do sistema

> A não ser quando explicitamente indicado, as telas e os procedimentos descritos neste capítulo são baseados na interface gráfica do Linuxconf. A diferença de operação entre uma interface e outra é mínima, portanto você não terá problemas em utilizar quaisquer das outras interfaces.

A janela apresenta um relatório (Figura 1-7) do que será executado, no caso de você desejar que as configurações sejam feitas.

Se você desistir de sair do programa, basta selecionar a opção *Volta ao linuxconf*, o que fará com que você volte à tela principal do Linuxconf. A opção *Cancelar* permite que você saia do programa sem efetuar as alterações, ao contrário da opção *Faça isso*, através da qual você sai do programa efetivando todas as alterações necessárias.

Uma outra maneira de ativar as mudanças na configuração do sistema é através da opção Controle → Painel de Controle → Ativar a configuração.

Se você costuma utilizar a linha de comando, existem dois comandos úteis. O comando **linuxconf *--status*** exibe o relatório do que precisa ser feito para sincronizar a configuração do sistema, e o comando **linuxconf *--update*** efetua as alterações, como ilustrado a seguir.

```
# linuxconf -status
Lista de pré-requisitos para ativar a configuração atual

# linuxconf -update
Checando configuração básica
  Checando os módulos do kernel
  Montando volumes locais
  Checando permissões de arquivos
  Checando o LILO
  Executando alguns scripts de inicialização Sysv
  Configuração do firewall
```

Ativando ou Desativando Módulos

O Linuxconf é composto por vários módulos, cada um com uma função específica. É possível desativar módulos desnecessários ou ativar os existentes para utilização. Acessando Controle → Arquivos de controle e sistemas → Configurar os módulos do Linuxconf você terá acesso à *Lista de módulos* (Figura 1-8). Esta lista mostra os módulos existentes, sua descrição e uma *checkbox* que informa se o módulo está ativo. Para confirmar qualquer alteração nesta tela clique em Aceitar.

Figura 1-8. Lista de Módulos do Linuxconf

Permissão e Propriedade de Arquivos

O Linuxconf mantém uma base de dados com permissões e propriedades de arquivos e diretórios importantes do sistema, evitando assim que estas caracterísi-

cas sejam acidentalmente alteradas.

Por exemplo, se você alterar o modo do diretório `/var/spool/mail` para *777*, ao ativar as configurações o Linuxconf irá configurá-lo novamente com o modo *775*, como ilustrado na Figura 1-9.

Em algumas situações, é possível que você necessite alterar permanentemente o modo (ou dono ou grupo) de um arquivo administrado pelo Linuxconf. Neste caso, é necessário alterar as informações do arquivo armazenadas no menu Controle → Arquivos de controle e sistemas → Configurar permissões e propriedades de arquivos. Ao acessar esta opção, será apresentada uma caixa de diálogo (Figura 1-10) na qual você poderá informar um prefixo para filtrar quais arquivos serão listados, já que a lista é bastante grande. Se você não colocar um prefixo, a listagem completa será exibida. A listagem, filtrada ou não, será exibida assim que você clicar no botão Aceitar.

A Figura 1-11 mostra uma listagem dos arquivos do diretório `/usr` que são administrados pelo Linuxconf.

Figura 1-11. Permissão de Arquivos Controlados pelo Linuxconf

Esta caixa de diálogo tem cinco colunas de informação:

Rota: exibe o caminho completo para o arquivo ou diretório.

Tipo: informa se é arquivo, diretório, dispositivo caractere ou dispositivo bloco.

Dono: exibe o dono e o grupo *padrão* do arquivo.

Permissões: informa as permissões *padrão* do arquivo.

Mod: informa se a configuração padrão do arquivo foi modificada.

Ao selecionar um dos arquivos da lista será apresentada uma outra caixa de diálogo, a qual permitirá que você altere as configurações padrão do arquivo. Você poderá alterar o *dono*, o *grupo* e as *permissões*.

Observe na Figura 1-11 que o arquivo `/usr/sbin/pppd` tem permissões `rwsr-xr-x`. Você pode querer, por exemplo, desabilitar o bit *suid* deste programa. Para isto, desmarque a opção *Indicador de Setuid* na caixa de diálogo de definições de permissões deste arquivo (Figura 1-12).

Figura 1-12. Definições de Permissões de um Arquivo

Na próxima vez que você *ativar as configurações*, esta alteração será automaticamente efetuada. Este tipo de alteração pode ser feita para qualquer arquivo controlado pelo Linuxconf.

> Sempre que você precisar alterar dono, grupo ou permissões de um arquivo controlado pelo Linuxconf será necessário modificar a configuração do arquivo neste programa.

Arquivos de Configuração

O Linuxconf faz o gerenciamento, teste, gera e utiliza vários arquivos de configuração. Através da opção Controle → Arquivos de controle e sistemas → Configurar todos os arquivos de configuração (Figura 1-13) você pode

visualizar quais são estes arquivos.

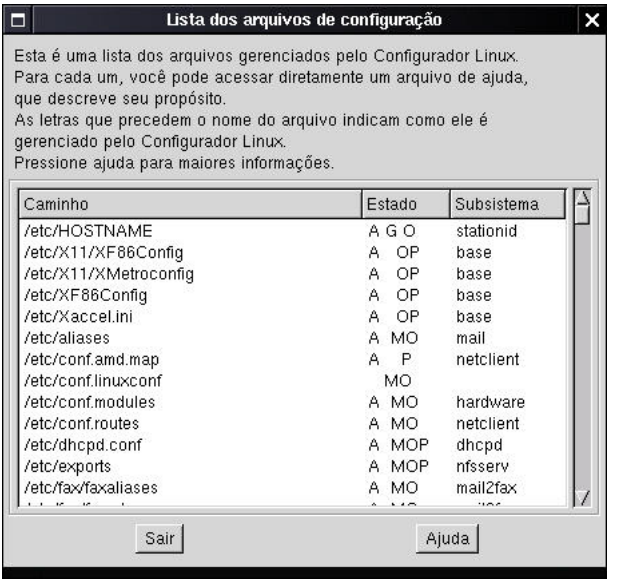


Figura 1-13. Lista dos Arquivos de Configuração

Como você pode observar, esta janela contém três colunas: *Caminho*, *Estado* e *Subsistema*.

O *Caminho* define a localização do arquivo gerenciado. A coluna *Estado* contém alguns identificadores, os quais podem ter os seguintes valores:

(em branco): indica que o arquivo é apenas lido pelo Linuxconf. Isso pode significar duas coisas: ou é um arquivo de referência usado pelo Linuxconf ou ele ainda não sabe como gerenciá-lo, mas utiliza seu conteúdo.

E: indica que o arquivo será sempre apagado pelo Linuxconf na inicialização.

G: indica que o arquivo é gerado pelo Linuxconf. Neste caso, o Linuxconf utiliza outros arquivos, como por exemplo o `/etc/conf.linuxconf`, para guardar a configuração relacionada a este serviço. Em geral significa que estes arquivos não devem ser alterados manualmente, pois o Linuxconf sobrescreverá estas alterações. Uma exceção a este caso é quando o arquivo também é marcado com *M*, o que é incomum.

M: indica que o arquivo é completamente gerenciado pelo Linuxconf. Isto significa que o Linuxconf sabe como processá-lo e reescrevê-lo apropriadamente. Também significa que você pode editar o arquivo diretamente, sem que o Linuxconf perca a habilidade de gerenciá-lo. O arquivo `/etc/resolv.conf` é um exemplo.

O: indica que o arquivo é opcional em um sistema Linux.

P: indica que o Linuxconf sabe muito pouco do arquivo em questão. Ele apenas testa sua existência e sua data de modificação. Baseado nisto, o Linuxconf decide se um serviço é necessário ou se um *daemon* precisa ser reiniciado ou sinalizado.

V: o Linuxconf utiliza arquivos virtuais especiais, os quais geralmente são partes de um arquivo de configuração real.

***:** indica que a rota do arquivo de configuração foi alterada, deixando de ter o valor original conhecido pelo Linuxconf.

A coluna *Subsistema* apenas apresenta uma divisão interna do Linuxconf, que informa a que parte do sistema pertence o arquivo.

A única configuração que pode ser feita nesta janela é a alteração da rota do arquivo, o que não é recomendado a não ser que você tenha certeza do que está fazendo.

Comandos e Programas Residentes

O Linuxconf utiliza vários comandos e programas do sistema para realizar diversas tarefas. Você pode saber quais são eles acessando Controle → Arquivos de controle e sistemas → Configurar todos os comandos e programas residentes (Figura 1-14). Além de visualizá-los, você pode fazer alterações e até mesmo torná-los inativos, como veremos a seguir.

Figura 1-14. Listagem de Comandos e Programas Residentes

Como você pode observar, a janela ilustrada na Figura 1-14 tem três colunas:

Nome: informa o nome do comando.

Caminho: informa a localização do comando que está sendo utilizado.

Mod: informa se a configuração original do Linuxconf foi modificada.

Esta característica é bastante útil, pois permite que você personalize algumas funções do Linuxconf de maneira simples. Por exemplo, se você precisa adicionar usuários na base de dados do sistema *e* ainda numa base de dados SQL, basta substituir o comando originalmente utilizado pelo Linuxconf por um *script* ou programa especialmente criado para isto.

Ao selecionar um dos comandos da lista, será exibida uma janela que permitirá a você:

- Desabilitar o comando, desmarcando a opção *o Configurador Linux pode operá-lo*.
- Modificar o comando que será executado, alterando o *Caminho do comando*.
- Adicionar, remover ou modificar os argumentos utilizados na execução do comando.

A Figura 1-15 ilustra uma situação na qual foi alterado o comando para adição de usuários no sistema.

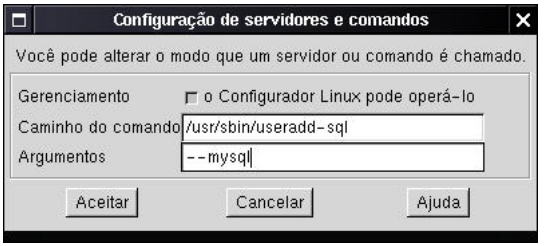


Figura 1-15. Alteração de Configuração de Comando

Com esta configuração, o comando utilizado pelo Linuxconf para adicionar usuários no sistema passa a ser `/usr/sbin/useradd-sql`, que poderá ser um *script* ou um programa binário que executa a tarefa de adicionar usuários de maneira personalizada. Note que este procedimento *não* vai modificar o módulo de adição de usuários do Linuxconf. A diferença é que o comando utilizado pelo módulo será outro.

Se você desativar um comando, desmarcando a opção *o Configurador Linux pode operá-lo*, o Linuxconf estará impedido de efetuar qualquer tarefa que dependa deste comando.

Estes procedimentos são válidos para quaisquer dos comandos utilizados pelo Linuxconf.

Controle de atividade dos serviços

O *Controle de atividade dos serviços* do Linuxconf serve basicamente para configurar o inetd. De todos os serviços controlados, apenas aquele chamado *firewall* não é um serviço executado através do inetd.

Esta configuração pode ser acessada através da opção Controle → Painel de controle → Controle de atividade dos serviços (Figura 1-4). Observe que esta janela foi apresentada quando demonstramos como habilitar o acesso ao Linuxconf via rede.

Para modificar a configuração de um serviço você deve primeiramente clicar sobre ele. Este procedimento fará com que seja exibida uma outra janela, a qual permite que você efetue as modificações que desejar. A Figura 1-16 ilustra as configurações do serviço *linuxconf*. Para ativar ou desativar um serviço basta modificar *Estado* para *Ativo* ou *Inativo*, respectivamente.

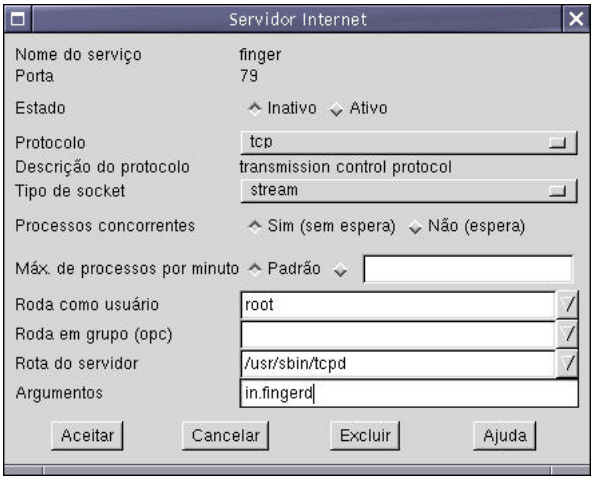


Figura 1-16. Configuração do Serviço *finger*

Mais Funcionalidades do Linuxconf

Neste capítulo, enfocamos a configuração do Linuxconf. Nos demais capítulos deste livro você conhecerá vários módulos que lhe permitirão gerenciar sua máquina de uma maneira bem simples e segura.

Novos módulos foram acrescidos a esta versão do Linuxconf; dentre eles podemos citar:

- Módulo para configuração do Wine, aplicativo para executar programas do Windows®.
- Módulo para configuração do Amanda, software para gerenciamento de backup.
- Módulo para configuração do Grub, boot *loader* com mais características que o LILO.
- Módulo para configuração do Postfix, servidor de e-mail.
- Módulo para configuração do Portslave, aplicativo usado para controle de portas.
- Módulo para configuração do LPRng, software para configuração e controle de impressoras.

logs do Linuxconf

É importante sempre ter como referência os logs do sistema antes, durante e depois do uso do Linuxconf. Estes arquivos podem ser sempre consultados em `/var/log`.

Podemos citar os seguintes arquivos que dizem respeito apenas ao uso do Linuxconf:

- `/var/log/netconf.log` - arquivo principal de log do Linuxconf, registra operações de forma clara e bem específica de todos os passos executados pelo Linuxconf.

- `/var/log/htmlaccess.log` - log de acesso do Linuxconf via WEB; se for utilizada esta interface use este arquivo como referência.

Capítulo 2. LVM

O Gerenciador de Volumes Lógicos[1](LVM) é um subsistema para gerenciamento ativo de armazenagem em disco que se transformou em um padrão para gerenciamento de armazenagem em sistemas UNIX.

O Gerenciador de Volumes Lógicos consiste em uma camada adicional entre os dispositivos físicos e a interface de E/S no kernel para fornecer uma visão lógica no armazenamento. Ao contrário dos esquemas de particionamento atuais onde discos são divididos em partições contínuas de tamanho fixo, o LVM permite ao usuário considerar discos, também conhecidos como Volumes Físicos[2] (PV), como um volume de armazenamento de dados, consistindo de extensões de tamanhos iguais.

Um sistema de LVM compõe-se de grupos arbitrários de volumes físicos, organizados em Grupos de Volumes[3](VG). Um grupo de volume pode consistir de um ou mais volumes físicos. Pode haver mais de um grupo de volume no sistema. Uma vez criado, o grupo de volume, e não o disco, é a unidade básica de armazenamento de dados (um disco virtual compondo-se de um ou mais discos físicos).

---

1. Logical Volume Manager

2. Physical Volumes

3. Volume Groups

A quantidade de espaço em disco, que é representada por um grupo de volume, pode ser alocada em partições virtuais, chamadas de Volumes Lógicos[4] (LV) de vários tamanhos. Um volume lógico pode conter um número de volumes físicos ou representar apenas uma porção de um volume físico. O tamanho de um volume lógico é determinado pelo seu número de extensões. Uma vez criados, volumes lógicos podem ser utilizados como partições de disco regulares - para criar um sistema de arquivos ou um dispositivo de troca.

O LVM foi inicialmente desenvolvido pela IBM e depois adotado pela OSF (agora OpenGroup (http://www.opengroup.org/)) para o seu sistema operacional OSF/1. A versão OSF então foi usada como uma base para implementação de LVM nos sistemas operacionais HP-UX e Digital UNIX. Outra implementação de LVM é disponibilizada pela Veritas (http://www.veritas.com) que funciona de uma forma diferente. A implementação do Linux é similar à implementação de LVM do HP-UX.

O conceito de LVM

Tradicionalmente, o tamanho de uma partição é definido na instalação do sistema, não podendo ser alterado posteriormente. O redimensionamento de partições estáticas pode ser realizado com o aplicativo partd. Isso requer que o administrador faça um planejamento prévio da quantidade máxima de dados que a partição poderá vir a armazenar no futuro. Quando um usuário exceder o espaço de uma

4. Logical Volumes

partição, ele terá de reparticionar (o que pode envolver uma reinstalação completa do sistema) ou se utilizar de artifícios, como as ligações simbólicas.

Por exemplo, suponha que temos um disco de 1GB e criamos a partição `/home` utilizando 600MB. Imagine que necessitamos de mais espaço e se descubra que iremos precisar de 1GB no `/home`. Utilizando a antiga noção de partições, precisaremos ter outra unidade de pelo menos 1GB de tamanho. Então poderemos adicionar o disco, criar o novo `/home` e copiar os dados existentes para ele.

Entretanto, com uma configuração LVM, podemos simplesmente adicionar um disco de 400MB (ou maior) e adicionar esta unidade de armazenamento na partição `/home`. Outras ferramentas permitem redimensionar um sistema de arquivos existente, ou seja, podemos simplesmente redimensioná-lo para ter a vantagem de uma partição de tamanho maior e para voltarmos ao trabalho.

Terminologia

O LVM vem com vários jargões que precisam ser entendidos para não haver problemas com os sistemas de arquivos. Nesta seção veremos estes terminologia utilizada pelo LVM.

A mídia física

Você deve usar a palavra *física* com um pouco de cuidado; de qualquer forma nós iremos entender inicialmente como sendo um simples disco rígido, ou uma partição. Por exemplo, `/dev/hda`, `/dev/hda2`, `/dev/sda`. Nós podemos transformar qualquer número consecutivo de blocos de um dispositivo de blocos em um Volume Físico.

Volume Físico (PV)

Um PV[5] não é nada mais que um meio físico com alguns dados administrativos adicionados a ele - uma vez que tenhamos adicionado estes dados o LVM irá reconhecê-los como proprietários das Extensões Físicas.

Extensões Físicas (PE)

Extensões Físicas[6] são como blocos de um sistema de arquivos (regiões contínuas do disco) realmente grandes, muitas vezes com um tamanho na casa dos

5. Physical Volume

6. Physical Extents

megabytes. PEs podem ser atribuídas a um Grupo de Volumes.

Grupo de Volumes (VG)

Um VG[7] é composto por um determinado número de Extensões Físicas. Deste Grupo de volumes, PEs podem ser atribuídas a um Volume Lógico.

Volume Lógico (LV)

Um Volume Lógico é o resultado final do nosso trabalho, é aqui que as informações são armazenadas. Ele é um dispositivo de bloco funcionalmente equivalente a uma partição.

É sobre o Volume Lógico que será criado um sistema de arquivos.

7. Volume Group

Sistema de Arquivos

O sistema de arquivos pode ser o que desejarmos: o ext2 padrão, ReiserFS, etc... Para o usuário, não há diferença entre uma partição regular e um Volume Lógico.

Seguem alguns diagramas que ajudarão a visualizar estes conceitos.

Um Volume Físico, contendo Extensões Físicas. Figura 2-1.

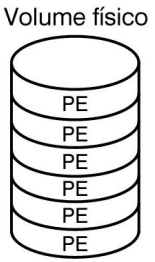


Figura 2-1. Volume Físico

Um Grupo de Volumes, contendo dois Volumes Físicos (PVs) com seis Extensões Físicas. Figura 2-2.

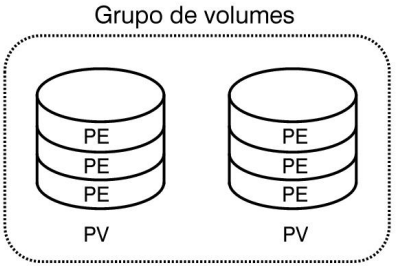


Figura 2-2. Grupo de Volumes

Agora nós podemos expandir este grupo. Figura 2-3.

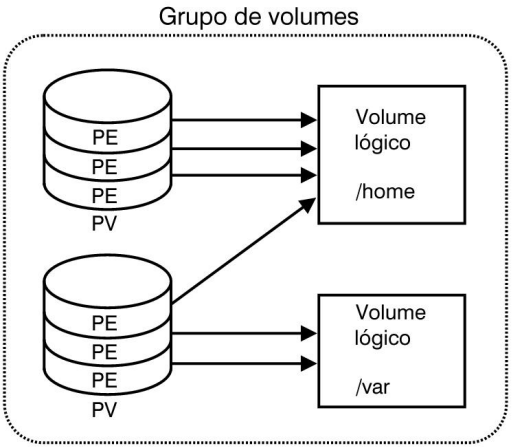


Figura 2-3. Grupo de Volumes expandido

Isto nos mostra dois sistemas de arquivos, dividindo dois discos. O sistema de arquivos `/home` contém quatro Extensões Físicas, o sistema de arquivos `/var` duas.

Criando um Volume Lógico

Apresentaremos aqui um exemplo comentado mostrando o processo para a criação de um Volume Lógico. Utilizaremos duas partições em um mesmo disco para este exemplo, `/dev/hda5` e `/dev/hda6` com 2GB e 1GB respectivamente. O

uso de LVM faz mais sentido com partições em discos diferentes, porém aqui, somente para fins didáticos, apresentaremos em um mesmo disco, sendo estas mesmas regras aplicáveis a vários discos. Os dados destas partições serão perdidos.

Observe as figuras mostradas anteriormente em caso de dúvida.

Primeiramente mudaremos os tipo das partições `/dev/hda5` e `/dev/hda6` para 0x8e.

```
# fdisk /dev/hda


Comando (m para ajuda): p


Disco /dev/hda: 255 cabeças, 63 setores, 784 cilindros
Unidades = cilindros de 16065 * 512 bytes


Dispositivo Boot    Início      Fim    Blocos   Id  Sistema
/dev/hda1             1        17    136521   82  Linux swap
/dev/hda2   *        18       272   2048287+  83  Linux
/dev/hda3           273       400   1028160   83  Linux
/dev/hda4           401       784   3084480    5  Estendida
/dev/hda5           401       655   2048256   83  Linux
/dev/hda6           656       783   1028128+  83  Linux
/dev/hda7           784       784      8001   82  Linux swap
```

```
Comando (m para ajuda): t
Número da partição (1-7): 5
Código hexadecimal (digite L para listar os códigos): 8e
O tipo da partição 5 foi alterado para 8e (Linux LVM)

Comando (m para ajuda): p

Disco /dev/hda: 255 cabeças, 63 setores, 784 cilindros
Unidades = cilindros de 16065 * 512 bytes

Dispositivo Boot    Início      Fim    Blocos   Id  Sistema
/dev/hda1             1        17    136521   82  Linux swap
/dev/hda2   *        18       272   2048287+  83  Linux
/dev/hda3           273       400   1028160   83  Linux
/dev/hda4           401       784   3084480    5  Estendida
/dev/hda5           401       655   2048256   8e  Linux LVM
/dev/hda6           656       783   1028128+  83  Linux
/dev/hda7           784       784      8001   82  Linux swap

Comando (m para ajuda): t
Número da partição (1-7): 6
Código hexadecimal (digite L para listar os códigos): 8e
```

```
O tipo da partição 6 foi alterado para 8e (Linux LVM)

Comando (m para ajuda): p

Disco /dev/hda: 255 cabeças, 63 setores, 784 cilindros
Unidades = cilindros de 16065 * 512 bytes

Dispositivo Boot    Início      Fim    Blocos   Id  Sistema
/dev/hda1             1        17    136521   82  Linux swap
/dev/hda2   *        18       272   2048287+  83  Linux
/dev/hda3           273       400   1028160   83  Linux
/dev/hda4           401       784   3084480    5  Estendida
/dev/hda5           401       655   2048256   8e  Linux LVM
/dev/hda6           656       783   1028128+  8e  Linux LVM
/dev/hda7           784       784      8001   82  Linux swap

Comando (m para ajuda): w
A tabela de partições foi alterada!

Chamando ioctl() para reler tabela de partições.

Sincronizando discos.
```

Caso o pacote do LVM não esteja instalado no seu sistema, instale-o com o comando:

```
# rpm -ivh /mnt/cdrom/conectiva/RPMS/lvm*
```

Carregue o módulo do LVM:

```
# insmod lvm-mod
Using /lib/modules/2.2.16-17cl/block/lvm-mod.o
```

Para criar o arquivo `/etc/lvmtab` vazio, execute o comando:

```
# vgscan
vgscan - reading all physical volumes (this may take a while...)
vgscan - "/etc/lvmtab" and "/etc/lvmtab.d" successfully created
```

Agora podemos criar os Volumes Físicos utilizando o comando **pvcreate `partição`** desta forma:

```
# pvcreate /dev/hda5
pvcreate - reinitializing physical volume
pvcreate - physical volume "/dev/hda5" successfully created

# pvcreate /dev/hda6
pvcreate - reinitializing physical volume
```

```
pvcreate - physical volume "/dev/hda6" successfully created
```

Nós podemos adicionar este dois PVs a um Grupo de Volumes chamado *test* com o comando **vgcreate *nome_do_VG partição1 partição2***:

```
# vgcreate test /dev/hda5 /dev/hda6
vgcreate - INFO: using default physical extent size 4 MB
vgcreate - INFO: maximum logical volume size is 255.99 Gigabyte
vgcreate - doing automatic backup of volume group "test"
vgcreate - volume group "test" successfully created and activated
```

Para criar o arquivo `/etc/lvmtab`, execute o comando:

```
# vgscan
vgscan - reading all physical volumes (this may take a while...)
vgscan - found active volume group "test"
vgscan - "/etc/lvmtab" and "/etc/lvmtab.d" successfully created
vgscan - WARNING: you may not have an actual VGDA backup of your volume group
```

Caso os Grupos de Volumes estejam inativos, utilize o comando **vgchange** com o parâmetro *-ay* para ativar todos os VGs disponíveis:

```
# vgchange -ay
```

```
vgchange - volume group "test" successfully activated
```

Agora temos um Grupo de Volumes vazio; vamos visualizá-lo com o comando **vgdisplay *-verbose nome_do_VG***:

```
# vgdisplay -v test
-- Volume group --
VG Name               test
VG Access             read/write
VG Status             available/resizable
VG #                  0
MAX LV                256
Cur LV                0
Open LV               0
MAX LV Size           255.99 GB
Max PV                256
Cur PV                2
Act PV                2
VG Size               2.93 GB
PE Size               4 MB
Total PE              750
Alloc PE / Size       0 / 0
Free  PE / Size       750 / 2.93 GB
```

```
-- No logical volumes defined in test --


-- Physical volumes --
PV Name (#)           /dev/hda5 (1)
PV Status             available / allocatable
Total PE / Free PE    500 / 500

PV Name (#)           /dev/hda6 (2)
PV Status             available / allocatable
Total PE / Free PE    250 / 250
```

Podemos observar que não há Volumes Lógicos definidos; devemos criar um para poder utilizá-lo. Também podemos ver com este comando o estado dos PVs, seus nomes e o número total de blocos alocados e disponíveis. Vamos gerar um volume de 500MB chamado *lv01* no Grupo de Volumes *test*:

```
# lvcreate -L 500M -n lv01 test
lvcreate - doing automatic backup of "test"
lvcreate - logical volume "/dev/teste/lv01" successfully created
```

Vamos criar um sistema de arquivos do tipo ext2, agora:

```
# mke2fs /dev/test/lv01
mke2fs 1.19, 13-Jul-2000 for EXT2 FS 0.5b, 95/08/09
Filesystem label=
OS type: Linux
Block size=1024 (log=0)
Fragment size=1024 (log=0)
128016 inodes, 512000 blocks
25600 blocks (5.00%) reserved for the super user
First data block=1
63 block groups
8192 blocks per group, 8192 fragments per group
2032 inodes per group
Superblock backups stored on blocks:
        8193, 24577, 40961, 57345, 73729, 204801, 221185, 401409

Writing inode tables: done
Writing superblocks and filesystem accounting information: done
```

Podemos criar um diretório para montar este sistema de arquivos e observar o seu tamanho:

```
# mkdir /mnt/lvm
# mount /dev/test/lv01 /mnt/lvm
```

```
# df -h /dev/test/lv01
Filesystem            Size  Used Avail Use% Mounted on
/dev/test/lv01        484M   13k  459M   0% /mnt/lvm
```

Vamos ver novamente o Grupo de Volumes e observar as mudanças:

```
# vgdisplay -v test
-- Volume group --
VG Name               teste
VG Access             read/write
VG Status             available/resizable
VG #                  0
MAX LV                256
Cur LV                1
Open LV               1
MAX LV Size           255.99 GB
Max PV                256
Cur PV                2
Act PV                2
VG Size               2.93 GB
PE Size               4 MB
Total PE              750
Alloc PE / Size       125 / 500 MB
```

```
Free  PE / Size       625 / 2.44 GB

-- Logical volume --
LV Name                /dev/test/lv01
VG Name                teste
LV Write Access        read/write
LV Status              available
LV #                   1
# open                 1
LV Size                500 MB
Current LE             125
Allocated LE           125
Allocation             next free
Read ahead sectors     120
Block device           58:0


-- Physical volumes --
PV Name (#)            /dev/hda5 (1)
PV Status              available / allocatable
Total PE / Free PE     500 / 375
```

```
PV Name (#)           /dev/hda6 (2)
PV Status             available / allocatable
Total PE / Free PE    250 / 250
```

Temos todas as informações do VG na saída deste comando, seu nome, tipo de acesso, estado atual, parâmetros do LV e PV e tamanhos totais e alocados do PE. O `/dev/hda6` está totalmente livre, enquanto que o `/dev/hda5` está com 125 Extensões Físicas em uso.

Redimensionando um Volume Lógico

Examinaremos passo a passo o processo de redimensionamento para uma visão geral da operação.

Aumentando um Volume Lógico

O pré-requisito para esta operação é ter espaço livre no Grupo de Volumes. Caso contrário teríamos de adicionar mais PVs. A seguinte linha de comando faz esta

operação:

```
# lvextend -L+2000M /dev/test/lv01
lvextend - extending logical volume "/dev/test/lv01" to 2.44 GB
lvextend - doing automatic backup of volume group "test"
lvextend - logical volume "/dev/test/lv01" successfully extended
```

Aumentamos com esta operação o Volume Lógico `/dev/test/lv01` em 2000MB. Note que ainda não redimensionamos o sistema de arquivos, portanto:

```
# df -h /dev/test/lv01
Filesystem            Size  Used Avail Use% Mounted on
/dev/test/lv01        484M   13k  459M   0% /mnt/lvm
```

A partição ainda apresenta o seu tamanho original.

Aumentando um sistema de arquivos

Primeiramente vamos desmontar o nosso sistema de arquivos:

```
# umount /mnt/lvm
```

Antes de redimensioná-lo force a verificação do sistema de arquivos com o **e2fsck**:

```
# e2fsck -f /dev/test/lv01
e2fsck 1.19, 13-Jul-2000 for EXT2 FS 0.5b, 95/08/09
Pass 1: Checking inodes, blocks, and sizes
Pass 2: Checking directory structure
Pass 3: Checking directory connectivity
Pass 4: Checking reference counts
Pass 5: Checking group summary information
/dev/test/lv01: 11/128016 files (0.0% non-contiguous), 16169/512000 blocks
```

Agora sim podemos redimensionar o sistema de arquivos com a ferramenta **resize2fs**:

```
# resize2fs /dev/test/lv01
resize2fs 1.19 (13-Jul-2000)
The filesystem on /dev/test/lv01 is now 2560000 blocks long.
```

Você também poderá utilizar o comando resize_reiserfs para redimensionar sistemas de arquivos ReiserFS.

Já podemos montar novamente o sistema de arquivos e verificar seu novo tamanho:

```
# mount /dev/test/lv01 /mnt/lvm/
[root@toy /root]# df -h /dev/test/lv01
```

```
Filesystem            Size  Used Avail Use% Mounted on
/dev/test/lv01        2.4G   13k  2.2G   0% /mnt/lvm
```

Diminuindo um sistema de arquivos

Vamos agora diminuir o sistema de arquivos, para depois podermos diminuir também o Volume Lógico.

Primeiramente desmonte o sistema de arquivos:

```
# umount /mnt/lvm/
```

Force a verificação do sistema de arquivos com o comando:

```
# e2fsck -f /dev/test/lv01
e2fsck 1.19, 13-Jul-2000 for EXT2 FS 0.5b, 95/08/09
Pass 1: Checking inodes, blocks, and sizes
Pass 2: Checking directory structure
Pass 3: Checking directory connectivity
Pass 4: Checking reference counts
Pass 5: Checking group summary information
```

```
/dev/test/lv01: 11/636016 files (9.1% non-contiguous), 80274/2560000 blocks
```

Redimensione o sistema de arquivos para 500 mil blocos (500MB aproximadamente); por exemplo:

```
# resize2fs /dev/test/lv01 500000
resize2fs 1.19 (13-Jul-2000)
The filesystem on /dev/test/lv01 is now 500000 blocks long.
```

Diminuindo um Volume Lógico

De uma forma similar ao comando que foi usado para aumentar o Volume Lógico, agora porém com um valor negativo, podemos diminuí-lo:

```
# lvreduce -L-2000M /dev/test/lv01
lvreduce - WARNING: reducing active logical volume to 500 MB
lvreduce - THIS MAY DESTROY YOUR DATA (filesystem etc.)
lvreduce - do you really want to reduce "/dev/test/lv01"? [y/n]: y
lvreduce - doing automatic backup of volume group "test"
lvreduce - logical volume "/dev/test/lv01" successfully reduced
```

Também podemos especificar um valor absoluto em blocos , `-L50` por exemplo. Forçamos a verificação do sistema de arquivos novamente:

```
# e2fsck -f /dev/test/lv01
e2fsck 1.19, 13-Jul-2000 for EXT2 FS 0.5b, 95/08/09
Pass 1: Checking inodes, blocks, and sizes
Pass 2: Checking directory structure
Pass 3: Checking directory connectivity
Pass 4: Checking reference counts
Pass 5: Checking group summary information
/dev/test/lv01: 11/123952 files (9.1% non-contiguous), 15657/499713
blocks
```

E redimensionamos novamente o sistema de arquivos para aproveitar ao máximo o tamanho do Volume Lógico:

```
# resize2fs /dev/test/lv01
resize2fs 1.19 (13-Jul-2000)
The filesystem on /dev/test/lv01 is now 512000 blocks long.
```

Montamos novamente o sistema de arquivos e observamos o seu tamanho reduzido:

```
# mount /dev/test/lv01 /mnt/lvm/
```

```
# df -h /dev/test/lv01
Filesystem            Size  Used Avail Use% Mounted on
/dev/test/lv01        484M   13k  469M   0% /mnt/lvm
```

Obtemos um valor um pouco diferente dos 500MB originais, pelo fato de 500 mil blocos não corresponderem exatamente a 500MB. Se fosse preciso ter um valor exato, teríamos de fazer o cálculo com mais precisão e especificar os valores precisos em número de blocos.

Redundância e Performance

Por questões de performance, é possível distribuir dados em múltiplos discos. Isto significa que o bloco 1 está no Volume Físico A, e o bloco 2 está no PV B, enquanto que o bloco 3 pode estar no PV A novamente. Também podemos fazer stripes com mais de dois discos.

Esse arranjo disponibiliza uma maior largura de banda, devido ao paralelismo no acesso aos dados.

Além de acrescentar performance, também é possível ter os dados copiados em múltiplos discos. Isto é chamado de espelhamento. Atualmente o LVM não tem suporte nativo, mas existem várias maneiras de realizar esta operação.

Vantagens de uma stripe

A performance de disco é influenciada pelo menos por três fatores. O mais óbvio é a velocidade em que cada dado no disco pode ser lido ou escrito seqüencialmente. Este é o fator limitante quando se está lendo ou gravando um arquivo grande em um barramento SCSI/IDE com apenas um disco.

Há a largura de banda disponível para o disco. Se temos sete discos em uma interface SCSI, a limitação de banda pode causar um impacto maior que a velocidade de escrita para o próprio disco. Com um orçamento suficiente, podemos nos prevenir e evitar que este gargalo se torne um problema.

A latência é sempre um problema e para minimizá-la não podemos simplesmente aumentar os custos para termos uma latência menor. A maioria dos discos aparentemente têm um latência de algo em torno de sete milissegundo. Existe a latência de SCSI, que tende a ser algo em torno de 25 milissegundos.

O que isto significa? A latência combinada em um caso típico será em torno de 30 milissegundos. Podemos então efetuar, aproximadamente, apenas 33 operações em disco por segundo. Se queremos capacidade para fazer várias centenas de requisições por segundo, e não temos um cache muito grande, não poderemos realizar esta tarefa.

Se temos múltiplos discos trabalhando em paralelo, podemos ter múltiplos comandos sendo executados simultaneamente, que facilmente irão resolver o problema da latência. Algumas aplicações, como um servidor de notícias muito grande, não irão funcionar sem striping ou outras técnicas ágeis de ES[8].

8. IO

Isto é o que o striping pode fazer. Se o barramento tem este suporte, cada leitura e cada escrita seqüencial poderão ser mais rápida.

Desvantagens

O striping sem medidas adicionais aumenta as chances de falhas, em uma visão *de bits*. Se alguma coisa nos discos falhar, todo o Volume Lógico irá falhar junto. Se concatenarmos dados, apenas uma parte do sistema de arquivos será perdida.

Em último caso podemos utilizar espelhamento em stripes.

Striping nativo do LVM

A configuração que especifica as stripes é feita quando criamos o Volume Lógico com o comando **lvcreate**. Há dois parâmetros relevantes. Com o **-i** nós dizemos ao LVM quantos Volumes Físicos serão usados. O striping na realidade não é feito em uma base *bit-por-bit*, mas em blocos. Com o **-I** podemos especificar a granulação em kilobytes. Note que este valor deve ser uma potência de 2, e que a granulação grosseira é de 128KB. Por exemplo:

```
# lvcreate -n slv01 -i 2 -I 64 test -L 200M
lvcreate - doing automatic backup of "test"
```

```
lvcreate - logical volume "/dev/test/slv01" successfully created
```

Criando o sistema de arquivos:

```
# mke2fs /dev/test/slv01
mke2fs 1.19, 13-Jul-2000 for EXT2 FS 0.5b, 95/08/09
Filesystem label=
OS type: Linux
Block size=1024 (log=0)
Fragment size=1024 (log=0)
51200 inodes, 204800 blocks
10240 blocks (5.00%) reserved for the super user
First data block=1
25 block groups
8192 blocks per group, 8192 fragments per group
2048 inodes per group
Superblock backups stored on blocks:
        8193, 24577, 40961, 57345, 73729

Writing inode tables: done
Writing superblocks and filesystem accounting information: done
```

Efetuamos a montagem e verificamos o tamanho:

```
# mount /dev/test/slv01 /mnt/lvm/

# df -h /dev/test/slv01

Filesystem            Size  Used Avail Use% Mounted on

/dev/test/slv01       194M   13k  184M   0% /mnt/lvm
```

Notícias de performance

O ganho de performance poderá ser muito negativo se colocarmos mais que uma partição do mesmo disco em uma stripe - isto deve ser evitado. O striping com dois discos em uma única interface IDE também se torna inviável - isto dependerá da tecnologia IDE resolver este problema.

Placas mãe antigas podem ter duas interfaces IDE, porém o uso da segunda pode ser catastrófico, dedicada a servir uma unidade de CDROM lenta. Podemos efetuar *benchmarks* com várias ferramentas; a mais notória se chama Bonnie++, pode ser encontrada em (http://www.coker.com.au/bonnie++/), pode ser usada para medir a performance dos dados.

Capítulo 3. RAID

RAID é acrônimo para Redundant Array of Inexpensive Disks[1]. Este arranjo é usado como um meio para criar um subsistema de unidade de disco, rápido e confiável, através de discos individuais.

Apesar do RAID ter sido feito para melhorar a confiabilidade no sistema, através da adição de redundância, pode também levar a uma falsa sensação de segurança e confiança quando usado incorretamente. Esta falsa confiança pode acarretar em grandes desastres. Particularmente, o RAID é feito para proteger falhas no disco, não para proteger falhas de energia ou erros do operador.

Falhas de energia, bugs no desenvolvimento do kernel, ou erros de administradores e operadores podem danificar os dados de uma forma irrecuperável. **RAID não é um substituto apropriado para fazer backup do seu sistema**. Saiba o que você está fazendo, faça testes, seja conhecedor e ciente de todos os detalhes que envolvem a implementação de RAID.

RAID permite que o computador ganhe performance nas operações de acesso a disco, e da mesma forma, rápida recuperação em caso de perda de algum disco. O tipo mais comum de arranjo de unidades é um sistema ou uma controladora que possibilita o uso de múltiplas unidades de disco rígido, configuradas para que o sistema operacional se comporte como se existisse apenas um disco instalado no computador.

1. Arranjo redundante de discos

RAID Via Hardware e Via Software

RAID pode ser implementado por hardware, na forma de controladoras especiais de disco, ou por software, como um módulo do kernel que é dividido entre a controladora de disco de baixo nível e o sistema de arquivos acima dele.

RAID Via Hardware

RAID por hardware é sempre uma controladora de disco, isto é, um dispositivo que pode através de um cabo conectar os discos. Geralmente ele vem na forma de uma placa adaptadora que pode ser plugada em um slot ISA/EISA/PCI/S-Bus/MicroChannel. Entretanto, algumas controladoras RAID vêm na forma de uma caixa que é conectada através de um cabo entre o sistema controlador de disco e os dispositivos de disco.

RAIDs pequenos podem ser ajustados nos espaços para disco do próprio computador; outros maiores podem ser colocados em um gabinete de armazenamento com seu próprio espaço para disco e suprimento de energia. O hardware mais recente de RAID usado com a mais recente e rápida CPU, irá geralmente fornecer a melhor performance total, porém com um preço significante. Isto porque a maioria das controladoras RAID vêm com processadores especializados na placa e memória cache que pode eliminar uma quantidade de processamento considerável da CPU. As controladoras RAID também podem fornecer altas taxas de transferência através do cache da controladora.

Um hardware de RAID antigo pode atuar como um desacelerador, quando usado com uma CPU mais nova: DSP[2] e cache antigos podem atuar como um gargalo, e esta performance pode ser freqüentemente superada por um RAID de software puro.

RAID por hardware geralmente não é compatível entre diferentes tipos, fabricantes e modelos: se uma controladora RAID falhar, é melhor que ela seja trocada por outra controladora do mesmo tipo. Para uma controladora de RAID via hardware poder ser usada no Linux ela precisa contar com utilitários de configuração e gerenciamento, feitos para este sistema operacional e fornecidos pelo fabricante da controladora.

DPT

É possível configurar RAID via hardware SCSI, contando com suporte no Linux e documentação de uma forma geral, através de adaptadores baseados em host da DPT. Informações de instalação e configuração podem ser obtidas no site DPT-RAID (http://www.ram.org/computing/linux/dpt_raid.html).

Controladoras Suportadas

Uma controladora de RAID via hardware baseada em host e bem suportada é uma controladora que possui um driver para o Linux, fabricada pela DPT

2. *Digital Signal Processor*

DPT (http://www.dpt.com). Entretanto, existem outras controladoras baseadas em host e SCSI à SCSI que podem funcionar no Linux. Isto inclui algumas controladoras fabricadas pela Syred (http://www.syred.com), ICP-Vortex ICP-Vortex (http://www.icp-vortex.com) e BusLogic (http://www.mylex.com). Para obter mais informações sobre este assunto, verifique a página Soluções de RAID para o Linux (http://linas.org/linux/raid.html).

Controladoras DPT

Dentre as controladoras DPT, essencialmente todas as controladoras SmartRAID IV são suportadas.

Controladoras ICP Vortex

A ICP Vortex tem uma linha completa de controladoras de arranjos de discos com suporte ao Linux. O driver ICP está no kernel do Linux desde a versão 2.0.31. Todas as distribuições principais do Linux têm suporte às controladoras ICP, como controladoras para boot e instalação. O sistema RAID pode ser facilmente configurado com seu próprio ROMSETUP, ou seja, você não precisa utilizar outros sistemas operacionais para fazer a configuração.

Com o utilitário de monitoramento GDTMON, é possível gerenciar por completo o sistema RAID ICP durante a operação. É possível também verificar taxas de transferência, configurar os parâmetros da controladora e dos discos rígidos, substituir discos defeituosos, etc.. Atualmente estão disponíveis vários modelos,

para os mais diversos níveis de RAID que você venha a utilizar.

Tipos de Hardware

Tipo Controladora

Tendo várias opções de controladoras, é necessário pensar cuidadosamente sobre o que você quer fazer. Dependendo do que se quer fazer e do nível de RAID que irá usar, algumas controladoras podem ser melhores que outras. Adaptadores SCSI à SCSI podem não ser tão bons quanto adaptadores baseados em host, por exemplo. Michael Neuffer <neuffer@kralle.zdv.uni-mainz.de>, o autor do driver EATA-DMA, tem uma boa discussão sobre isto em sua página: Linux High Performance SCSI and RAID (http://www.uni-mainz.de/~neuffer/scsi/).

Tipo Encapsulado

O tipo encapsulado é ligado diretamente à habilidade de troca “à quente” da unidade e aos sistemas de advertência, ou seja, exibe indicação da falha, falhas da unidade e que tipo de tratamento sua unidade receberá. Um exemplo para isto pode ser refrigeração redundante e fornecimento de energia. Os encapsulamentos fornecidos pela DPT, HP, IBM e Compaq trabalham extremamente bem, mas têm um custo alto também.

RAID Via Software

RAID via software é uma configuração de módulos do kernel, juntamente com utilitários de administração que implementam RAID puramente por software, e não requer um hardware extraordinário. Pode ser utilizado o sistema de arquivos ext2fs, DOS-FAT ou outro.

Este tipo de RAID é implementado através dos módulos MD[3] do Kernel do Linux e das ferramentas relacionadas.

RAID por software, por ter sua natureza no software, tende a ser muito mais flexível que uma solução por hardware. O lado negativo é que ele em geral requer mais ciclos e potência de CPU para funcionar bem, quando comparado a um sistema de hardware. Ele oferece uma importante e distinta característica: opera sobre qualquer dispositivo do bloco, podendo ser um disco inteiro (por exemplo, `/dev/sda`), uma partição qualquer (por exemplo, `/dev/hdb1`), um dispositivo de loopback (por exemplo, `/dev/loop0`) ou qualquer outro dispositivo de bloco compatível, para criar um único dispositivo RAID. Isto é um contraste para a maioria das soluções de RAID via hardware, onde cada grupo junta unidades de disco inteiras em um arranjo.

Comparando as duas soluções, o RAID via hardware é transparente para o sistema operacional, e isto tende a simplificar o gerenciamento. Via software, há de longe mais opções e escolhas de configurações, fazendo com que o assunto se torne mais complexo.

3. *Multiple Devices*

O Controlador de Múltiplos Dispositivos (MD)

O controlador MD é usado para agrupar uma coleção de dispositivos de bloco, em um único e grande dispositivo de bloco. Normalmente, um conjunto de dispositivos SCSI e IDE são configurados em um único dispositivo MD. Como é encontrado no kernel do Linux 2.x, isto é feito apenas para remapear conjuntos de setores e dispositivos em novos conjuntos de setores e dispositivos. Pode ser feito através de dois modos diferentes: Linear (modo de concatenação) e *striping* (modo RAID-0).

As extensões do controlador MD implementam RAID-0 (striping), RAID-1 (espelhamento[4]), RAID-4 e RAID-5 por software. Isto quer dizer que, com MD, não é necessário hardware especial ou controladoras de disco para obtermos a maioria dos benefícios de RAID.

> A administração de RAID no Linux não é uma tarefa trivial, e é mais voltada para administradores de sistema experientes. A teoria da operação é complexa. As ferramentas do sistema exigem modificações nos scripts de inicialização. E recuperar-se de uma falha no disco não é uma tarefa simples, é passível de erros humanos. RAID não é para iniciantes, e qualquer benefício em busca de confiabilidade e performance pode ser facilmente acrescido de complexidade extra.
>
> Certamente, unidades de disco evoluídas são muito confiáveis, e controladoras e CPUs avançadas são muito potentes. Você pode obter mais facilmente os níveis de confiabilidade e performance desejados, comprando hadware de alta qualidade e

4. *mirroring*

potência.

Não se pode usar RAID via software com sistema de arquivos *journalled*, pois o Linux 2.2 não possui nenhum mecanismo para *pinning* de *buffers* que estão na memória.

Níveis de RAID

As diferentes maneiras de combinar os discos em um só, chamados de **níveis de RAID**[5], podem fornecer tanto grande eficiência de armazenamento como simples espelhamento, ou podem alterar a performance de latência (tempo de acesso). Podem também fornecer performance da taxa de transferência de dados para leitura e para escrita, enquanto continua mantendo a redundância. Novamente, isto é ideal para prevenir falhas.

Os diferentes níveis de RAID apresentam diferentes performance, redundância, capacidade de armazenamento, confiabilidade e características de custo. A maio-

5. *RAID levels*

ria, mas nem todos os níveis de RAID, oferecem redundância a falha de disco. Dos que oferecem redundância, RAID-1 e RAID-5 são os mais populares. RAID-1 oferece performance melhor, enquanto que RAID-5 fornece um uso mais eficiente do espaço disponível para o armazenamento dos dados.

De qualquer modo, o ajuste de performance é um assunto totalmente diferente. A performance depende de uma grande variedade de fatores como o tipo da aplicação, os tamanhos dos discos, blocos e arquivos.

Existe uma variedade de tipos diferentes e implementações de RAID, cada uma com suas vantagens e desvantagens. Por exemplo, para colocarmos uma cópia dos mesmos dados em dois discos (chamado de espelhamento de disco[6] ou RAID nível 1), podemos acrescentar performance de leitura, lendo alternadamente cada disco do espelho. Em média, cada disco é menos usado, por estar sendo usado em apenas metade da leitura (para dois discos), ou um terço (para 3 discos), etc.. Além disso, um espelho pode melhorar a confiabilidade: se um disco falhar, o(s) outro(s) disco(s) têm uma cópia dos dados.

A seguir descreveremos os diferentes níveis de RAID, no contexto de implementação de RAID por software no Linux:

RAID-linear

é uma simples concatenação de partições para criar uma grande partição virtual. Isto é possível se você tem várias unidades pequenas, e quer criar uma única e

6. disk mirroring

grande partição. Esta concatenação não oferece redundância, e de fato diminui a confiabilidade total: se qualquer um dos discos falhar, a partição combinada irá falhar.

RAID-0

A grande maioria dos níveis de RAID envolve uma técnica de armazenamento chamada de segmentação de dados (*data stripping*). A implementação mais básica dessa técnica é conhecida como RAID-0 e é suportada por muitos fabricantes. Contudo, pelo fato deste nível de arranjo não ser tolerante a falhas, RAID-0 não é verdadeiramente RAID, ao menos que seja usado em conjunção com outros níveis de RAID.

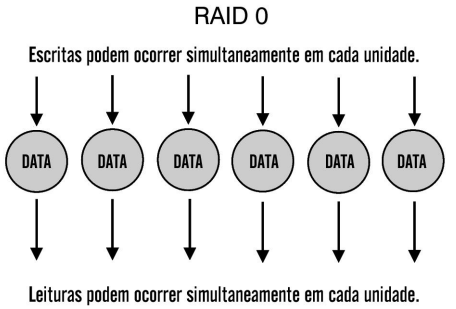


Figura 3-1. RAID-0

Segmentação (*stripping*) é um método de mapeamento de dados sobre o meio físico de um arranjo, que serve para criar um grande dispositivo de armazenamento. Os dados são subdivididos em segmentos consecutivos ou *stripes* que são escritos seqüencialmente através de cada um dos discos de um arranjo. Cada segmento tem um tamanho definido em blocos.

Por exemplo, sabendo que o tamanho de cada segmento está defindo em 64 kbytes, e o arranjo de discos contem 2 discos, quando um arquivo de 128 kbytes for gravado, os primeiros 64 kbytes serão gravados no primeiro disco, sendo que os últimos 64 kbytes irão para o segundo disco, e normalmente isso é feito em paralelo, aumentando consideravelmente a performance.

Um arranjo desse tipo pode oferecer uma melhor performance, quando comparada a um disco individual, se o tamanho de cada segmento for ajustado de acordo com a aplicação que utilizará o arranjo:

- Em um ambiente com uso intensivo de E/S ou em um ambiente de banco de dados onde múltiplas requisições concorrentes são feitas para pequenos registros de dados, um segmento de tamanho grande é preferencial. Se o tamanho de segmento para um disco é grande o suficiente para conter um registro inteiro, os discos do arranjo podem responder independentemente para as requisições simultâneas de dados.

- Em um ambiente onde grandes registros de dados são armazenados, segmentos de pequeno tamanho são mais apropriados. Se um determinado registro de dados extende-se através de vários discos do arranjo, o conteúdo do registro pode ser lido em paralelo, aumentando o desempenho total do sistema.

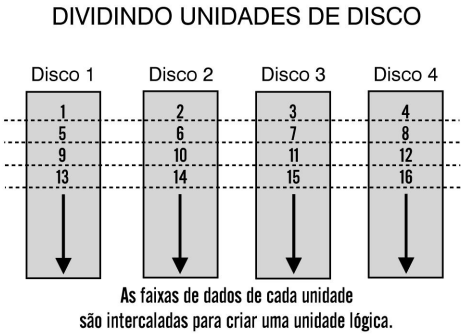


Figura 3-2. Stripping

Arranjos RAID-0 podem oferecer alta performance de escrita se comparados a verdadeiros níveis de RAID por não apresentarem sobrecarga[7] associada com cálculos de paridade ou com técnicas de recuperação de dados. Esta mesma falta de previsão para reconstrução de dados perdidos indica que esse tipo de arranjo deve ser restrito ao armazenamento de dados não críticos e combinado com eficientes programas de backup.

7. overhead

RAID-1

A forma mais simples de arranjo tolerante a falhas é o RAID-1. Baseado no conceito de espelhamento (*mirroring*), este arranjo consiste de vários grupos de dados armazenados em 2 ou mais dispositivos. Apesar de muitas implementações de RAID-1 envolverem dois grupos de dados (daí o termo espelho - *mirror*), três ou mais grupos podem ser criados se a alta confiabilidade for desejada.

Se ocorre uma falha em um disco de um arranjo RAID-1, leituras e gravações subseqüentes são direcionadas para o(s) disco(s) ainda em operação. Os dados então são reconstruídos em um disco de reposição (*spare disk*) usando dados do(s) disco(s) sobreviventes. O processo de reconstrução do espelho tem algum impacto sobre a performance de E/S do arranjo, pois todos os dados terão de ser lidos e copiados do(s) disco(s) intacto(s) para o disco de reposição (*spare disk*).

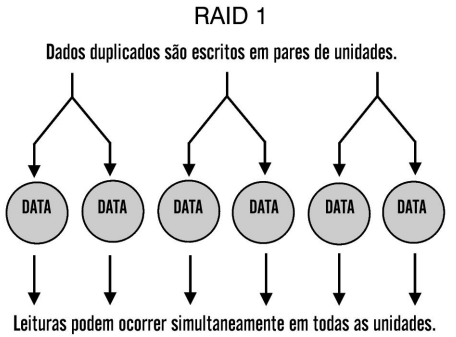


Figura 3-3. RAID-1

RAID-1 oferece alta disponibilidade de dados, porque no mínimo 2 grupos completos são armazenados. Conectando os discos primários e os discos espelhados em controladoras separadas, pode aumentar a tolerância a falhas pela eliminação da controladora como ponto único de falha.

Dentre os não híbridos, este nível tem o maior custo de armazenamento por requerer capacidade suficiente para armazenar no mínimo 2 grupos de dados. Este é melhor adaptado para servir pequenas base de dados ou sistemas de pequena escala que necessitem confiabilidade.

RAID-2 e RAID-3

Raramente são usados, e em algum momento ficaram obsoletos pelas novas tecnologias de disco. RAID-2 é similar ao RAID-4, mas armazena informação ECC (error correcting code), que é a informação de controle de erros, no lugar da paridade. Isto ofereceu pequena proteção adicional, visto que todas as unidades de disco mais novas incorporaram ECC internamente.

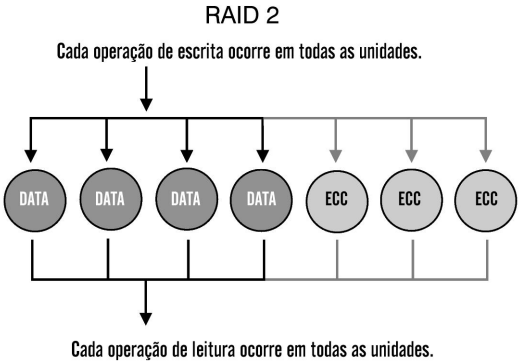


Figura 3-4. RAID-2

RAID-2 pode oferecer maior consistência dos dados se houver queda de energia durante a escrita. Baterias de segurança e um desligamento correto, porém, podem oferecer os mesmos benefícios. RAID-3 é similar ao RAID-4, exceto que ele usa o menor tamanho possível para a *stripe*. Como resultado, qualquer pedido de leitura invocará todos os discos, tornando as requisições de sobreposição de I/0 difíceis ou impossíveis.

A fim de evitar o atraso devido a latência rotacional, o RAID-3 exige que todos os eixos das unidades de disco estejam sincronizados. A maioria das unidades de disco mais recentes não possuem a habilidade de sincronização do eixo, ou se são capazes disto, faltam os conectores necessários, cabos e documentação do fabricante. Nem RAID-2 e nem RAID-3 são suportados pelos drivers de RAID por software no Linux.

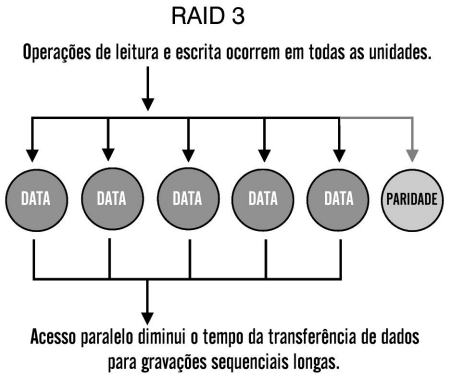


Figura 3-5. RAID-3

RAID-4

Este é um tipo de arranjo segmentado, mas incorpora um método de proteção de dados mais prático. Ele usa informações sobre paridade para a recuperação de dados e as armazena em disco dedicado. Os discos restantes, usados para dados, são configurados para usarem grandes (tamanho medido em blocos) segmentos de dados, suficientemente grandes para acomodar um registro inteiro. Isto permite leituras independentes da informação armazenada, fazendo de RAID-4 um arranjo perfeitamente ajustado para ambientes transacionais que requerem muitas leituras pequenas e simultâneas.

Arranjos RAID-4 e outros arranjos que utilizam paridade fazem uso de um processo de recuperação de dados mais envolvente que arranjos espelhados, como RAID-1. A função *ou exclusivo* (XOR) dos dados e informações sobre paridade dos discos restantes é computada para reconstruir os dados do disco que falhou. Pelo fato de que todos os dados sobre paridade são escritos em um único disco, esse disco funciona como um gargalo durante as operações de escrita, reduzindo a performance durante estas operações (*write bottleneck*).

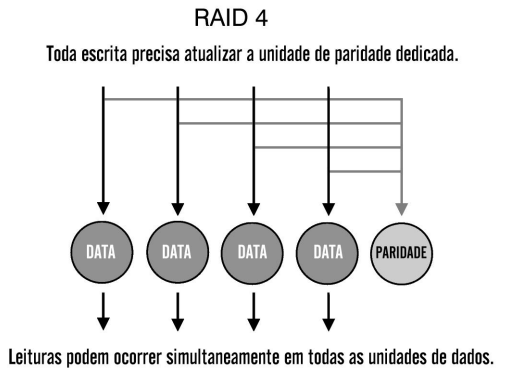


Figura 3-6. RAID-4

Sempre que os dados são escritos no arranjo, informações sobre paridade normalmente são lidas do disco de paridade e uma nova informação sobre paridade deve sempre ser escrita para o disco de paridade antes da próxima requisição de escrita ser realizada. Por causa dessas duas operações de E/S, o disco de paridade é o fator limitante da performance total do arranjo. Por causa dele requerer

somente um disco adicional para proteção de dados, arranjos RAID-4 são mais baratos que arranjos RAID-1.

RAID-5

Este tipo de RAID largamente usado funciona similarmente ao RAID 4, mas supera alguns dos problemas mais comuns sofridos por esse tipo. As informações sobre paridade para os dados do arranjo são distribuídas ao longo de todos os discos do arranjo, ao invés de serem armazenadas em um disco dedicado.

Essa idéia de paridade distribuída reduz o gargalo de escrita (*write bottleneck*) que era o único disco de um RAID-4, porque agora as escritas concorrentes nem sempre requerem acesso às informações sobre paridade em um disco dedicado. Contudo, a performance de escrita geral ainda sofre por causa do processamento adicional causado pela leitura, recálculo e atualização da informação sobre paridade.

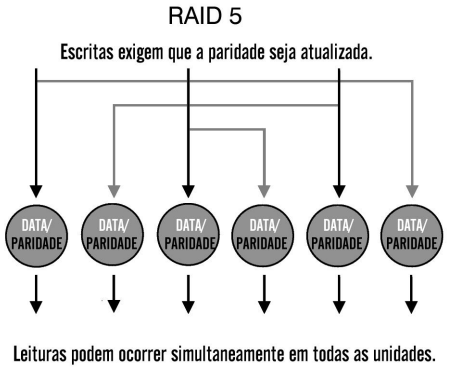


Figura 3-7. RAID-5

Para aumentar a performance de leitura de um arranjo RAID-5, o tamanho de cada segmento em que os dados são divididos pode ser otimizado para a aplicação que estiver usando o arranjo. A performance geral de um arranjo RAID-5 é equivalente ao de um RAID-4, exceto no caso de leituras seqüenciais, que reduzem a eficiência dos algoritmos de leitura por causa da distribuição das informações sobre paridade.

Como em outros arranjos baseados em paridade, a recuperação de dados em um arranjo RAID-5 é feita calculando a função XOR das informações dos discos restantes do arranjo. Pelo fato de que a informação sobre paridade é distribuída ao longo de todos os discos, a perda de qualquer disco reduz a disponibilidade de ambos os dados e informação sobre paridade, até a recuperação do disco que falhou. Isto pode causar degradação da performance de leitura e de escrita.

Tipos Híbridos

Para suprir as deficiências de um nível ou outro de RAID, é possível usar um nível de RAID sobre outro, aproveitando por exemplo, a excelente performance de um determinado nível e a confiabilidade de outro. Isso tudo é claro, pagando o preço de uma maior quantidade de material.

Um exemplo é o RAID-10. Como o seu nome implica, é a combinação de discos espelhados (RAID-1) com a segmentação de dados (*data stripping*) (RAID-0).

O método de criação de um arranjo RAID-10 é diversificado. Em uma implementação RAID-0+1, os dados são segmentados através de grupos de discos espelhados, isto é, os dados são primeiro segmentados e para cada segmento é feito um espelho. Já em um RAID-1+0, os dados são primeiramente espelhados, e para cada espelho há a segmentação sobre vários discos.

RAID-10 oferece as vantagens da transferência de dados rápida de um arranjo espelhado, e as características de acessibilidade dos arranjos espelhados. A performance do sistema durante a reconstrução de um disco é tambem melhor que nos arranjos baseados em paridade, pois os dados são somente copiados do dispositivo sobrevivente.

O RAID-50 é um arranjo híbrido que usa as técnicas de RAID com paridade em conjunção com a segmentação de dados. Um arranjo RAID-50, é essencialmente um arranjo com as informações segmentadas através de dois ou mais arranjos RAID-5.

Dependendo do tamanho de cada segmento estabelecido durante a configuração do arranjo, estes arranjos híbridos podem oferecer os benefícios de acesso par-

alelo dos arranjos com paridade (alta velocidade na transferência de dados) ou de acesso independente dos arranjos com paridade (grande quantidade). Como em outros arranjos RAID com paridade, a reconstrução de um disco falho gera um impacto na performance do programa usando o arranjo.

Desempenho de RAID

Utilizando RAID por software (MD), a possibilidade de acrescentar velocidade e avaliar o desempenho depende muito da configuração que você está usando. Para isto, nesta seção, iremos analisar algumas destas configurações.

Desempenho no MD RAID-0 e no MD RAID-linear

Se o sistema é altamente carregado com muitas operações de E/S (entrada e saída), estatisticamente, algumas operações irão para um disco, e algumas para os outros discos. Assim, o desempenho irá melhorar em um único disco grande. A melhora real depende muito dos dados reais, do tamanho das *stripes*, e de outros fatores. Em um sistema com uma baixa utilização de E/S, o desempenho é igual ao de um único disco.

Desempenho de Leitura no MD RAID-1

O MD implementa balanceamento de leitura, isto é, o código RAID-1 irá alternar entre cada um (dois ou mais) dos discos no espelho, fazendo leituras alternadas para cada um. Em uma situação de baixa E/S, isto não poderá mudar o desempenho total: você terá que esperar por um disco para completar a leitura. Porém, com dois discos em um ambiente de alta E/S, isto poderia aumentar duas vezes o desempenho de leitura, desde que as leituras possam ser emitidas para cada um dos discos em paralelo. Para N discos no espelho, a melhora do desempenho pode ser de 2N.

Desempenho de Escrita no MD RAID-1

Deve-se esperar a escrita ocorrer para todos os discos no espelho. Isto porque uma cópia dos dados deve ser escrita para cada um dos discos no espelho. Assim, o desempenho será aproximadamente igual ao desempenho de escrita para um único disco.

Desempenho de Leitura no MD RAID-4/5

Estatisticamente, um bloco pode estar em qualquer uma das unidades de disco, e assim o desempenho de leitura do RAID-4/5 é um tanto parecido com o do RAID-0. Isto irá depender dos dados, do tamanho da *stripe* e da aplicação. Não será tão bom quanto o desempenho de leitura de um arranjo espelhado.

Desempenho de Escrita no MD RAID-4/5

Será no geral consideravelmente mais lento do que aquele para um único disco. Isto porque a paridade deve ser escrita em um disco, assim como os dados em outro. Entretanto, para processar a nova paridade, a paridade antiga e os dados antigos devem ser lidos primeiramente. Os dados antigos, os dados novos e a paridade antiga devem ser todos comparados juntos, através da operação lógica XOR, para determinar a nova paridade: isto requer consideráveis ciclos de CPU em adição aos numerosos acessos ao disco.

Comparação dos Níveis de RAID

Podemos fazer uma comparação entre os vários níveis de RAID, de acordo com desempenho (leitura, gravação e reconstrução), disponibilidade de dados e o número mínimo de unidades requeridas. Observe na tabela a descrição destes atributos para comparação dos níveis de RAID.

Tabela 3-1. Atributos de Comparação dos Vários Níveis de RAID

Nível de RAID	Disponibilidade dos Dados	Desempenho de Leitura	Desempenho de Gravação	Desempenho de Reconstrução	Número Mínimo de Unidades Requeridas
RAID 0	Nenhuma	Muito bom	Muito bom	Não disponível	N
RAID 1	Excelente	Muito bom	Bom	Bom	2N
RAID 4	Boa	E/S seqüencial: Boa E/S transacional: Boa	E/S seqüencial: Muito Boa E/S transacional: Ruim	Satisfatória	N + 1 (N pelo menos 2)

RAID 5	Boa	E/S seqüencial: Boa E/S transacional: Muito Boa	Satisfatória (a menos que o cache write-back seja usado)	Ruim	N + 1 (N pelo menos 2)
RAID 10	Excelente	Muito boa	Satisfatória	Boa	2N
RAID 50	Excelente	Muito boa	Satisfatória	Satisfatória	N+2

o número **N** é o requerimento de espaço para armazenamento de dados do nível de RAID. Exemplo: se o requesito mínimo é ter 6GB de espaço para um arranjo RAID-5, então deve-se ter ao menos 2 discos de 3GB cada e mais um disco de 3GB, sendo 6GB (2 discos) + 3GB (1 disco).

Configuração de RAID

Antes de configurar qualquer um dos níveis de RAID, siga os seguintes procedimentos:

- Instale as ferramentas para RAID:

```
# rpm -ivh raidtools*
raidtools ############################### #
```

- Observe conteúdo do arquivo `/proc/mdstat`:

```
# cat /proc/mdstat
Personalities : read_ahead not set
unused devices: <none> #
```

  Este arquivo você sempre irá verificar para checar as configurações de RAID. Observe que nenhum dispositivo de RAID está atualmente ativo.

- Crie as partições que você desejar incluir em sua configuração de RAID, por exemplo:

```
# fdisk /dev/hda

Comando (tecle m para obter ajuda): n
```

- O próximo passo dependerá do nível de RAID que você escolheu usar; estaremos vendo a seguir cada uma destas configurações.

Modo Linear

Se você tem duas ou mais partições que não são necessariamente do mesmo tamanho. Você poderá concatenar uma com a outra.

Crie o arquivo `/etc/raidtab` para descrever sua configuração. Uma raidtab para dois discos em modo linear, terá uma aparência semelhante a esta:

```
raiddev /dev/md0
raid-level linear
nr-raid-disks 2
chunk-size 32
persistent-superblock 1
device /dev/hda6
raid-disk 0
device /dev/hda7
raid-disk 1
```

Nos exemplos utilizaremos duas ou três partições de aproximadamente 1GB, sendo elas `hda5`, `hda6` e `hda7`, dependendo da configuração de RAID. Discos sobressalentes não são suportados aqui. Se um disco falhar, o arranjo irá falhar juntamente com ele. Não existem informações que possam ser colocadas em um disco sobressalente.

Para criar o arranjo execute o comando:

```
# mkraid /dev/md0
handling MD device /dev/md0
analyzing super-block
disk 0: /dev/hda6, 1028128kB, raid superblock at 1028032kB
disk 1: /dev/hda7, 1028128kB, raid superblock at 1028032kB #
```

Isto irá inicializar o arranjo, escrever os blocos persistentes e deixar pronto para uso. Checando o arquivo `/proc/mdstat` você poderá ver que o arranjo está funcionando:

```
# cat /proc/mdstat
Personalities : [linear]
read_ahead 1024 sectors
md0 : active linear hda7[1] hda6[0] 2056064 blocks 32k rounding
unused devices: <none>
#
```

Agora você já pode criar um sistema de arquivos, como se fosse em um dispositivo normal:

```
# mke2fs /dev/md0
mke2fs 1.18, 11-Nov-1999 for EXT2 FS 0.5b, 95/08/09
Filesystem label=
OS type: Linux
```

```
Block size=4096 (log=2)
Fragment size=4096 (log=2)
257024 inodes, 514016 blocks
25700 blocks (5.00%) reserved for the super user
First data block=0
16 block groups
32768 blocks per group, 32768 fragments per group
16064 inodes per group
Superblock backups stored on blocks:
    32768, 98304, 163840, 229376, 294912

Writing inode tables: done
Writing superblocks and filesystem accounting information: done
```

Criar um ponto de montagem e montar o dispositivo:

```
# mkdir /mnt/md0
# mount /dev/md0 /mnt/md0
# df
Filesystem 1k-blocks Used Available Use% Mounted on
/dev/md0 2023760 20 1920940 0% /mnt/md0 #
```

Observe que o tamanho total é de aproximadamente 2GB, pelo fato de termos

feito uma concatenação de duas unidades, cada uma com aproximadamente 1GB.

RAID-0

Tendo dois ou mais dispositivos aproximadamente do mesmo tamanho, é possível combinar suas capacidades de armazenamento, bem como seus desempenhos, através do acesso em paralelo.

Modifique ou crie o arquivo `/etc/raidtab` para descrever a sua configuração. Observe o exemplo:

```
raiddev /dev/md0
raid-level 0
nr-raid-disks 2
persistent-superblock 1
chunk-size 4
device /dev/hda6
raid-disk 0
device /dev/hda7
raid-disk 1
```

Como no modo linear, não há suporte para discos reserva. RAID-0 não oferece redundância: se um disco falhar todo o conjunto irá falhar.

Se você já possui um dispositivo de RAID existente, execute o comando para interrompê-lo e forçar a construção. Crie o dispositivo de RAID através dos comandos:

```
# raidstop /dev/md0
# mkraid -force /dev/md0
DESTROYING the contents of /dev/md0 in 5 seconds, Ctrl-C if unsure!
 handling MD device /dev/md0
analyzing super-block
disk 0: /dev/hda6, 1028128kB, raid superblock at 1028032kB
disk 1: /dev/hda7, 1028128kB, raid superblock at 1028032kB
#
```

Isto irá inicializar os superblocos e iniciar o dispositivo raid. Observando o arquivo `/proc/mdstat` temos:

```
# cat /proc/mdstat
Personalities : [raid0]
read_ahead 1024 sectors
md0 : active raid0 hda7[1] hda6[0] 2056064 blocks 4k chunks
unused devices: <none>
#
```

Agora o dispositivo `/dev/md0` já está pronto. Pode ser criado um sistema de ar-

quivos e ser montado para uso.

RAID-1

Com dois dispositivos aproximadamente do mesmo tamanho, é possível fazer com que um seja espelho do outro. Se você tiver mais dispositivos, poderá usá-los como um sistema de discos sobressalentes; isto será feito automaticamente por uma parte do espelho se um dos dispositivos operantes falhar.

Para isto, configure o arquivo `/etc/raidtab` da seguinte maneira:

```
raiddev /dev/md0
raid-level 1
nr-raid-disks 2
nr-spare-disks 0
chunk-size 4
persistent-superblock 1
device /dev/hda6
raid-disk 0
device /dev/hda7
raid-disk 1
```

Se você usar discos sobressalentes, adicione no final da especificação do dispos-

itivo o seguinte:

```
device /dev/hdb1
spare-disk 0
```

Onde `/dev/hdb1` é um disco sobressalente. Configure o número de entrada dos discos sobressalentes, sempre de uma forma proporcional.

Tendo tudo pronto para começar a inicialização do RAID, o espelho poderá ser construído. E os índices (não no caso de dispositivos sem formatação) dos dois dispositivos serão sincronizados. Execute:

```
# mkraid /dev/md0
```

Neste momento veja este comando que irá fazer a inicialização do espelho. Observe agora o arquivo `/proc/mdstat`; ele irá mostrar que o dispositivo `/dev/md0` foi inicializado, que o espelho começou a ser reconstruído, e quanto falta para a reconstrução ser completada:

```
# cat /proc/mdstat
Personalities : [raid1]
read_ahead 1024 sectors
md0 : active raid1 hda7[1] hda6[0] 1028032 blocks [2/2]
[UU] resync=63% finish=2.5min
unused devices: <none> #
```

O processo de reconstrução é transparente: você poderá usar os dispositivos normalmente durante a execução deste processo. É possível até formatar o dispositivo enquanto a reconstrução está sendo executada. Você também pode montar e desmontar as unidades neste período (somente se um disco falhar esta ação será prejudicada).

Agora já é possível montar e visualizar o tamanho do dispositivo final:

```
# mount /dev/md0 /mnt/md0
# df
Filesystem  1k-blocks  Used Available Use%  Mounted on
/dev/md0    1011928      20     960504  0%    /mnt/md0
#
```

Observe que o tamanho do dispositivo corresponde ao tamanho de um único dispositivo, por se tratar de um espelhamento de discos.

RAID-4

Com três ou mais dispositivos aproximadamente do mesmo tamanho, sendo um dispositivo significativamente mais rápido que os outros dispositivos, é possível combiná-los em um único dispositivo grande, mantendo ainda informação de redundância. Eventualmente você pode colocar alguns dispositivos para serem usados como discos sobressalentes.

Um exemplo de configuração para o arquivo `/etc/raidtab`:

```
raiddev /dev/md0
raid-level 4
nr-raid-disks 3
nr-spare-disks 0
persistent-superblock 1
chunk-size 32
device dev/hda5
raid-disk 0
device /dev/hda6
raid-disk 1
device /dev/hda7
raid-disk 2
```

Se houverem discos sobressalentes, será necessário configurar da mesma forma, seguindo as especificações do disco raid. Veja o exemplo:

```
 device /dev/hdb1
spare-disk 0
```

O disco sobressalente é criado de forma similar em todos os níveis de RAID. Inicialize o RAID-4 com o comando:

```
# mkraid /dev/md0
handling MD device /dev/md0
analyzing super-block
disk 0: /dev/hda5, 1028128kB, raid superblock at 1028032kB
disk 1: /dev/hda6, 1028128kB, raid superblock at 1028032kB
disk 2: /dev/hda7, 1028128kB, raid superblock at 1028032kB #
```

Você poderá acompanhar o andamento da construção do RAID através do arquivo `/proc/mdstat`:

```
# cat /proc/mdstat
Personalities : [raid5]
read_ahead 1024 sectors
md0 : active raid5 hda7[2] hda6[1] hda5[0] 2056064 blocks level 4,
32k chunk, algorithm 0 [3/3] [UUU] resync=59% finish=4.6min
unused devices: <none>
#
```

Para formatar o RAID-4, utilize as seguintes opções especiais (-R stride=8) do **mke2fs**:

```
# mke2fs -b 4096 -R stride=8 /dev/md0
mke2fs 1.18, 11-Nov-1999 for EXT2 FS 0.5b, 95/08/09
Filesystem label=
```

```
OS type: Linux
Block size=4096 (log=2)
Fragment size=4096 (log=2)
257024 inodes, 514016 blocks
25700 blocks (5.00%) reserved for the super user
First data block=0
16 block groups 32768 blocks per group,
32768 fragments per group 16064 inodes per group
Superblock backups stored on blocks:
      32768, 98304, 163840, 229376, 294912

Writing inode tables: done
Writing superblocks and filesystem accounting information: done #
```

Basta montar o RAID para uso. O tamanho total será de N-1, ou seja, o tamanho total de todos os dispositivos menos um, reservado para a paridade:

```
# df
Filesystem 1k-blocks Used Available Use% Mounted on
/dev/md0     2023760   20   1920940   0%   /mnt/md0 #
```

Note que o RAID-4 carrega o MD do RAID-5, por se tratarem de níveis similares de RAID.

RAID-5

Similar ao RAID-4, porém é implementado através de três ou mais dispositivos de tamanho aproximado, combinados em um dispositivo maior. Ainda mantém um grau de redundância para proteger os dados. Podem ser usados discos sobressalentes, tomando parte de outros discos automaticamente caso eles venham a falhar.

Se você está usando N dispositivos onde o menor tem um tamanho S, o tamanho total do arranjo será (N-1)*S. Esta perda de espaço é utilizada para a paridade (redundância) das informações. Assim, se algum disco falhar, todos os dados continuarão intactos. Porém, se dois discos falhares, todos os dados serão perdidos.

Configure o arquivo `/etc/raidtab` de uma forma similar a esta:

```
raiddev /dev/md0
raid-level 5
nr-raid-disks 3
nr-spare-disks 0
persistent-superblock 1
parity-algorithm left-symmetric c
chunk-size 32
device /dev/hda5
raid-disk 0
device /dev/hda6
```

```
raid-disk 1
device /dev/hda7
raid-disk 2
```

Se existir algum disco sobressalente, ele pode ser inserido de uma maneira similar, seguindo as especificações de disco raid. Por exemplo:

```
 device /dev/hdb1
spare-disk 0
```

Um tamanho do pedaço (chunk size) de 32 KB é um bom padrão para sistemas de arquivos com uma finalidade genérica deste tamanho. O arranjo em qual o raidtab anterior é usado é de (n-1)*s = (3-1)*2 = 2 GB de dispositivo. Isto prevê um sistema de arquivos ext2 com um bloco de 4 KB de tamanho. Você poderia aumentar, juntamente com o arranjo, o tamanho do pedaço e o tamanho do bloco do sistema de arquivos. Se seu sistema de arquivos fosse muito maior, ou se irá usar arquivos muito grandes.

Execute o comando **mkraid** para o dispositivo `/dev/md0`. Isto irá começar a reconstrução do seu arranjo. Observe o arquivo `/proc/mdstat` para poder fazer um acompanhamento do processo:

```
# cat /proc/mdstat
Personalities : [raid5]
read_ahead 1024 sectors
md0 : active raid5 hda7[2] hda6[1] hda5[0] 2056064 blocks level 5,
```

```
32k chunk, algorithm 2 [3/3] [UUU] resync=29% finish=11.4min

unused devices: <none>

#
```

Se o dispositivo for criado com sucesso, a reconstrução foi iniciada. O arranjo não estará consistente até a fase de reconstrução ter sido completada. Entretanto, o arranjo é totalmente funcional (exceto para troca de dispositivos que falharam no processo); você pode formatar e usar o arranjo enquanto ele estiver sendo reconstruído.

Formate o arranjo com o comando: **mke2fs -b 4096 -R stride=8 /dev/md0**. Quando você tiver um dispositivo RAID executando, você pode sempre parar ou reiniciar usando os comandos: **raidstop /dev/md0** ou **raidstart /dev/md0**.

Mais informações e detalhes do processo de criação de RAID podem ser obtidas em RAID Solutions for Linux (http://linas.org/linux/raid.html).

Uso de RAID para Obter Alta Disponibilidade

Alta disponibilidade é difícil e cara. Quanto mais arduamente você tenta fazer

um sistema ser tolerante a falhas, mais ele passa a ser dispendioso e difícil de implementar. As seguintes sugestões, dicas, idéias e suposições poderão ajudar você a respeito deste assunto:

- Os discos IDE podem falhar de tal maneira que o disco que falhou em um cabo do IDE possa também impedir que um disco bom, no mesmo cabo, responda, fazendo assim uma aparência de que os dois discos falharam. Apesar de RAID não oferecer proteção contra falhas em dois discos, você deve colocar apenas um disco em um cabo IDE, ou se houverem dois discos, devem pertencer à configurações diferentes de RAID.

- Discos SCSI podem falhar de tal maneira que o disco que falhou em uma cadeia pode impedir todos os dispositivos da série de serem acessados. O modo de falha envolve a posição do pino de leitura de dispositivo comum (compartilhado); apesar deste pino ser compartilhado, nenhuma arbitrariedade pode ocorrer até a posição estar desligada. Assim, dois discos SCSI na mesma cadeia não devem pertencer ao mesmo arranjo RAID.

- Observações similares são aplicadas às controladoras de disco. Não sobrecarregue os canais em uma controladora; utilize controladoras múltiplas.

- Não utilize o mesmo tipo ou número de modelo para todos os discos. Não é incomum em variações elétricas bruscas perder dois ou mais discos, mesmo com o uso de supressores - eles não são perfeitos ainda. O calor e a ventilação pobre do compartimento de disco são outras causas das perdas de disco. Discos baratos freqüentemente funcionam aquecidos. Utilizar diferentes tipos de discos e controladoras diminui a probabilidade de danificação de um disco (calor, choque físico, vibração, choque elétrico).

- Para proteger contra falhas de controladora ou de CPU, é possível construir um com-

partimento de disco SCSI que tenha cabos gêmeos, ou seja, conectado a dois computadores. Um computador irá montar o sistema de arquivos para leitura e escrita, enquanto outro computador irá montar o sistema de arquivos somente para leitura, e atuar como um computador reserva ativo. Quando o computador reserva é capaz de determinar que o computador mestre falhou (por exemplo, através de um adaptador *watchdog*), ele irá cortar a energia do computador mestre (para ter certeza que ele está realmente desligado), e então fazer a verificação com o fsck e remontar o sistema para leitura e escrita.

- Sempre utilize um **no-break**, e efetue os desligamentos corretamente. Embora um desligamento incorreto não possa danificar os discos, executar o **ckraid** em qualquer arranjo pequeno é extremamente lento. Você deve evitar a execução do **ckraid** sempre que for possível, ou pode colocar um hack no kernel e começar a reconstrução do código verificando erros.

- Cabos SCSI são conhecidos por serem muito sujeitos a falhas, e podem causar todo tipo de problemas. Utilize o cabeamento de mais alta qualidade que você puder encontrar a venda. Utilize por exemplo o *bubble-wrap* para ter certeza que os cabos fita não estão muito perto um do outro e do *cross-talk*. Observe rigorosamente as restrições do comprimento do cabo.

- Dê uma olhada em SSI (arquitetura de armazenamento serial). Embora seja muito caro, parece ser menos vulnerável aos tipos de falhas que o SCSI apresenta.

Capítulo 4. LDAP

Neste capítulo apresentaremos informações sobre instalação, configuração, execução e administração de um Servidor LDAP (Lightweight Directory Access Protocol) em um computador com Linux. Você aprenderá como recuperar informações do seu *Diretório*, utilizando os clientes e utilitários fornecidos. Trataremos de como *migrar* a sua base de usuários para um banco de dados LDAP, quais informações serão *importadas*, de que modo efetuar autenticação e acesso remoto através do LDAP. Mostraremos também como usar o Livro de Endereços do Netscape Communicator, envio de e-mails e a navegação através de URLs, fazendo o uso dos recursos de LDAP.

> A versão 2.0 do OpenLDAP se encontra no CD 2 da distribuição do Conectiva Linux. Por estar em estado de implementação e com a documentação ainda incompleta, não documentaremos esta versão. Apenas mostraremos as principais diferenças entre a versão 1.0 (a qual trataremos neste capítulo) e a nova versão 2.0. Mais informações consulte o[1] OpenLDAP 2.0 Administrator's Guide.

Introdução e Conceitos

LDAP é um protocolo (executado sobre o TCP/IP) cliente-servidor, utilizado para

1. http://www.openldap.org/doc/admin/

acessar um serviço de Diretório. Ele foi inicialmente usado como uma interface para o X.500, mas também pode ser usado com autonomia e com outros tipos de servidores de Diretório. Atualmente vem se tornando um padrão, diversos programas já têm suporte a LDAP. Livros de endereços, autenticação, armazenamento de certificados digitais (S/MIME) e de chaves públicas (PGP), são alguns dos exemplos onde o LDAP já é amplamente utilizado.

Serviço de Diretório

Um *Diretório* é como um banco de dados, mas tende a conter mais informações descritivas, baseadas em atributo e é organizado em forma de árvore, não de tabela. A informação em um Diretório é geralmente mais lida do que é escrita. Como conseqüência, Diretórios normalmente não são usados para implementar transações complexas, ou esquemas de consultas regulares em bancos de dados, transações estas que são usadas para fazer um grande volume de atualizações complexas. Atualizações em Diretórios são tipicamente simples ou nem são feitas.

Diretórios são preparados para dar resposta rápida a um grande volume de consultas ou operações de busca. Eles também podem ter a habilidade de replicar informações extensamente; isto é usado para acrescentar disponibilidade e confiabilidade, enquanto reduzem o tempo de resposta.

Existem várias maneiras diferentes para disponibilizar um serviço de Diretório. Métodos diferentes permitem que diferentes tipos de informações possam ser armazenadas no Diretório, colocando requerimentos diferentes, sobre como aquela informação poderá ser referenciada, requisitada e atualizada, como ela é prote-

gida de acessos não autorizados, etc.. Alguns serviços de Diretório são locais, fornecendo o serviço para um contexto restrito (ex., o serviço finger em uma máquina isolada). Outros serviços são globais, fornecendo o serviço para um contexto muito maior (por exemplo, a própria Internet).

Serviços globais normalmente são distribuídos (Figura 4-1), ou seja, cada servidor é responsável por uma parte apenas. O DNS (Domain Name System) é um exemplo, ele é um tipo de serviço de Diretório, embora bastante especializado.

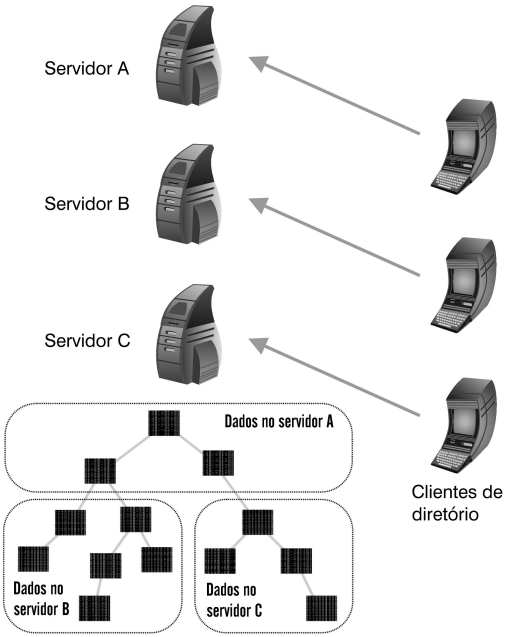


Figura 4-1. Dados de diretório distribuídos em três servidores

Tipo de Informação

O modelo de serviço do Diretório LDAP é baseado em **entradas**. Uma entrada é um conjunto de **atributos** e é referenciada através de um **nome distinto**[2]. O DN é usado para referenciar uma entrada de forma não ambígua. Cada um dos atributos de entrada tem um **tipo** e um ou mais **valores**. Este tipos geralmente são palavras mnemônicas, como `cn` para nome comum, ou `mail` para endereço de correio eletrônico; existem *RFCs* (Request For Comments) que determinam estas palavras. Os valores dependem do tipo de atributo. Por exemplo, um atributo `mail` pode conter o valor <`mari@marilia.br`>. Um atributo `fotoJpeg` irá conter uma fotografia.

Organizando a Informação

No LDAP, entradas de Diretório são organizadas em uma hierarquia de árvore invertida, semelhante em alguns aspectos à organização do DNS. A estrutura desta árvore geralmente reflete limites políticos, geográficos e/ou organizacionais. O nó mais alto (**root**) é tipicamente o componente nome de domínio **dc**[3] de uma companhia, estado ou organização. Abaixo ficam as entradas representando es-

2. *distinguished name (DN).*

3. *domain component*

tados ou organizações nacionais. Abaixo elas podem ser entradas representando pessoas, unidades organizacionais, impressoras, documentos, ou qualquer outra coisa em que você possa pensar. A Figura 4-2 mostra um exemplo de um Diretório LDAP em árvore.

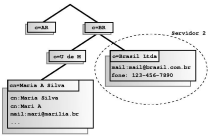


Figura 4-2. Árvore de Diretório LDAP

Apesar de termos entradas para países, o Diretório não possui uma entidade reguladora ou centralizadora como, por exemplo, o *root servers* do DNS. A separação por países, por exemplo, pode ser útil para empresas multi-nacionais. A Figura 4-2 também ilustra uma outra vantagem de um serviço de Diretórios. Os *ramos* da árvore podem estar em máquinas diferentes. No caso da Figura 4-2, a entrada `o=Brasil Ltda` está em um outro computador. Observamos que esta característica também é típica do DNS.

Classes de Objetos

Já vimos alguns tipos de atributos usados nas entradas em um serviço de Diretórios: `mail`, `cn`, `telephoneNumber` e outros. Podemos criar qualquer tipo de atributo, mas isto não é recomendado. No LDAP existem diversas classes de objetos,

e cada classe contém uma lista de atributos obrigatórios e opcionais. Essa lista é definida em uma RFC.

Por exemplo, a classe *person* é definida da seguinte maneira:

```
objetclass person requires objectClass sn, cn allows
    description, seeAlso, telephoneNumber, userPassword
```

O servidor LDAP pode ser configurado para verificar as classes (através da opção `schemacheck`) e forçar o uso correto dos atributos. Isto geralmente é uma boa idéia; com a checagem ligada, por exemplo, será obrigatória a inserção dos atributos `objectClass`, `sn` e `cn`. Quando definirmos que uma entrada do Diretório é da classe *person*, um atributo *description* será opcional. Entradas em Diretórios podem ter várias classes diferentes, basta apenas observarmos os requisitos de atributos de cada classe.

Referenciando a Informação

Uma entrada é referenciada pelo seu nome distinto DN. O DN é único e na sua construção utiliza o *caminho* inteiro, desde a entrada até o topo do Diretório. Por exemplo, na Figura 4-2, DN="cn=Maria A Silva,o=U de M,c=BR". As entradas também podem ser referenciadas através de um RDN (Relative Distinguished Name). Ainda neste exemplo o RDN é cn=Maria A. Silva. Podemos fazer uma comparação com `hostname` (RDN) e FQDN (DN).

Acessando a Informação

O LDAP define operações para consultar e atualizar o Diretório. Operações são fornecidas para adição e remoção de uma entrada do Diretório, modificação de uma entrada existente e modificação do nome de uma entrada. A operação LDAP de busca pode abranger a árvore toda (uma busca com escopo *subtree*) ou apenas um ramo, sem *descer* ou *subir* para os demais. Além de especificar com filtros quais entradas se deseja encontrar, também é possível especificar quais atributos desta entrada estão sendo procurados. Se os atributos não forem especificados, todos serão retornados.

Por exemplo, na Figura 4-2 você pode querer pesquisar toda a sub-árvore de Diretório abaixo da Universidade de Marília, procurando por pessoas com o nome de Maria Silva, recuperando o endereço de correio eletrônico para cada entrada encontrada. O LDAP permite que você faça isto facilmente. Ou você pode querer buscar as entradas diretamente abaixo do `c=BR`, entrada para organizações com a palavra "Brasil" no seu nome, e que tenham um número de telefone. O LDAP permite que você faça isto também. A próxima seção descreve com mais detalhes o que você pode fazer com LDAP e como isto poderá ser útil.

Proteção Contra Acessos Não-Autorizados

Alguns serviços de Diretório não fornecem proteção, permitindo que qualquer

um possa ver as informações. O LDAP fornece um método para autenticação de um cliente, ou prova sua identidade para um servidor de Diretório, pavimentando o caminho para um rico controle de acesso, protegendo as informações contidas no servidor. A sugestão da Conectiva para o arquivo de configuração do servidor contém um exemplo de lista de controle de acesso ACL.

Funcionamento do LDAP

O serviço de Diretório LDAP é baseado em um modelo *cliente-servidor*. Um ou mais servidores LDAP contém os dados criando a árvore de Diretório LDAP. Um cliente LDAP conecta-se a um servidor e faz uma requisição. O servidor responde com a requisição, ou exibe um ponteiro para onde o cliente pode conseguir a informação (tipicamente, outro servidor LDAP). Podemos fazer novamente uma comparação com o DNS, a diferença é que o servidor LDAP não faz buscas recursivas, ou seja, em nome do cliente. O cliente é encarregado de procurar pelo servidor até encontrar a informação desejada.

Conceito e Utilização do *slapd*

O *slapd* é um servidor de Diretório LDAP que pode ser executado em diferentes

plataformas Linux. Você pode usá-lo para fornecer o seu próprio serviço de Diretório. Seu Diretório pode conter qualquer coisa que você queira colocar. Você pode conectá-lo a um serviço de Diretório LDAP global, ou executar o serviço para você mesmo. Algumas das características e potencialidades mais interessantes do *slapd* incluem:

Escolha do banco de dados: O slapd vem com três tipos diferentes de banco de dados que você pode escolher. São eles: LDBM, um banco de dados baseado em disco de alta performance; SHELL, uma interface de banco de dados para comandos arbitrários do Linux ou *scripts* de linha de comando e PASSWD, um banco de dados simples de um arquivo de senhas.

Múltiplas instâncias dos bancos de dados: O *slapd* fornece uma rica e poderosa facilidade no controle de acesso, permitindo a você controlar o acesso a informação em seu(s) banco(s) de dados. Você pode controlar o acesso às entradas baseadas em informação de autenticação LDAP, endereço IP, nome do domínio e outros critérios.

API genérica do banco de dados: O *slapd* utiliza vários processos para ter uma alta performance. Um único sub-processo *slapd* manuseia todas as requisições vindas, reduzindo a quantidade requisitada de recursos do sistema. O *slapd* irá automaticamente selecionar o melhor suporte a vários processos para a sua plataforma.

Controle de acesso: O *slapd* pode ser configurado para usar réplicas. Este esquema de replicação mestre/escravo é vital em ambientes de grande volume, onde um único *slapd* não pode fornecer a disponibilidade ou a confiabilidade necessárias.

Sub-processos: O *slapd* é altamente configurável. Através de um único arquivo de configuração, ele permite a você mudar simplesmente tudo, sempre que você quiser alterar. As opções de configuração têm padrões razoáveis, tornando o seu trabalho muito

mais fácil.

O *slapd* do OpenLDAP 1.2.x é um servidor LDAPv2. A especificação para o LDAPv3 já foi feita e foi implementada no OpenLDAP 2.0; suas novas características são:

LDAPv2 e LDAPv3: O slapd suporta as versões 2 e 3 do LDAP. Ele fornece suporte para as últimas características enquanto mantém interoperabilidade com os clientes existentes. O slapd tem suporte ao IPv4.

Autenticação SASL: O slapd tem suporte a serviços de autenticação diferenciados através do uso de SASL. A implementação SASL do slapd utiliza o software Cyrus SASL com suporte a vários mecanismos incluindo DIGEST-MD5, EXTERNAL.

Camada de Transporte Segura: O slapd fornece proteções de privacidade e integridade através do uso de TLS. A implementação TLS do slapd utiliza o software OpenSSL.

Internacionalização: O slapd suporta Unicode e tags de linguagem.

LDAP e o X.500

O LDAP foi originalmente desenvolvido como um cliente para o X.500, o serviço de Diretório OSI. O X.500 define o Protocolo de Acesso a Diretório (DAP[4]) para

4. Directory Access Protocol.

os clientes usarem quando estiverem em contato com servidores de Diretório. O DAP é um protocolo peso-pesado, que roda sobre uma camada OSI completa, e precisa de uma quantidade significante de recursos computacionais para ser executado. O LDAP roda diretamente sobre o TCP e fornece a maioria das funcionalidades do DAP, a um custo muito menor.

Este uso do LDAP torna fácil acessar o Diretório X.500, mas ainda exige um serviço X.500 completo, para tornar os dados disponíveis aos vários clientes LDAP que estão sendo desenvolvidos. Assim como clientes X.500 DAP completos, um servidor X.500 completo não é um pequeno pedaço de programa para ser executado.

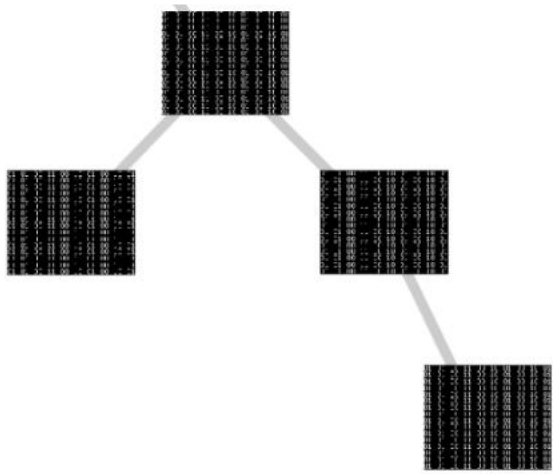
Se você já está executando um serviço X.500 e quer continuar a fazer isto, você provavelmente pode parar de ler este capítulo, ele é todo sobre como executar o LDAP via *slapd*, sem utilizar o X.500. Se você não está usando o X.500, ou quer parar de usar o X.500, ou não tem planos imediatos para executar o X.500, continue lendo.

É possível replicar dados de um servidor de Diretório *slapd* para um DAP X.500; isto permite que sua organização torne seus dados disponíveis como parte de um serviço de Diretório X.500 global em uma base somente para leitura.

Um outro caminho para tornar os dados em um servidor *slapd* disponíveis para a comunidade X.500, seria usando um DAP X.500 para porta de entrada do LDAP.

Replicação

O *slurpd* é um servidor para Linux que auxilia o *slapd*, provendo a replicação do banco de dados. Ele é responsável pela distribuição das mudanças ocorridas no servidor master para o servidor slave (a réplica). Veja a Figura 4-3.



dores

O *slapd* e o *slurpd* se comunicam através de um simples arquivo texto, que é usado para registrar as mudanças. A sintaxe deste arquivo lembra um pouco a sintaxe dos arquivos resultantes do *diff*, no sentido de que estão descritas as entradas ou atributos que devem ser removidos, adicionados ou modificados. O *slurpd* irá se encarregar de aplicar estas mudanças ao servidor da réplica. Durante este processo, a réplica e o master ficarão diferentes.

Instalando e Configurando o LDAP

Instalando os Pacotes

1. Acesse o diretório de pacotes do Conectiva Linux:

```
# cd /mnt/cdrom/conectiva/RPMS/
```

2. Instale o pacote do servidor LDAP openldap:

```
# rpm -ivh openldap-1*
openldap ###################################
```

3. Edite o Arquivo `/etc/openldap/slapd.conf`:

```
suffix "o=minhaorganizacao, c=br"

rootdn "cn=lroot, o=minhaorganizacao, c=br"

rootpw minha-senha

defaultaccess read

access to attr=userpassword by self write by dn="cn=lroot,
o=minhaorganizacao, c=br" write by * none

access to * by self write by dn="cn=lroot, o=minhaorganizacao,
c=br" write by * read
```

```
loglevel 2880
```

`suffix`: a raiz, a base do seu Diretório.

`rootdn`: o login do administrador.

`rootpw`: a senha do administrador; pode ser colocada criptografada.

`default access`: direitos de acesso padrão.

`access to`: aqui começam as definições das ACLs. Estas definições permitem somente que o administrador e o próprio usuário tenham acesso ao atributo `userpassword`.

`loglevel`: tipo de mensagens de log que serão geradas.

Criando o Diretório

Edite o arquivo `/usr/share/openldap/migration/migrate_common.ph`:

```
$DEFAULT_MAIL_DOMAIN = "minhaorganizacao.com.br";

$DEFAULT_BASE = "o=minhaorganizacao,c=br";

$EXTENDED_SCHEMA = 1;
```

$EXTENDED_SCHEMA = 1 irá ativar o suporte a outras classes de objetos, como *person*, por exemplo.

Executando o Script migrate_all_offline.sh

Este script ira pesquisar vários arquivos do diretório `/etc` e criar as entradas no seu Diretório.

```
# cd /usr/share/openldap/migration/
#./migrate_all_offline.sh
Creating naming context entries...
Migrating aliases...
Migrating groups...
Migrating hosts...
Migrating networks...
Migrating users...
Migrating protocols...
Migrating rpcs...
Migrating services...
Migrating netgroups...
Importing into LDAP...
```

```
Migrating netgroups (by user)...
Migrating netgroups (by host)...
Preparing LDAP database...
```

Editando o Arquivo `/etc/openldap/ldap.conf`

```
BASE o=minhaorganizacao,c=br
HOST localhost
```

Inicializando o Servidor LDAP

```
# cds
atd          gpm       keytable          lpd
crond        halt      killall           mars-nwe
dhcpd        hdparm    kudzu             named
functions    httpd     ldap              netfs
gated        inet      linuxconf-setup   network
```

```
# ./ldap start
Iniciando ldap:                            [ OK ]
```

O OpenLDAP é ligado com a biblioteca TCP/Wrappers, por este motivo o controle de acesso pode ser feito através dos arquivos `/etc/hosts.allow` e `/etc/hosts.deny`, além do recurso de ACLs do próprio OpenLDAP. Utilize este arquivos para controlar as máquinas que irão acessar o servidor LDAP. Para acessar através do próprio servidor, caso o arquivo `/etc/hosts.deny` esteja com o parâmetro `ALL:ALL`, insira no `/etc/hosts.allow` a linha

```
    ALL:
            localhost
```

.

Utilizando o LDAP

Fazendo Pesquisas na Linha de Comando

Abra um terminal e utilize os seguintes comandos:

- para verificar tudo que existe no Diretório:

```
$ ldapsearch "objectclass=*"
o=minhaorganizacao,c=br
o=minhaorganizacao
objectclass=top
objectclass=organization
objectclass=domainRelatedObject
associateddomain=minhaorganizacao.com.br
...
```

- para verificar se os usuários foram inseridos:

```
$ ldapsearch uid=login-do-usuario
uid=login-do-usuario,ou=People,o=minhaorganizacao,c=br
```

```
uid=login-do-usuario
cn=login-do-usuario
sn=login-do-usuario
mail=login-do-usuario@minhaorganizacao.com.br
objectclass=person
objectclass=organizationalPerson
objectclass=inetOrgPerson
objectclass=account
objectclass=posixAccount
objectclass=top
objectclass=kerberosSecurityObject
krbname=login-do-usuario@MINHAORGANIZACAO.COM.BR
loginshell=/bin/bash
uidnumber=550
gidnumber=907
homedirectory=/home/login-do-usuario
```

Note que o atributo `userpassword` não apareceu nesta busca.

- para verificar se as senhas foram inseridas usando a senha do administrador do Diretório:

```
$ ldapsearch -D cn=lroot,o=minhaorganizacao,c=BR -W uid=meu-usuario
Enter LDAP Password:
```

```
uid=meu-usuario,ou=People,o=minhaorganizacao,c=br
uid=meu-usuario
cn=meu-usuario
sn=meu-usuario
mail=meu-usuario@minhaorganizacao.com.br
objectclass=person
objectclass=organizationalPerson
objectclass=inetOrgPerson
objectclass=account
objectclass=posixAccount
objectclass=top
objectclass=kerberosSecurityObject
userpassword={crypt}VazDY6ytbW/YI
krbname=meu-usuario@MINHAORGANIZACAO.COM.BR
loginshell=/bin/bash
uidnumber=500
gidnumber=500
homedirectory=/home/meu-usuario
```

De acordo com as ACLs, o administrador **sempre** tem acesso a todos os atributos.

- para verificar a senha do seu usuário usando sua própria senha:

```
$ ldapsearch -D uid=meu-usuario,ou=people,o=minhaorganizacao,c=br -W
uid=meu-usuario
Enter LDAP Password:
uid=meu-usuario,ou=People,o=minhaorganizacao,c=br
uid=meu-usuario
cn=meu-usuario
sn=meu-usuario
mail=meu-usuario@minhaorganizacao
objectclass=person
objectclass=organizationalPerson
objectclass=inetOrgPerson
objectclass=account
objectclass=posixAccount
objectclass=top
objectclass=kerberosSecurityObject
userpassword={crypt}VazDY6ytbW/YI
krbname=meu-usuario@MINHAORGANIZACAO.COM.BR
loginshell=/bin/bash
uidnumber=500
gidnumber=500
homedirectory=/home/meu-usuario
```

Devido às ACLs, um usuário somente tem acesso ao seu próprio atributo `user-`

```
password.
```

Configurando o Netscape Communicator

Quando se trabalha com servidores LDAP, é comum existir uma limitação para a quantidade máxima de respostas retornadas pelo servidor. Esta limitação existe sempre no servidor, mas pode existir também no cliente, como no caso do Netscape.

Entre no ambiente gráfico com o seu login de usuário, execute o Netscape Communicator e faça as seguintes configurações:

1. No Livro de Endereços (**Alt**-**Shift**-**2**) clique em Arquivo→Diretório Novo...; surgirá a janela *Directory Info* (Figura 4-4). Basta preencher esta janela da seguinte maneira:

Figura 4-4. Informações do Diretório

2. No campo **Diretórios**, selecione o Diretório que você adicionou, efetue uma pesquisa de todos os usuários que existem no Diretório digitando no campo *digite o nome que está procurando* um ***** seguido de um **Enter**. Você deverá visualizar todos os usuários encontrados no diretório. Será possível ver aqui também os usuários administrativos, como `bin`, `daemon`, etc.. Eles podem ser removidos do Diretório.

3. Configure o correio do Netscape para utilizar o **endereçamento de mensagens** através do servidor de Diretório.

   Em Editar→Preferências, clique na seta para expandir a categoria **Correio e Notícias** e selecione a subcategoria **Endereçamento**.

   Habilite a opção **Servidor de Diretório:** e selecione o servidor que você adicionou (no nosso exemplo: *minhaorganização*).

4. Sempre que for enviar uma mensagem bastará colocar um dado qualquer, ou apenas parte dele, de um usuário existente no Diretório. O Netscape se encarregará de preencher o restante. Caso exista mais de uma entrada, ele mostrará a lista de usuários encontrados, para você selecionar o usuário desejado.

Acessando o Servidor LDAP por URLs

Também é possível usar o Netscape Communicator para se comunicar com um servidor LDAP através do navegador. A sintaxe é a seguinte:

```
ldap[s]://<hostname><:port>/<base_dn>?<atributos>?<escopo>?<Filtro>
```

O [s] é usado quando temos uma conexão segura (ssl). Vejamos um exemplo com algumas utilizações de URLs do Netscape para o LDAP:

Exemplo 4-1. Utilizando as URLs do Netscape Communicator

- `ldap://localhost/o=minhaorganizacao,c=br??sub?`

  Isto retornará do servidor cada registro do banco de dados.

- `ldap://localhost/o=minhaorganizacao,c=br?cn,mail?sub?`

  Isto irá retornar apenas os objetos (pessoas) nome e endereço de correio eletrônico para cada pessoa do banco de dados.

- `ldap://localhost/o=minhaorganizacao,c=br??sub?(cn=maria)`

  Retornará apenas o registro *maria*.

- `ldap://localhost/o=minhaorganizacao,c=br??sub?(cn=maria*)`

  Trará para você qualquer registro em que o nome inicie com *maria*.

- `ldap://localhost/o=minhaorganizacao,c=br??sub?(sn=silva)`

  Isto lhe dará todos os registros que tenham o sobrenome *silva*.

Autenticação e NSS com o LDAP

Seu servidor LDAP pode autenticar usuários, usando um mecanismo chamado PAM[5] (módulos de autenticação plugáveis). Desde o princípio do Linux, a autenticação de um usuário foi feita através da entrada de uma senha pelo usuário, e o sistema verificando se a senha digitada corresponde a senha oficial encriptada, que fica armazenada no arquivo `/etc/passwd`. Isto foi apenas no início. Desde então, um número de novos caminhos para a autenticação de usuários vem se tornando popular, incluindo substituições mais complicadas, como por exemplo para o arquivo `/etc/passwd` e dispositivos de hardware chamados de *Smart Cards*.

O problema é que a cada vez que um novo esquema de autenticação é desen-

5. Pluggable Authentication Module.

volvido, requer que todos os programas necessários (login, ftpd, etc.) sejam reescritos para suportar este novo esquema. O PAM fornece um caminho para desenvolver programas que são independentes do esquema de autenticação. Estes programas precisam de módulos de autenticação, anexados a eles em tempo de execução, para que possam funcionar.

A seguir veremos como configurar o seu sistema para fazer a autenticação via LDAP. O programa authconfig realiza quase todas estas alterações. Para fazer o uso de SSL (criptografia) com LDAPv2 em um servidor remoto será necessário instalar o pacote stunnel.

Autenticação no LDAP e o NSS

Como superusuário, entre no diretório onde se encontram os pacotes da distribuição e execute:

```
# rpm -ivh nss_ldap* pam_ldap*
nss_ldap   ##############################
pam_ldap   ##############################
```

Configurando o PAM para Utilizar o LDAP

No diretório `/usr/share/doc/pam_ldap-XX`, onde `XX` é a versão do módulo instalado, você encontrará o diretório `pam.d.conectiva` que é a recomendação da Conectiva para o conteúdo do diretório `/etc/pam.d`. Faça um backup do seu diretório `/etc/pam.d` original e copie o novo diretório recomendado para o mesmo local:

```
# mv /etc/pam.d /etc/pam.d.org
# cp -R /usr/share/doc/pam_ldapXX/pam.d.conectiva /etc/pam.d
```

Execute o aplicativo authconfig como superusuário; você terá a Figura 4-5 ilustrando as configurações para o nosso exemplo:

```
# authconfig
```

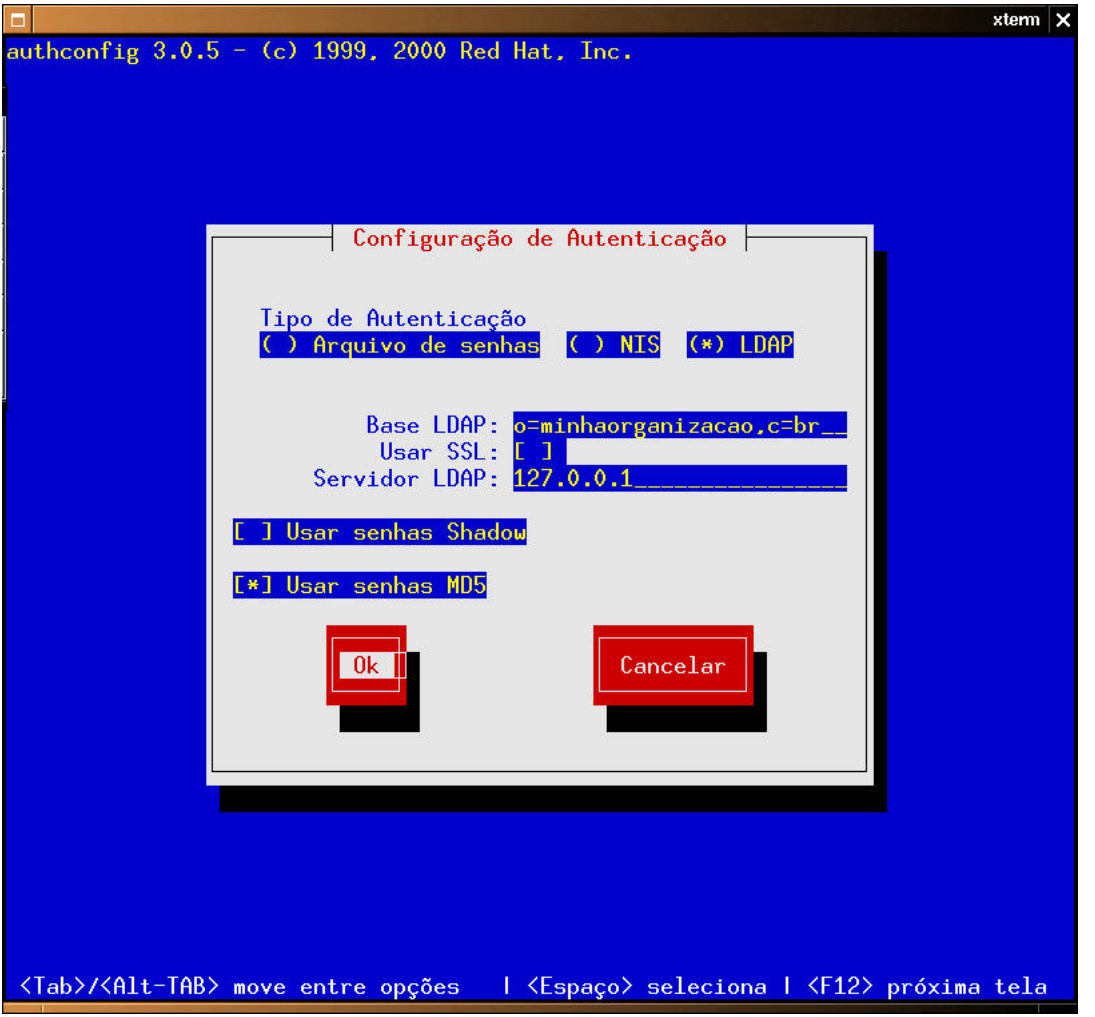


Figura 4-5. Configuração de Autenticação

A opção USAR SSL só estará habilitada se o authconfig conseguir detectar a instalação do pacote stunnel. Com essa instalação seu sistema tentará autenticar o usuário localmente (através dos arquivos `/etc/shadow`, `/etc/passwd`, etc.); em caso de resposta negativa, usará o LDAP com a mesma senha, sem pedir duas senhas para o usuário.

Testando a Autenticação e o NSS

Para testar a autenticação e o NSS, faça uma cópia do seu `/etc/passwd`:

```
# cp /etc/passwd /etc/passwd.org
```

Remova deste arquivo um usuário com o comando **# userdel `nome-do-usuário`**, para ter certeza de que ele não será encontrado no `/etc/passwd`.

Então experimente:

```
$ ls -la /home
```

Será possível visualizar o nome do usuário, em vez do seu UID. Experimente também acessar o Conectiva Linux, com o usuário que havia no arquivo `/etc/passwd`.

Se não for utilizar LDAP para autenticação, não esqueça de recuperar o seu `/etc/passwd` original para continuar com o uso do sistema:

```
# mv /etc/passwd.org /etc/passwd
```

Adicionando e Removendo Usuários Via LDAP

Para adicionar e remover usuários do LDAP, existem dois comandos que são utilizados para esta tarefa. São eles: **ldapadduser** e **ldapdeluser**. Executando estes comandos sem parâmetros, será apresentada na tela a forma de uso. Você poderá usá-los da seguinte maneira:

```
# ldapadduser meu-usuario
```

ou

```
# ldapdeluser meu-usuario -r
```

Na remoção do usuário, foi usado o parâmetro **-r**. Ele é utilizado quando se deseja remover o `/home/meu-usuario` juntamente com a conta do usuário. Se não for esta a intenção, não utilize este parâmetro.

Acrescentando o log do LDAP

No arquivo `/etc/syslog.conf` se encontra a seguinte linha:

```
local4.* /var/log/ldap.log
```

Você poderá acompanhar possíveis erros de autenticação no `/var/log/messages`, e o log do LDAP em `/var/log/ldap`.

Ferramentas Gráficas para o LDAP

Além do Netscape existem outras ferramentas LDAP que podem ser usadas no ambiente gráfico. Pesquisas, visualização e até mesmo manutenções na base de dados podem ser feitas através destes programas.

O Cliente de LDAP GQ

O GQ é um cliente LDAP gráfico, com uma interface simples escrito para o Gnome, sendo possível executá-lo em outros gerenciadores de janela também. Instale-o da seguinte forma: como superusuário no diretório `RPMS` do CD2 do

Conectiva Linux execute:

```
# rpm -ivh gq-*
gq ################################
```

Como usuário normal inicialize o programa com o comando **gq**. Sua configuração também é simples, bastando adicionar o servidor LDAP que você gostaria de usar, e a Base DN do Diretório. Um recurso interessante deste aplicativo é o modo de navegação, sendo possível observar o Diretório em árvore e ter uma visão completa de todos os dados do Diretório. Observe na Figura 4-6 os detalhes deste exemplo:

```
$ gq
```

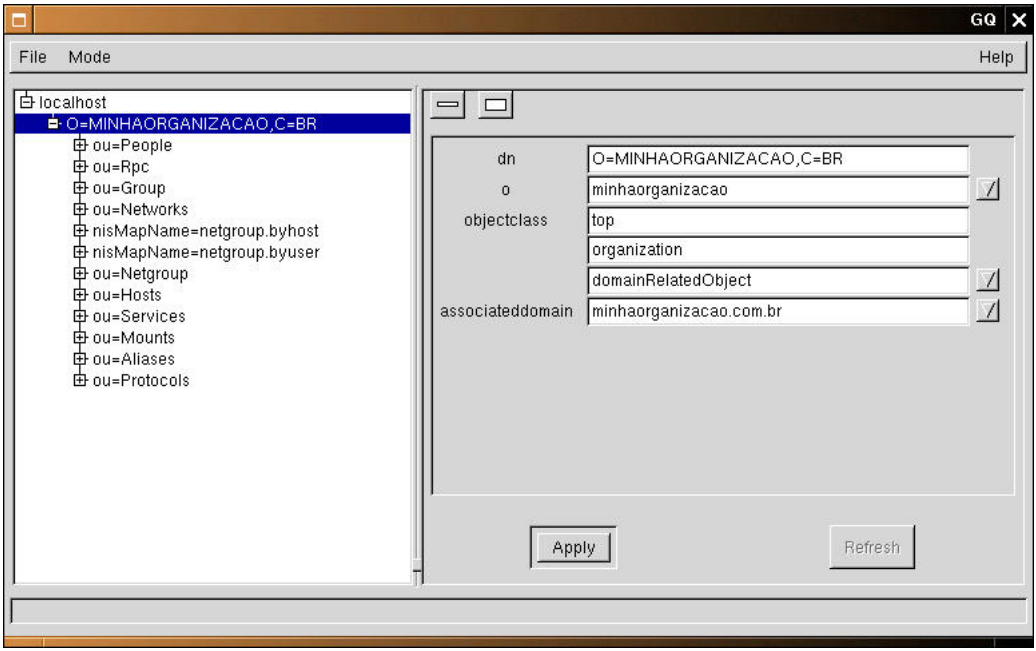


Figura 4-6. O Cliente de LDAP GQ

Acesso Móvel

O objetivo do Acesso Móvel é que em qualquer lugar que você esteja na rede, você poderá recuperar seus bookmarks, preferências, filtros de e-mail, entre outros, utilizando o Netscape e um servidor LDAP. Esta é uma característica muito boa: imagine que, de qualquer lugar que você acesse a Web, você poderá ter as suas próprias configurações no navegador. Se você for viajar e precisar acessar aquele site de notícias que está armazenado em seu bookmarks local, não haverá problemas: envie os bookmarks e outros arquivos de configuração para um servidor LDAP e você poderá recuperá-los depois, independente do lugar em que você estiver.

Implementando o Acesso Móvel

Para implementar o Acesso Móvel você terá de seguir os seguintes passos:

- Alterar seu arquivo de descrição de atributos.
- Alterar seu arquivo de descrição `objectclass`.
- Alterar o arquivo LDIF para incluir os perfis.
- Configurar o Netscape Navigator para usar o servidor LDAP como um servidor de Acesso Móvel.

- Reiniciar o servidor LDAP com as novas configurações.

Alterando o Arquivo de Atributos

Adicione estes novos atributos na lista do arquivo `/etc/openldap/slapd.at.conf`:

```
attribute       nsLIPtrURL                      ces
attribute       nsLIPrefs                       ces
attribute       nsLIProfileName                 cis
attribute       nsLIData                        bin
attribute       nsLIElementType                 cis
attribute       nsLIServerType                  cis
attribute       nsLIVersion                     bin
attribute       nsServerPort                    cis
```

Alterando o Arquivo `objectclass`

Você também deve adicionar algumas classes novas para habilitar o Acesso Móvel. Isto pode ser feito no arquivo `/etc/openldap/slapd.oc.conf`:

```
objectclass nsLIPtr
       requires
         objectclass
       allows
         nsLIPtrURL,
         owner

    objectclass nsLIProfile
       requires
         objectclass,
         nsLIProfileName
       allows
         nsLIPrefs,
         uid,
         owner

    objectclass nsLIProfileElement
       requires
         objectclass,
         nsLIElementType
       allows
         owner,
```

```
        nsLIData,
        nsLIVersion

    objectclass nsLIServer
       requires
        objectclass,
        serverhostname
       allows
        description,
        cn,
        nsServerPort,
        nsLIServerType,
        serverroot
```

Personalizando o `slapd.conf`

O próximo passo é editar o seu arquivo `/etc/openldap/slapd.conf`. A seguir apresentaremos um exemplo deste arquivo que suporta Acesso Móvel. Modifique e adicione as seguintes linhas no arquivo padrão:

```
suffix "o=top"
```

```
rootdn "cn=root, o=top"


lastmod on
access to dn=".*,ou=Roaming,o=top" by dnattr=owner write
access to attr=userpassword
        by self write
        by * none
```

Alterando o Arquivo LDIF

Agora você tem de alterar o seu arquivo LDIF, adicionando entradas de perfil para cada usuário que irá utilizar a opção de Acesso Móvel do Netscape. Crie um arquivo `/etc/openldap/ldif` e acrescente as seguintes linhas, como no exemplo:

```
dn: o=top
objectclass: top


dn: ou=People, o=top
objectclass: top
objectclass: organizationalUnit
```

```
dn: cn=meu-usuario, ou=People, o=top
objectclass: top
objectclass: person
userpassword: senha-do-usuario

dn: ou=Roaming, o=top
objectclass: top
objectclass: organizationalUnit

dn: nsLIProfileName=meu-usuario, ou=Roaming, o=top
objectclass: top
objectclass: nsLIProfile
owner: cn=meu-usuario, ou=People, o=top
```

Adicione esta nova entrada no diretório com o comando **ldapadd**:

 # ldapadd -D "cn=root, o=top" -w minha-senha -f ldif

Reinicializando o Servidor LDAP

Para as alterações entrarem em vigor, será necessário reinicializar o servidor

LDAP. Para isto, como superusuário execute:

```
# /etc/rc.d/init.d/ldap restart
Desligando ldap:  [ OK ]
Iniciando ldap:   [ OK ]
```

Configurando o Netscape

Para configurar o Netscape e habilitar o Acesso Móvel através do seu servidor LDAP, siga os seguintes passos:

- Clicando em Editar→Preferências na categoria usuário, marque a opção **Habilite Acesso Móvel para este perfil de usuário**. Digite no campo Nome do Usuário o login a ser usado no servidor LDAP; se desejar digitar a senha apenas uma vez (quando o Netscape for reiniciado), marque a opção Lembre de Minha Senha de Acesso Móvel.

- Na subcategoria Informações do Servidor, digite no campo Endereço:

  ```
  url="ldap://localhost/nsLIProfileName=meu-usuario,ou=Roaming,o=top,c=br"
  ```

  Em DN do Usuário digite o seguinte:

  ```
  cn=meu-usuario,ou=People,o=top,c=br
  ```

- Após ter feito estas configurações, feche o Netscape Arquivo→Sair (**Alt-Q**) e abra-o novamente. Surgirá uma janela pedindo a senha para o servidor de Acesso Móvel; clicando no botão Opções você verá uma janela equivalente a da Figura 4-7.

Figura 4-7. Informações do Servidor

Esta janela contém o endereço do servidor e o DN do usuário que você configurou anteriormente. Verifique se as informações estão todas corretas.

Com isto você poderá utilizar o Netscape remotamente através do LDAP como um servidor de Acesso Móvel, tendo disponível os seus Marcadores, Cookies, Filtros de Correio, Livro de Endereços e Preferências do Usuário.

Capítulo 5. DNS

Neste capítulo apresentamos informações sobre instalação, configuração e manutenção de um servidor DNS (Domain Name System[1]) em uma máquina com Linux. Você aprenderá como criar um domínio e administrar as máquinas ligadas a ele. Veremos como fazer com que estações possam utilizar o servidor DNS para acessar umas às outras através de seus respectivos nomes. Além disso, você aprenderá um pouco sobre como o DNS consegue organizar um número absurdamente grande de máquinas conectadas possibilitando que se enxerguem, umas às outras, em uma rede.

Introdução e Conceitos

O DNS converte nomes de máquinas em endereços IP. Ele mapeia nomes para IPs e IPs para nomes. Ele é um banco de dados distribuído, permitindo, assim, que uma seção seja gerenciada localmente e esteja, mesmo assim, disponível para todo o mundo.

Os servidores de nomes compõem a parte servidor do mecanismo cliente-servidor do DNS. Os servidores de nomes contêm informações sobre uma parte do banco de dados e as torna disponíveis para os clientes ou *resolvedores*.

1. Sistema de nomes de domínio.

A estrutura do banco de dados do DNS é semelhante à estrutura do sistema de arquivos do Conectiva Linux, representada por uma árvore invertida. No sistema de arquivos, tudo parte do diretório raiz; no DNS tudo parte de um nulo (“”), representado em texto como um ponto (“.”).

Cada ramo da árvore representa uma partição do banco de dados geral - um *diretório* no sistema de arquivos do Conectiva Linux ou um *domínio* no DNS. Cada domínio pode ser dividido em mais partes chamadas *subdomínios*.

Cada domínio tem um nome. Este nome é dividido em duas partes. A primeira identifica sua relação ao domínio pai. A segunda parte é o *nome do domínio*, que identifica sua posição no banco de dados. Por exemplo, podemos ver que em `kepler.minhaorganizacao.com.br`, o nome de domínio é `minhaorganizacao.com.br` e o nome da máquina é `kepler`.

Cada domínio pode ser administrado por uma organização diferente. Estas organizações podem quebrar estes domínios em subdomínios e delegar o controle dos mesmos a outras organizações, tornando, assim, a administração extremamente descentralizada.

A estrutura pode parecer um tanto complicada, mas é muito mais simples do que parece. Tudo é um questão de partir de um domínio e ir descendo, até chegar a uma máquina (ou *host*).

Funcionamento do DNS

Espaço de Nomes de Domínio

Como já foi mencionado anteriormente, o DNS funciona de forma análoga ao sistema de arquivos do Conectiva Linux. Cada unidade de dados do banco distribuído do DNS é indexada por um nome. Este nome é, basicamente, uma rota em uma árvore invertida, chamada de *Espaço de Nomes de Domínios*. No topo desta árvore está o domínio raiz. Como em um sistema de arquivos, cada ramo da árvore de domínios pode ter um número qualquer de outros ramos.

Nomes de Domínio

Cada ramo da árvore de domínios é identificado por um nome de, no máximo, 63 caracteres. Estes nomes não podem ser nulos, já que o nulo é reservado ao domínio raíz da árvore.

Quando o domínio raiz aparece no nome de domínio de um ramo, o nome parece terminar com um ponto, quando, na verdade, ele termina com um ponto e o domínio raíz, que é representado por uma seqüência nula de caracteres. Assim, alguns programas interpretam um ponto no final de um nome de domínio como significando que o nome de domínio é absoluto. Um nome de domínio abso-

luto identifica a localização do ramo na hierarquia sem ambigüidade. Nomes não seguidos por pontos são chamados de nomes relativos, já que eles não especificam sua localização exata na árvore, podendo, assim, ser relativos a diversos pontos da mesma.

O sistema de nomes de domínios requer que os ramos irmãos (ou seja, os ramos que partem diretamente de um ramo comum) tenham nomes únicos. Comparando com o sistema de arquivos, da mesma forma como não se pode ter dois `/usr/bin`, não se pode ter dois `copernico.minhaorganizacao.com.br`. Isso não chega a ser um problema, já que os nomes só têm de ser únicos entre os ramos filhos, ou seja, é possível existir dois ramos de mesmo nome desde que os mesmos não sejam irmãos.

Domínios

Um *domínio* nada mais é do que uma subárvore do espaço de nomes de domínio. O nome de um domínio é o nome do ramo que está no topo daquele domínio. Por exemplo, o topo do domínio `minhaorganizacao.com.br` é um ramo chamado `com.br`, da mesma forma como você esperaria encontrar o diretório `/usr` no topo de `/usr/lib`.

Cada subárvore é considerada parte de um domínio. Assim como um nome de domínio pode estar em diversas subárvores, um nome de domínio pode estar em diversos domínios. Por exemplo, `minhaorganizacao.com.br` faz parte do domínio `com.br` e também do domínio `br`.

Como um domínio é basicamente uma árvore de nomes de domínio, chega-se a conclusão de que as máquinas conectadas ao sistema também devem ser domínios. Lembre-se de que os nomes de domínio são apenas índices do banco de dados do DNS; assim, as máquinas são os nomes de domínio que apontam para informações sobre máquinas individuais.

Os domínios localizados nas pontas dos ramos da árvore de domínios geralmente representam máquinas individuais. Os nomes de domínios podem apontar para um endereço de rede ou informações de roteamento de correio eletrônico. Os domínios internos podem apontar para uma máquina específica e podem apontar para informações estruturais sobre os subdomínios. Por exemplo, `minhaorganizacao.com.br` pode ser o nome do domínio da Minha Organização e ainda o nome de domínio de uma máquina que encaminha correio eletrônico entre a Internet e a empresa.

O Espaço de Nomes de Domínios da Internet

O Sistema de Nomes de Domínios não impõe muitas regras aos nomes associados aos domínios. Além disso, nenhum significado particular é associado aos nomes de um nível particular. Quando você cria um domínio, você pode definir suas próprias regras para os nomes.

O espaço de nomes de domínios atual da Internet tem algumas regras para a sua estruturação. Em especial, os domínios próximos à raiz seguem certas tradições.

Isso evita que os nomes de domínios pareçam desorganizados e sem sentido.

Domínios de Primeiro Nível

Originalmente, a Internet foi dividida em 7 domínios de uma maneira a dividir a Internet por tipo de organização. Estes domínios foram chamados de *Domínios de Primeiro Nível* ou DPN. Os domínios originais são:

com: Organizações comerciais

edu: Organizações de ensino

gov: Organizações governamentais

mil: Organizações militares

net: Organizações da rede

org: Organizações internacionais

É possível notar que os domínios acima parecem ser específicos para organizações norte-americanas. Isso se deve ao fato de a Internet ter-se originado da ARPANET, que era um projeto norte-americano. Na época, não se podia prever o sucesso da ARPANET e a conseqüente criação da Internet. Para acomodar a internacionalização da Internet, foi feita uma alteração nos DPNs. Foram reservados, além dos sete domínios originais, domínios que designavam localizações geográficas. Estes nomes de domínios seguem uma padronização internacional

chamada ISO 3166. Esta padronização define códigos de duas letras para cada país do mundo (por exemplo, *br* para Brasil).

Embora os domínios originais devessem continuar a ser respeitados dentro de cada um dos domínios internacionais, isto acabou não ocorrendo. Cada país definiu suas próprias regras para divisão. A maioria manteve a divisão por organizações, embora não necessariamente com os domínios originais. A Inglaterra, por exemplo, define `co.uk` para instituições comerciais e `ac.uk` para instituições acadêmicas. Já o Brasil manteve os domínios originais (por exemplo, `com.br`, `net.br`) e, recentemente, criou domínios adicionais como `eti.br`, para especialistas em tecnologia da informação, `psi.br` para provedores de acesso, `g12.br` para instituições de ensino de 1º e 2º graus, etc.. Você pode obter mais informações sobre outros domínios na página da FAPESP http://registro.br/.

Delegação

Um dos requisitos para o sucessor do `hosts.txt` era a descentralização da administração; isto foi conseguido através da *delegação*. A delegação de domínios não é diferente do processo de delegação em uma empresa: o trabalho vai sendo mandado para o nível mais abaixo.

Ora, um domínio pode ser dividido em subdomínios. Cada um desses subdomínios pode ser delegado a uma outra organização e assim por diante. A organização delegada recebe a responsabilidade de manter os dados daquele subdomínio. O responsável pelo domínio não tem realmente informações sobre as máquinas ligadas àquele domínio, mas apenas informações sobre os mantenedores dos sub-

domínios.

Servidores de Nomes

Os programas que guardam as informações sobre as máquinas conectadas são chamados *Servidores de Nomes*. Estes servidores de nomes normalmente mantêm informações completas sobre um determinado espaço de nomes de domínio, chamado de *zona*. Um único servidor de nomes pode ter autoridade sobre múltiplas zonas.

A diferença entre zona e domínio é bastante sutil. Uma zona contém informações sobre os nomes de domínios e os dados que um domínio contém, com exceção dos nomes de domínios delegados.

Porém, se um subdomínio de um domínio não foi delegado a ninguém, a zona contém os nomes de domínio e os dados daquele subdomínio, também. A diferença entre zona e domínio fica mais clara na Figura 5-1.

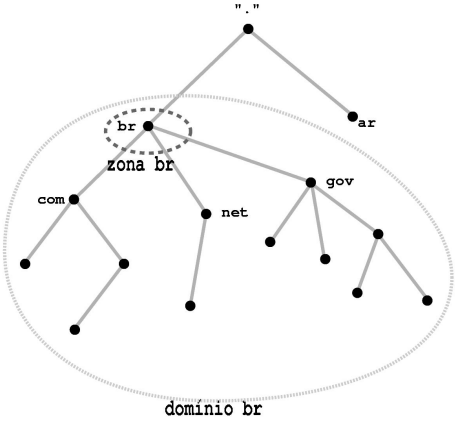


Figura 5-1. Zona vs. Domínio

Pode-se ver que o uso de zonas em vez de domínios evita que um domínio tenha que ter mais informações do que o necessário, pois ele conteria informações delegadas a outros servidores de nomes.

Note que, quando é feita delegação, o servidor de nomes não tem informações sobre as máquinas de um subdomínio, de forma que, quando lhe é requisitada alguma informação sobre uma dessas máquinas, o servidor de nomes se resume a responder com o endereço do servidor de nomes responsável por aquele subdomínio, para que a mesma pesquisa seja passada para o mesmo.

Existem dois tipos de servidores de nomes: os *primários* e os *secundários*. Os servidores de nomes primários usam os dados tirados de arquivos localizados nas máquinas em que os mesmos são executados. Um servidor secundário utiliza seus

dados de outro servidor da zona. Quando um servidor secundário é acionado, ele busca informações da zona de um servidor primário.

Estes dois tipos foram criados para facilitar a tarefa de administração. Após criar um servidor de nomes para a sua zona, não é necessário fazer tudo de novo para cada novo servidor de nomes na mesma zona. Basta criar servidores secundários que utilizem informações do seu servidor primário.

Resolvedores

Os clientes que acessam um servidor de nomes são chamados *Resolvedores*. Os programas sendo executados em uma máquina que precisam de informações sobre o domínio utilizam o *resolvedor*. O resolvedor cuida de:

- Consultar um servidor de nomes;
- Interpretar as respostas (que tanto podem ser registro como erros);
- Retornar a informação para os programas que a requisitaram.

Resolução de Nomes

O processo pelo qual os servidores de nomes fornecem informações sobre as

zonas e domínios é chamado de *resolução de nomes*. Já que o espaço de nomes é estruturado como uma árvore invertida, o servidor de nomes só precisa de uma parte da informação para encontrar seu caminho a qualquer ponto da árvore.

Cache

Uma das características que aceleram o processo de procura de uma máquina é chamada de *caching*.

Um servidor de nomes procurando uma máquina pode ter de enviar um número considerável de pesquisas até encontrá-la. Enquanto faz isso, ele recebe uma grande quantidade de informações sobre os outros servidores.

O servidor de nomes guarda esta informação para acelerar futuras pesquisas. Na próxima vez em que o servidor de nomes tiver de pesquisar algo sobre isso, o processo será acelerado. Mesmo que ele não tenha a resposta em *cache*, ele pode ter informações sobre o servidor de nomes responsável por sua zona.

Instalando e Configurando o DNS

Instalando os Pacotes

1. Acesse o diretório de pacotes do Conectiva Linux:

```
# cd /mnt/cdrom/conectiva/RPMS/ #
```

2. Instale o servidor de nomes BIND:

```
# rpm -ivh bind-8.*.rpm
bind ############################## #
```

Configurando o Servidor DNS

A configuração do seu servidor de DNS pode ser realizada com facilidade através do Linuxconf, o utilitário de configurações do Conectiva Linux.

É possível configurar o serviço de servidor de nome apenas através da edição

manual de arquivos de configuração, mas este capítulo se concentrará na configuração que utiliza o Linuxconf.

Entre no Linuxconf e vá, então, para o menu Ambiente de Rede→Tarefas de Servidor→DNS. Você verá a tela inicial de configuração como a Figura 5-2.

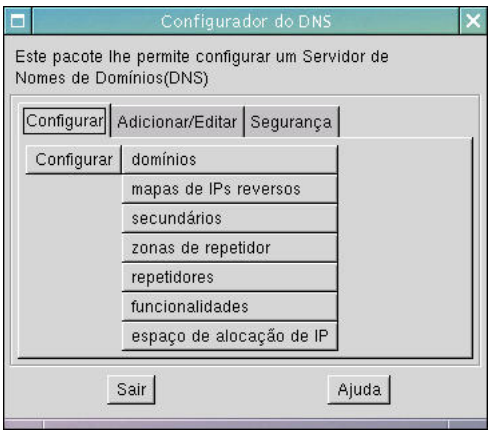


Figura 5-2. Tela de Configuração do Servidor DNS

A partir desta tela, você pode configurar o seu servidor DNS inteiro sem a necessidade de edição dos arquivos de configuração.

Para começar, é necessária a configuração básica do servidor, isto é, nome do domínio, endereço de correio eletrônico do administrador e máquina servidor. Para realizar estas configurações, pressione o botão domínios. Uma tela aparecerá onde você pode adicionar, editar ou excluir os domínios de DNS. Pressione

Adicionar para que possamos adicionar um domínio. Uma tela semelhante à Figura 5-3 aparecerá:

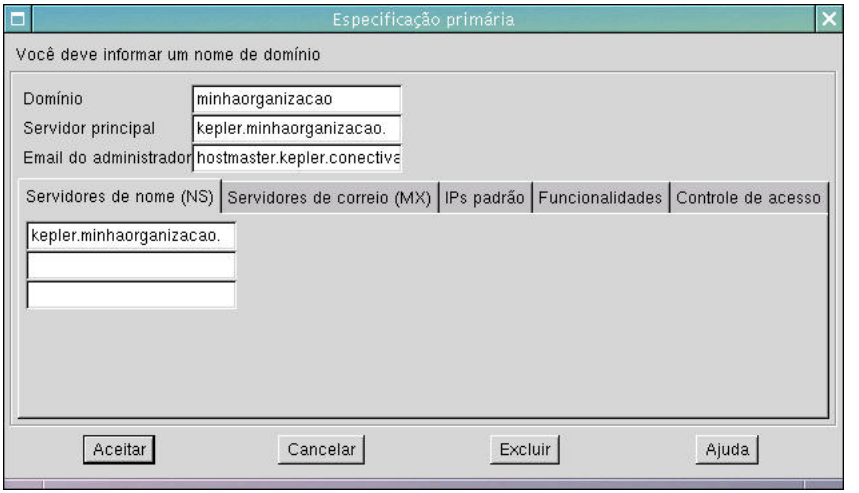


Figura 5-3. Adicionando um Domínio

Nesta tela, você deve informar os dados referentes ao seu domínio.

Domínio: este é o nome do domínio, no caso, estamos criando um domínio chamado de `minhaorganizacao`. Vide a seção *Domínios* para mais informações.

Servidor principal: este é o nome da máquina onde o servidor de nomes estará sendo executado. No caso de nosso exemplo, o domínio `minhaorganizacao` será controlado pela

máquina `ns.minhaorganizacao.`

Email do administrador: este é o endereço de correio eletrônico do administrador de sistema. Em caso de problemas, este administrador poderá ser avisado. Note que usa-se um ponto (“.”) no lugar de arroba (“@”) neste campo.

Há, ainda, algumas outras configurações que podem ser feitas nesta tela, mas que não cobriremos neste livro. São elas:

Divulgando o DNS(NS): em uma configuração simples, basta o nome do servidor principal. Além disso, você deverá informar aqui quais serão os servidores secundários de seu domínio.

Divulgando o EMAIL(MX): aqui você pode definir o servidor que encaminha as mensagens de correio eletrônico do seu domínio para a Internet.

IPs padrão: aqui você pode definir um ou mais endereços de IP de máquinas que serão acessadas através do domínio. É normal pesquisas em servidores de nome se referirem apenas ao domínio, mas os domínios não possuem IP’s, apenas máquinas os têm, assim, definindo IPs padrão; uma pesquisa ao domínio `minhaorganizacao` irá resultar naquele IP padrão.

Funcionalidades: aqui podem ser definidas algumas funcionalidades do domínio. Por exemplo, pode-se definir de quanto em quanto tempo os servidores secundários serão atualizados.

Access control: você pode definir algumas opções de segurança para seu servidor de nomes.

Estas configurações já são suficientes para que o servidor de nomes possa fun-

cionar corretamente. Mas há muito mais configurações que podem ser feitas ainda em seu servidor de DNS.

Configurando Mapas de IPs Reversos

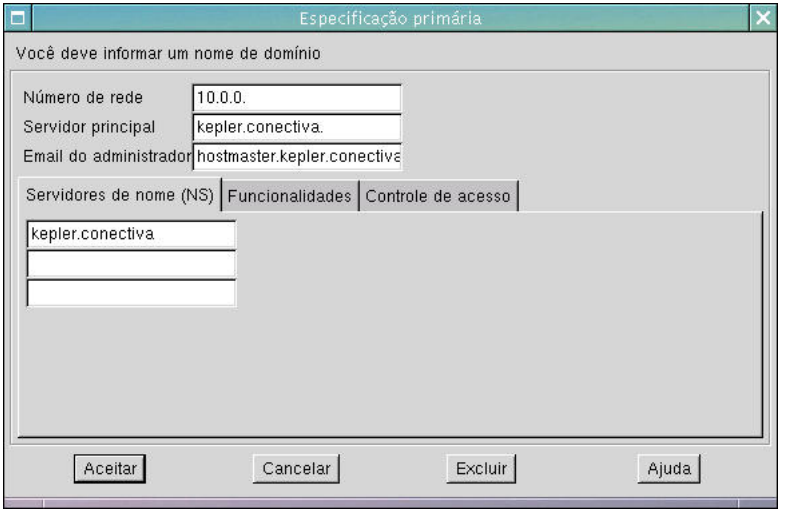


Figura 5-4. Adicionando um Mapa de IP Reverso

A tarefa principal do servidor de nomes é fazer o mapeamento entre nomes de

máquinas e endereços IP. Ele realiza automaticamente a tradução de um nome de máquina para um endereço IP. Porém, às vezes é necessário fazer a tradução de um endereço IP para um nome. Isto é feito através de mapas de IPs reversos.

A configuração de um mapa de IP reverso é muito semelhante à configuração de um domínio, basta comparar a Figura 5-3 e a Figura 5-4 para verificar as similaridades.

Configurando um Servidor Secundário

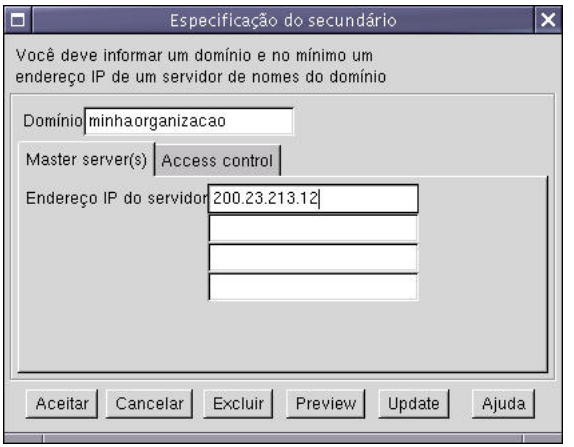


Figura 5-5. Configurando um Servidor Secundário

A configuração de servidores secundários é bastante simples, basta especificar o nome do domínio para o qual este servidor será secundário e informar o IP do servidor primário de onde este servidor buscará as informações. Veja a seção *Servidores de Nomes* para mais informações sobre servidores primários e secundários.

Forward Zones

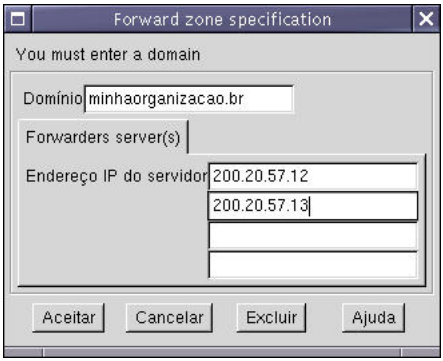


Figura 5-6. Configurando Forwarders

Existem casos em que não é interessante que o servidor de nomes envie uma grande quantidade de pacotes para fora da rede local. Isto pode ocorrer por diversos motivos, como, por exemplo, no caso de empresas que se conectam com

a matriz através de antenas. Seria ineficiente que o servidor ficasse tentando localizar algo através do servidor da matriz. Para isso, pode-se criar servidores de nomes que servem para criar um grande *cache* (veja a seção *Cache*). Estes servidores são chamados de *forwarders*.

Por exemplo, se sua empresa tem um servidor 200.20.57.1 e deseja fazer um *cache* dos servidores 200.20.57.12 e 200.20.57.13, então você poderia configurar as zonas de *forward* conforme a Figura 5-6.

Para configurar um servidor de nomes como *forwarder*, não é necessária qualquer configuração especial. Você só precisa configurar os outros servidores de nomes para encaminharem suas requisições para o *forwarder*. Desta forma, os servidores tentam resolver nomes através do *forwarder*, que, por sua vez, tem grandes possibilidades de já ter a resposta em seu *cache*, evitando, assim, que a requisição tenha de sair da rede local.

Repetidores

Figura 5-7. Configurando Repetidores

O seu servidor de nomes pode ter dificuldades para resolver nomes fora do domínio

por ele gerenciado. Isso pode acontecer se o DNS estiver atrás de um *firewall* e, portanto, não pode ver a Internet, ou se o DNS estiver ligado a uma conexão lenta.

Isto pode ser resolvido criando-se repetidores. Os *repetidores* são servidores de nomes que podem ser utilizados para resolver nomes externos em lugar do servidor primário.

Quando o servidor primário não consegue resolver um nome, ele delega a tarefa para o repetidor. Como o repetidor é muito mais usado, ele tem muito mais informações guardadas, tendo uma chance muito maior de conseguir resolver nomes.

Para configurar um servidor de nomes como repetidor não é necessária nenhuma configuração especial. A configuração é toda feita no servidor que utilizará o repetidor.

Para fazer com que este servidor utilize um ou mais repetidores, você deve informar os endereços IP dos mesmos na tela mostrada na Figura 5-7. Note que **a ordem é importante**, pois o servidor tentará sempre enviar as requisições para o primeiro, depois para o segundo e assim por diante. Assim, sempre coloque o melhor primeiro para obter uma performance desejável.

Funcionalidades

Na tela de funcionalidades do servidor (Figura 5-8), você pode fazer configurações diversas para alterar o funcionamento de seu servidor.

Alocação de Faixas de IP

Um servidor de nomes geralmente gerencia uma grande quantidade de máquinas associadas a endereços IP. Cada vez que uma nova máquina é adicionada ao domínio, um endereço IP tem de ser associado a ela e, por isso, o DNS tem de saber muito sobre a organização da rede para decidir qual endereço IP será associado à nova máquina.

Para simplificar este processo, o Linuxconf lhe dá a possibilidade de criar faixas de endereços IP que podem ser identificadas de maneira a organizar a rede.

Por exemplo, você pode criar uma faixa de endereços a serem utilizados em máquinas da matriz e faixas para máquinas das filiais:

10.0.1.1-27

: Matriz

10.0.2.1-15

: Filial 1

10.0.3.1-21

: Filial 2

Isto facilita e organiza o processo de decisão de qual IP será designado a qual máquina.

Para criar uma faixa de endereços IP, digite a faixa no campo Uma faixa de IP a descrição (nome) no campo Identificação/descrição e pressione Aceitar. Você pode criar múltiplas faixas através do botão Adicionar.

Inicializando o Serviço

Para inicializar o serviço de servidor de nomes em seu servidor, você deve abrir um terminal como superusuário e inicializar o **named**:

```
# cds


atd     gpm        keytable  lpd        nfs      sendmail  syslog
crond   halt       killall   mars-nwe   pcmcia   single    xfs
dhcpd   httpd      kudzu     named      network  portma    snmpd
ypbind  functions  inet      linuxconf  netfs    random    sshd



# ./named start Inicializando named: [ OK ]
```

Note que isso não fará com que o **named** seja reinicializado junto com o servidor. Para fazer isso, você deve utilizar o comando **ntsysv** e marcar o serviço **named** para ser inicializado sempre que o servidor for reiniciado conforme a Figura 5-10.

Figura 5-10. Configuração do named Através do ntsysv

Marcando o **named** para reinicializar junto com o servidor, sempre que o sistema operacional entrar em ação, o servidor de nomes será inicializado com ele.

Arquivos de Configuração do BIND

Como já foi mencionado anteriormente neste capítulo, a configuração do BIND pode ser feita sem o auxílio do Linuxconf através da edição de diversos arquivos de configuração.

Embora este capítulo tenha se dedicado a demonstrar a configuração do BIND através do Linuxconf, algumas notas devem ser feitas em relação aos arquivos de configuração por ele modificados. É importante conhecer estes arquivos até por uma questão de segurança. Perca ou danifique estes arquivos e você estará automaticamente dizendo adeus ao seu domínio.

Assim sendo, lembre-se de manter cópias de segurança destes arquivos!

O Arquivo `/etc/named.conf`

O `/etc/named.conf` é o primeiro arquivo que você deve conhecer. Ele é um ar-

quivo novo no BIND, pois até o BIND 4 a configuração era feita pelo arquivo `/etc/named.boot`, enquanto que o BIND 8 faz tudo no `/etc/named.conf`. O arquivo `/etc/named.conf` do domínio `minhaorganizacao.com.br` se parece com isso:

```
// Configuração para o domínio minhaorganizacao.com.br

options { directory "/var/named"; };

zone "." { type hint; file "root.hints"; };

zone "0.0.127.in-addr.arpa" { type master; file "zone/127.0.0"; };

zone "minhaorganizacao.com.br" { type master; file
        "zone/minhaorganizacao.com.br"; };

zone "177.6.206.in-addr.arpa" { type master; file "zone/206.6.177";
        };
```

Note as duas últimas seções deste arquivo. A primeira define o domínio mestre (este é um domínio primário). A segunda define o IP reverso, que será usado pelo servidor de nomes para fazer o caminho inverso, ou seja, a resolução de um nome a partir de um endereço IP.

O Arquivo `/var/named/nome-do-dominio`

Os domínios sobre os quais este servidor tem autoridade possuem um arquivo no diretório `/var/named` com o nome do próprio domínio. Em nosso exemplo, portanto, este arquivo chama-se `/var/named/minhaorganizacao`. Nele estão as informações do domínio que foram configuradas na tela mostrada na Figura 5-11.

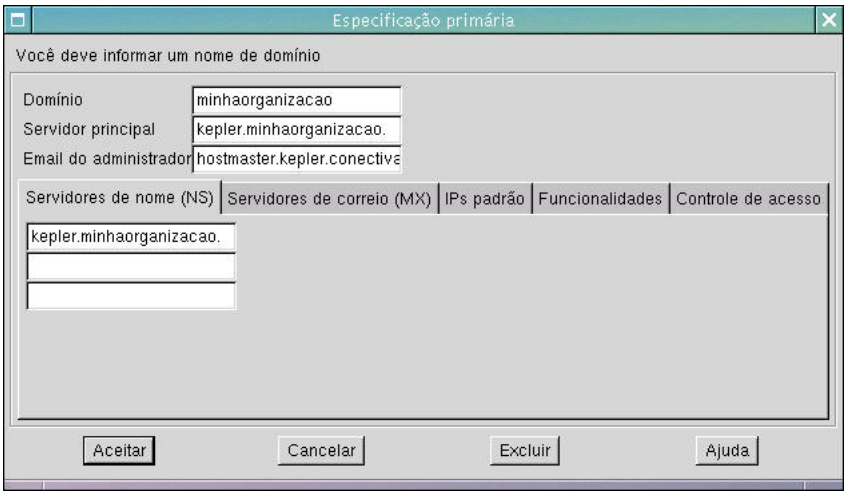


Figura 5-11. Adicionando um Domínio

O arquivo se parece com:

```
@ IN SOA
ns.minhaorganizacao.  hostmaster.ns.minhaorganizacao. (
2000051001 ; serial 3600 ; refresh 900 ; retry 1209600 ; expire
43200 ; default_ttl ) @ IN MX 5 mx.minhaorganizacao.  @ IN NS
ns.minhaorganizacao.  ns IN A 10.0.0.1
```

O Arquivo `/var/named/named.local`

O arquivo `/var/named/named.local` define o domínio local da máquina. Ele é um arquivo padronizado, não sendo necessária a sua configuração. Basicamente, ele é uma versão de `/var/named/nome-do-dominio` adaptado para o domínio e a máquina local (`localdomain` e `localhost`, respectivamente).

```
@ IN SOA localhost.
root.localhost. ( 1997022700 ; serial 28800 ; refresh 14400 ;
retry 3600000 ; expire 86400 ; default_ttl ) @ IN NS localhost.
1 IN PTR localhost.
```

O Arquivo `/var/named/named.ca`

O arquivo `/var/named/named.ca` é um arquivo fornecido pela InterNIC com informações necessárias para iniciar o *cache* do servidor de nomes. Este arquivo e deve ser atualizado periodicamente, o que pode ser feito através de FTP no servidor FTP ftp://ftp.rs.internic.net/ da InterNIC, no diretório `/domain`

```
; This file holds the information on root name servers
needed to ; initialize cache of Internet domain name servers ;
(e.g. reference this file in the "cache .  arquivo" ;
configuration file of BIND domain name servers).  ; ; This file
is made available by InterNIC registration services ; under
anonymous FTP as ; file /domain/named.root ; on server
FTP.RS.INTERNIC.NET ; -OR- under Gopher at RS.INTERNIC.NET ;
under menu InterNIC Registration Services (NSI) ; submenu
InterNIC Registration Archives ; file named.root ; ; last
update: Aug 22, 1997 ; related version of root zone: 1997082200
; ; ; formerly NS.INTERNIC.NET ; .  3600000 IN NS
A.ROOT-SERVERS.NET.  A.ROOT-SERVERS.NET.  3600000 A 198.41.0.4 ;
; formerly NS1.ISI.EDU ; .  3600000 NS B.ROOT-SERVERS.NET.
B.ROOT-SERVERS.NET.  3600000 A 128.9.0.107 ; ; formerly
C.PSI.NET ; .  3600000 NS C.ROOT-SERVERS.NET.
C.ROOT-SERVERS.NET.  3600000 A 192.33.4.12 ; ; formerly
TERP.UMD.EDU ; .  3600000 NS D.ROOT-SERVERS.NET.
```

```
D.ROOT-SERVERS.NET.  3600000 A 128.8.10.90 ; ; formerly
NS.NASA.GOV ; .  3600000 NS E.ROOT-SERVERS.NET.
E.ROOT-SERVERS.NET.  3600000 A 192.203.230.10 ; ; formerly
NS.ISC.ORG ; .  3600000 NS F.ROOT-SERVERS.NET.
F.ROOT-SERVERS.NET.  3600000 A 192.5.5.241 ; ; formerly
NS.NIC.DDN.MIL ; .  3600000 NS G.ROOT-SERVERS.NET.
G.ROOT-SERVERS.NET.  3600000 A 192.112.36.4 ; ; formerly
AOS.ARL.ARMY.MIL ; .  3600000 NS H.ROOT-SERVERS.NET.
H.ROOT-SERVERS.NET.  3600000 A 128.63.2.53 ; ; formerly
NIC.NORDU.NET ; .  3600000 NS I.ROOT-SERVERS.NET.
I.ROOT-SERVERS.NET.  3600000 A 192.36.148.17 ; ; temporarily
housed at NSI (InterNIC) ; .  3600000 NS J.ROOT-SERVERS.NET.
J.ROOT-SERVERS.NET.  3600000 A 198.41.0.10 ; ; housed in LINX,
operated by RIPE NCC ; .  3600000 NS K.ROOT-SERVERS.NET.
K.ROOT-SERVERS.NET.  3600000 A 193.0.14.129 ; ; temporarily
housed at ISI (IANA) ; .  3600000 NS L.ROOT-SERVERS.NET.
L.ROOT-SERVERS.NET.  3600000 A 198.32.64.12 ; ; housed in Japan,
operated by WIDE ; .  3600000 NS M.ROOT-SERVERS.NET.
M.ROOT-SERVERS.NET.  3600000 A 202.12.27.33 ; End of File
```

Configuração dos Clientes

Configuração Através do Linuxconf

A configuração de máquinas clientes de DNS é muito mais simples do que a configuração do servidor. Aquela configuração envolve basicamente a edição do arquivo `/etc/resolv.conf` ou pequenas configurações no Linuxconf.

Novamente, vamos nos concentrar na configuração via Linuxconf por ser ela muito mais robusta e menos propensa a erros.

Entre no Linuxconf e siga para Ambiente de Rede→Tarefas do Cliente→DNS para abrir a tela de especificação do servidor de nomes que pode ser vista na Figura 5-12.

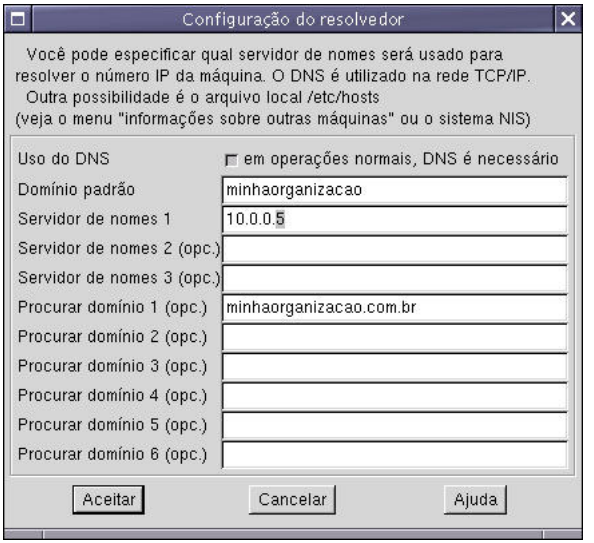


Figura 5-12. Especificação do Servidor de Nomes

Nesta tela você pode configurar as opções do servidor de nomes a ser utilizado pela estação. São elas:

Uso do DNS: esta opção serve apenas para indicar ao Linuxconf se o mesmo deve, ou não, preocupar-se com o DNS. Ela não altera o funcionamento da máquina.

Domínio Padrão: o domínio padrão é o domínio mais utilizado. Normalmente é o domínio de sua empresa. Quando você procura um nome sem domínio, o servidor de nomes procura pelo nome no domínio padrão.

Servidor de Nomes: aqui você pode definir até 3 endereços IPs de servidores de nomes. Lembre-se de que a ordem é importante, portanto coloque sempre o melhor servidor (o mais rápido) no topo.

Procurar domínio: você pode definir vários domínios nos quais um nome poderá ser encontrado. Quando um nome sem domínio não é encontrado no domínio padrão, o servidor de nomes começa a procurar nestes domínios. A ordem é importante, mas não da mesma forma como nos servidores de nomes. Aqui, você não precisa colocar os servidores mais rápidos antes, mas sim, os servidores mais utilizados.

O Arquivo `/etc/resolv.conf`

A configuração via Linuxconf é muito menos propensa a erros e muito mais intuitiva do que a edição do arquivo `resolv.conf`. Mesmo assim, este arquivo é extremamente simples, contendo apenas informações sobre o(s) servidor(es) a ser(em) utilizado(s).

Geralmente, este arquivo será bem pequeno e semelhante a este:

```
domain minhaorganizacao
search minhaorganizacao.com.br
nameserver 10.0.0.5
nameserver 10.0.0.7
```

O que este arquivo está nos dizendo é que esta estação está no domínio `minhaorganizacao`, está utilizando os servidores `10.0.0.5` e `10.0.0.7` para a resolução de nomes e que o servidor deve procurar por nomes no domínio `minhaorganizacao.com.br` se o mesmo não puder ser encontrado no domínio local.

Considerações Finais

Este capítulo deu uma pequena introdução do funcionamento, instalação e configuração do BIND para que você pudesse ter uma noção de um servidor de nomes. Foi-lhe demonstrado, também, como configurar suas estações para a utilização de servidores de nomes.

As configurações apresentadas neste capítulo são extremamente genéricas, sendo voltadas para a configuração de um servidor de nome simples.

Capítulo 6. Servidor Internet

Neste capítulo falaremos sobre os servidores Internet. Vamos mostrar a você como configurar um servidor de páginas da *web* e um servidor FTP. Além disso, você verá como montar um servidor *proxy*.

Falaremos primeiramente um pouco sobre os conceitos por trás da Internet. Você terá uma breve introdução aos protocolos utilizados na rede.

Servidor *Web*

Introdução e Conceitos

A *web* teve um crescimento muito grande desde o seu início, na década de 90. A *web* nada mais é do que uma forma de se visualizar documentos em hipertexto.

O Hipertexto

O termo *hipertexto* foi criado em 1965 para diferenciar um texto normal e linear de um texto não-linear. Um texto não-linear é um texto que contém referências

a informações extras. Por exemplo, um texto contendo a palavra *Linux* poderia conter uma referência a um artigo explicando o que é o Linux.

O exemplo mais conhecido de hipertexto atualmente é uma página da *web*. Você segue as referências entre as páginas sem seguir um roteiro linear.

O Protocolo HTTP

Para que você possa visualizar um documento de hipertexto na Internet, é necessário um protocolo para fazer a comunicação entre você e o servidor. Este protocolo é o HTTP[1]. Uma sessão HTTP geralmente envolve poucos passos. Por exemplo:

1. O cliente estabelece a conexão com o servidor (isso é feito através de outros protocolos de rede, geralmente TCP/IP) e solicita um documento:

   ```
   GET /index.html HTTP/1.0
   ```

   Neste exemplo, o cliente está solicitando o arquivo `/index.html` que é, normalmente, o arquivo padrão. Veremos mais sobre isso posteriormente. O importante agora é notar que estamos apenas enviando uma requisição ao servidor HTTP.

1. HyperText Transfer Protocol

2. Após a requisição, o servidor responde. Esta resposta é dividida em três partes:

   - Um código de retorno. A grande maioria das implementações do HTTP retornam este código seguido de uma mensagem (geralmente **OK** ou uma descrição do erro, se for o caso). Além disso, é retornado um texto identificando a versão do protocolo. Em nosso exemplo, esta linha é:

     ```
     HTTP/1.1 200 OK
     ```

     significando que o servidor está se comunicando através do **HTTP 1.1** e a operação (a requisição do arquivo) foi bem sucedida.

   - Um cabeçalho. Este cabeçalho contém diversas informações sobre o arquivo sendo enviado, como tamanho e informações sobre o próprio servidor:

     ```
     Date: Fri, 19 May 2000 20:53:51 GMT
     Server: Apache/1.3.12 (Unix)  (Conectiva/Linux) mod_ssl/2.6.0
     OpenSSL/0.9.4
     Last-Modified: Thu, 15 Apr 1999 16:38:13 GMT
     ETag: "177c3-508-371615f5"
     Accept-Ranges: bytes
     Content-Length: 1288
     Connection: close
     Content-Type: text/html; charset=iso-8859-1
     ```

     As informações acima demonstram que estamos conectados a uma máquina executando o Apache 1.3.12. Temos a data da última modificação do ar-

quivo, seu tamanho e seu tipo. Estas informações podem ser utilizadas pelo programa cliente para decidir o que fazer com determinado arquivo.

- O arquivo propriamente dito. Após o cabeçalho, uma linha em branco é enviada pelo servidor, indicando que, a partir daquele ponto, tudo o que for mandado pelo mesmo será parte do arquivo requisitado. Um programa cliente pode controlar o progresso da transmissão monitorando quanto já foi transmitido e comparando esta informação com o tamanho informado no cabeçalho.

O Apache

O Apache é o servidor web mais popular do mundo. Uma pesquisa recente demonstrou que o Apache é mais utilizado do que todos os outros servidores disponíveis juntos.

A popularização da *web* nos últimos anos tem obrigado as empresas a disponibilizarem conteúdo na mesma. Para isso, a utilização do Apache é imperativa para qualquer empresa que deseja manter uma presença na rede.

Além de permitir que você disponibilize conteúdo na Internet, o Apache lhe permite a publicação de informações em sua Intranet, tornando-o realmente um produto indispensável.

Instalando o Apache

1. Acesse o CD da distribuição do Conectiva Linux:

```
# cd /mnt/cdrom/conectiva/RPMS
```

2. Instale o pacote do Apache:

```
# rpm -ivh apache-*
apache       ########################################
apache-devel ########################################
apache-doc   ########################################
```

Configurando o Apache

O Apache que acompanha a distribuição do Conectiva Linux já vem configurado com as opções mais utilizadas, de forma que você só precisa iniciar o servidor para que seu Conectiva Linux seja um servidor *web*. Quando você inicializa o servidor *web*, você pode acessar sua máquina via HTTP e visualizar a página

padrão como mostrada na Figura 6-1:

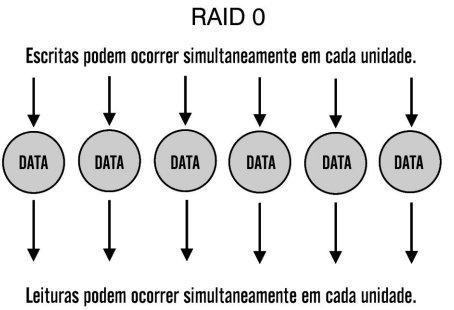


Figura 6-1. Página Inicial doApache Conectiva Linux Vista no Netscape®

Para inicializar o servidor Apache, abra um terminal e digite:

```
# cds
atalk   functions  keytable         lpd       network
atd     gpm        killall          mars-nwe  nfs
autofs  halt       kudzu            mysql     nfslock
crond   httpd      ldap             named     pcmcia
dhcpd   inet       linuxconf-setup  netfs     portmap
# ./httpd start
Iniciando httpd:                              [  OK  ]
#
```

A configuração do Apache depende muito do perfil de servidor *web* desejado. Nesta seção você verá como configurar o Apache da maneira mais simples possível. Depois, você saberá um pouco sobre os módulos mais populares do Apache e como instalá-los e configurá-los.

Para configurar o Apache, você deve acessar o Linuxconf e entrar em Ambiente de rede→Tarefas de servidor→Apache - servidor www. Você verá o menu inicial da configuração do Apache como mostrada na Figura 6-2.

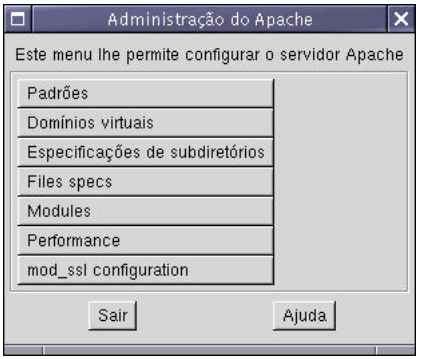


Figura 6-2. Tela Incial de Configuração do Apache

Clique em Padrões para alterar as opções básicas de seu servidor WWW.

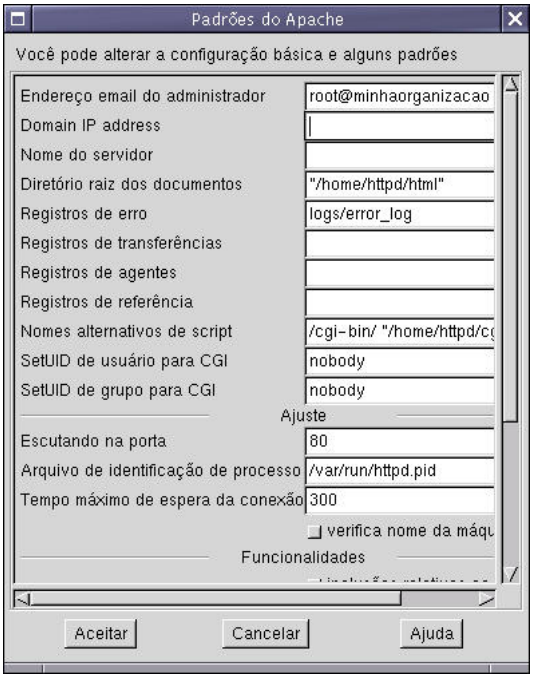


Figura 6-3. Configurações Básicas do Apache

Há um grande número de opções a serem configuradas nesta tela, mas nos ateremos às mais comuns:

- **Endereço de email do administrador:** aqui você poderá informar o endereço de correio eletrônico do administrador do *site*.

- **Domain IP address:** neste campo você poderá informar um endereço IP padrão para o domínio. Este endereço IP é, geralmente, o endereço IP do servidor www, e será utilizado quando alguém tentar acessar a página através do nome do domínio ao invés do nome da máquina. Por exemplo, imagine que o servidor Apache está sendo executado na máquina `kepler.minhaorganizacao`, que tem o endereço IP 10.0.0.1. Se você informar o mesmo endereço IP da máquina `kepler` (10.0.0.1) como **Domain IP address**, quando alguém tentar acessar o endereço `minhaorganizacao` (o domínio), ele irá, na verdade, acessar `kepler.minhaorganizacao` (a máquina que realmente possui o endereço de IP especificado).

- **Nome do servidor:** você poderá informar o nome da máquina onde o Apache está sendo executado. Em condições normais, este campo não é necessário, já que o Apache é capaz de descobrir o nome através do **DNS** ou do próprio arquivo `hosts`.

- **Diretório raiz dos documentos:** você poderá informar aqui o diretório onde estarão os arquivos do seu *site*. O diretório padrão é o `/home/httpd/html`.

- **Diretório alternativo de scripts:** você poderá informar vários *apelidos* para os diretórios de CGI. Isso quer dizer que você vai definir um diretório virtual e associá-lo a um diretório real. Por exemplo, você pode definir que quando uma página fizer um referência ao diretório virtual `/cgi-bin`, ele estará, na realidade, acessando os arquivos do diretório `/home/httpd/cgi-bin`.

Uma das características mais utilizadas no Apache é a sua capacidade de lidar com *máquinas virtuais*[2]. Uma máquina virtual é, na verdade, um pequeno truque

2. No Apache, este conceito é chamado de *VirtualHost*

envolvendo o Apache e o serviço de nomes do servidor (DNS ou o arquivo `hosts`). Basicamente, uma máquina virtual é um apelido para a máquina real. Este apelido deve ter um IP próprio. Com isso, pode-se fazer com que apenas um servidor Apache sirva diversos *sites* separadamente.

Em nosso exemplo, assumimos que nossa máquina chama-se `kepler`. Agora vamos supor que queiramos disponibilizar informações de suporte técnico através de outro nome de máquina, por exemplo `suporte.minhaorganizacao`. O conteúdo deste outro *site* deverá estar localizado na mesma máquina `kepler`.

Primeiramente, você deve estabelecer um apelido de IP para a máquina `kepler`. Para fazer isso, você deve pressionar o botão Apelidos de IP para máquinas virtuais no menu Ambiente de Rede do Linuxconf. A Figura 6-4 mostra a tela de configurações dos apelidos de IP. Note que você deve escolher a *interface* de rede a ser utilizada. Esta deve ser a *interface* utilizada para acessar a máquina.

Figura 6-4. Apelidos de IP

Basta informar o novo endereço de IP para a máquina. No exemplo da Figura 6-4, definimos que a máquina `kepler` (o nosso servidor) responderá ao endereço IP 10.0.1.1 além do seu endereço de IP *real*.

Note, porém que, antes de continuarmos, você deve configurar o seu serviço de nomes para que este associe o nome `suporte` a este endereço IP. Não faz parte do escopo deste capítulo o processo de atualização do DNS, verifique a documentação disponível sobre servidores de nomes para aprender como fazer esta configuração.

Agora você pode voltar à tela de configuração do Apache no Linuxconf e pressionar Máquinas Virtuais seguido de Adicionar. Na tela da Figura 6-5, você poderá definir as opções de sua máquina virtual.

Figura 6-5. Máquina Virtual do Apache

Note que as opções disponíveis são semelhantes às utilizadas na configuração dos padrões do Apache. Mas vamos ver o significado dos valores definidos em nosso exemplo:

- **Nome da máquina virtual:** aqui definimos que nossa máquina virtual se chamará `suporte`. Novamente, lembre-se de que o seu DNS deve estar configurado para reconhecer este nome e mapeá-lo para o apelido de IP que escolhemos.

- **Endereço email do administrador:** aqui apenas definimos que o endereço de correio

eletrônico do administrador é `root@minhaorganizacao`.

- **Domain IP address:** especificamos o endereço do nosso domínio. Este endereço será utilizado quando for feita uma tentativa de acesso à máquina através do nome do domínio sem o nome da máquina.

- **Nome do servidor:** este é o nome da máquina servidor.

- **Diretório raíz dos documentos:** este é o diretório onde nós iremos colocar os arquivos da máquina `suporte`. Assim, todas as páginas e figuras do suporte técnico estarão no diretório `/home/httpd/suporte/html`.

- **Registros de erro:** quando algum erro ocorrer durante uma tentativa de acesso às páginas de `suporte`, o Apache salvará informações sobre o mesmo neste arquivo.

- **Registros de transferência:** este arquivo contém um registro dos acessos à máquina virtual `suporte`. Estas informações podem ser utilizadas para a obtenção de informações de segurança.

- **Nomes alternativos de *script*:** aqui você pode definir diretórios dos *scripts* CGI a serem utilizados pela máquina `suporte`. Note que é possível utilizar o mesmo diretório para todas as máquinas, sejam elas virtuais ou reais.

Servidor FTP

Nesta seção trataremos do servidor FTP. No Conectiva Linux o WU-FTPD é quem realiza os serviços de FTP. Assim, esta seção irá ser voltada ao WU-FTPD.

O WU-FTPD

FTP é um acrônimo para *File Transfer Protocol* ou *Protocolo de Transferência de Arquivos*. O protocolo FTP permite a transferências de arquivos binários e arquivos texto com alta eficiência através de uma rede.

Instalação e Configuração

1. Para instalar o WU_FTPD, acesse o diretório de pacotes do CD da distribuição de seu Conectiva Linux:

```
# cd /mnt/cdrom/conectiva/RPMS
```

2. Instale o pacote do WU_FTP:

```
# rpm -ivh wu-ftpd-*
wu-ftpd ####################################
```

3. Certifique-se que a linha abaixo esteja presente no arquivo `/etc/inetd.conf` e que ela não esteja comentada:

```
ftp stream tcp nowait root /usr/sbin/tcpd in.ftpd -l -a
```

4. Se você houver feito alterações ao arquivo `/etc/inetd.conf`, você deve reiniciar o **inetd**:

```
# cds
atd       gpm    keytable         lpd       nfs     sendmail syslog
crond     halt   killall          mars-nwe  pcmcia  single   xfs
dhcpd     httpd  kudzu            netfs     portmap snmpd    ypbind
functions inet   linuxconf-setup  network   random  sshd
```

```
# ./inet stop
Interrompendo os serviços INET:                          [  OK  ]
# ./inet start
Iniciando os serviços INET:                              [  OK  ]
```

Com o servidor FTP devidamente instalado, você pode acessar o Linuxconf para iniciar o processo de configuração.

No Linuxconf, vá para Ambiente de Rede → Tarefas de Servidor → Wu-ftp - servidor de ftp para abrir a tela inicial de configuração do servidor FTP. Esta tela é mostrada na Figura 6-6.

Clique em Configuração básica→ Diversos para abrir a tela mostrada na Figura 6-7.

Figura 6-7. Configurações Básicas do Servidor FTP

Estas são as opções mais básicas do servidor FTP. Com elas, você poderá definir o comportamento geral de seu servidor.

- **Email do administrador:** endereço de correio eletrônico do administrador do sistema.
- **Grupo de convidados:** aqui você pode informar o grupo do Linux ao qual o usuário **anonymous** pertencerá. Você terá mais informações sobre acesso anônimo ao servidor na seção *Acessos Anônimos*. Se este campo não for preenchido, o grupo **nobody** será utilizado.
- **Arquivo de *banner*:** o conteúdo do arquivo de *banner* será mostrado aos usuários no momento em que os mesmos acessarem com sucesso o seu servidor.
- **Mensagem de encerramento:** se o arquivo informado existir, sempre que um usuário tentar acessar o servidor, seu conteúdo será mostrado e o servidor irá fechar a conexão. O arquivo é bastante útil sempre que você quiser interromper o serviço de FTP temporariamente.

- **Permitir acesso anônimo:** aqui você pode permitir ou proibir os acessos anônimos. Mais sobre o assunto na seção *Acessos Anônimos*.

Agora pressione Controle nesta mesma tela para acessar as opções de controle de acesso do servidor FTP. A tela é mostrada na Figura 6-8.

Figura 6-8. Configurações de Controle de Acessos

Existem, na realidade, três telas de configuração de controle de acesso:

- **Usuários reais:** controle de acesso dos usuários reais do seu sistema. Esses são os usuários que têm contas em sua rede.

- **Usuários convidados:** controle de acesso a usuários convidados.

- **Anônimos:** controle de acesso de usuários que se conectam anonimamente.

As três telas são absolutamente idênticas umas às outras. As opções disponíveis são:

- **pode requisitar arquivos comprimidos:** define se o usuário pode requisitar que seus arquivos sejam compactados. O WU-FTPD permite a compactação de arquivos durante

a transmissão.

- **pode requisitar arquivos tar:** especifica se o usuário tem permissão de solicitar o arquivamento de arquivos transmitidos com o tar.
- **pode usar chmod para arquivos:**especifica se o usuário pode modificar as permissões de arquivos localizados no servidor FTP.
- **pode excluir arquivos:** define se o usuário tem permissão de apagar arquivos localizados no servidor FTP.
- **pode atualizar arquivos:** define se o usuário pode sobrescrever arquivos no servidor.
- **pode renomear arquivos:** especifica se o usuário pode modificar o nome dos arquivos localizados no servidor.
- **registrar transferências recebidas:** especifica se o servidor deve manter um registro de arquivos recebidos.
- **registrar transferências expedidas:** especifica se o servidor deve manter um registro de arquivos enviados.

Acessos Anônimos

Pode ser permitido ao usuário acessar seu servidor de maneira anônima. Isso é

muito útil no caso de você desejar disponibilizar arquivos a pessoas de fora de sua organização. Como essas pessoas não possuem contas de usuário em seu sistema, a única forma de acessar seus arquivos é através do acesso anônimo.

Para permitir o acesso anônimo ao seu servidor:

1. Acesse o diretório de pacotes do CD do Conectiva Linux:

```
# cd /mnt/cdrom/conectiva/RPMS
```

2. Instale o pacote de acesso anônimo:

```
# rpm -ivh anonftp-*
anonftp  ##############################################
```

A partir desse momento, para acessar o servidor FTP anonimamente, o usuário deverá fornecer o nome de usuário **anonymous** e seu endereço de correio eletrônico como senha.

```
$ ftp localhost
Conectado na máquina localhost.
220 einstein.minhaorganizacao FTP server
(Version wu-2.6.0(1) Fri May 12 11:05:03 BRST 2000) ready.
```

```
Usuário (localhost:albert): anonymous
331 Guest login ok, send your complete e-mail address as password.
Senha:
230 Guest login ok, access restrictions apply.
O tipo do sistema remoto é UNIX.
Usando modo binary para transmitir/receber arquivos.
ftp>
```

Note que no exemplo acima, a senha não é mostrada, mas o usuário teve de digitar seu endereço de e-mail para poder ter acesso ao servidor. O usuário **anonymous** não precisa (nem deve) ser cadastrado em seu Conectiva Linux, já que ele é um usuário especial para o servidor FTP. Quando é feita uma tentativa de acesso com o usuário **anonymous**, o servidor automaticamente trata o acesso como anônimo, aceitando o endereço de correio eletrônico como senha.

Permitindo Envio de Arquivos

Normalmente, você não precisará (e provavelmente nem desejará) que os usuários possam gravar arquivos em seu servidor FTP. Porém, em alguns casos, pode haver interesse em disponibilizar-se uma área para que os usuários possam guardar arquivos.

Tornou-se um costume fazer com que os usuários tenham um local específico nos

servidores de FTP para gravarem arquivos. Esse local é o diretório `/incoming`.

> Permitir que usuários gravem em seu servidor FTP é um grande risco e, por isso, deve-se pensar muito bem antes de fazê-lo.
>
> Um dos maiores problemas com isso é que você não tem um grande controle sobre aquilo que é gravado em seu servidor. Você não pode facilmente impedir que usuários guardem material ilegal em seu servidor.
>
> Recomendamos, portanto, que você não permita o acesso de escrita em seu servidor. Caso você não tenha escolha, você deve ter alguém responsável por monitorar os arquivos guardados em seu servidor para evitar arquivos que possam trazer problemas no futuro.

Para criar o `/incoming`:

1. Acesse o diretório raiz do FTP:

```
# cd /home/ftp
```

2. Crie o diretório `incoming`

```
# mkdir incoming
```

3. Agora você deve fazer com que o diretório criado seja de propriedade de um usuário e grupo diferente de **root** e de **ftp**. Você pode criar um usuário e grupo específicos para isto se desejar, mas utilizaremos **nobody.nobody** em nosso exemplo.

```
# chown nobody incoming
# chgrp nobody incoming
# chmod 3773 incoming
```

4. Agora você deve editar o arquivo `/etc/ftpaccess` para permitir a escrita ao diretório `/incoming`. Note que, se você houver criado um usuário e grupo para ser dono do diretório, você deverá informar isso na linha abaixo no lugar de **nobody**.

```
upload /home/ftp /incoming yes nobody nobody 0400 dirs
```

   O formato desta linha é:

```
upload HOME DIR GRAVA USUARIO GRUPO PERMS DIRS
```

   Onde:

   - **HOME:** diretório *home* do usuário. Em nosso exemplo, informamos `/home/ftp`. Isso quer dizer que esta linha se aplica a qualquer usuário cujo diretório *home* seja `/home/ftp`.

- **DIR:** diretório ao qual se refere a linha. Esse diretório é relativo à raiz do diretório do FTP. Em nosso exemplo, informamos que esta linha se aplica ao diretório `/incoming`.

- **GRAVA:** aqui você informa se é ou não é permitida a gravação no diretório ao qual a linha se refere. Os valores permitidos são **YES** ou **NO**. Em nosso exemplo, estamos permitindo a escrita.

- **USUARIO:** é o nome do usuário a quem todos os arquivos gravados no diretório pertencerão. Em nosso exemplo esse usuário é **nobody**.

- **GRUPO:** é o grupo a quem todos os arquivos gravados no diretório pertencerão. Em nosso exemplo esse grupo é **nobody**.

- **PERMS:** após gravados, os arquivos terão as permissões trocadas para estas. Em nosso exemplo definimos que os arquivos gravados neste diretório passariam a ter permissão 0400, ou seja, apenas para leitura do dono (no caso, o usuário **nobody.nobody**). Recomendamos estas permissões, já que elas não permitem que usuários utilizem o seu servidor para troca de arquivos ilegais. Isso assegura que alguém terá de verificar o arquivo e trocar suas permissões antes que alguém possa acessá-lo via FTP.

- **DIRS:** especifica se o usuário anônimo pode criar diretórios dentro do diretório `/incoming`. Em nosso exemplo o usuário pode criar. Os valores possíveis são **dirs** e **nodirs**.

Arquivos de Mensagens e *Banners*

Se você já acessou algum servidor FTP, então já deve ter notado que é comum aparecer mensagens informativas quando se conecta ou quando se muda de diretório. Estas mensagens são muito úteis para informar o usuário das possibilidades e regras a serem seguidas no servidor.

Arquivo de *Banner*

Quando você configura o WU-FTPD no Linuxconf, há uma opção chamada Arquivo de banner.

Você pode informar um arquivo cujo conteúdo será mostrado ao usuário antes da conexão em si. Ele é útil para uma breve mensagem de boas-vindas ao servidor. Pode-se fazer uma breve explicação sobre o servidor e os direitos de acesso ao mesmo.

> Lembre-se que o arquivo de *banner* é apresentado ao usuário antes do *login*. Assim, evite dar muita informação sobre o servidor através deste arquivo.

O Arquivo `.message`

Um dos arquivos mais comuns e mais úteis em um servidor FTP é o arquivo `.message`. Quando o servidor encontra este arquivo em um diretório, ele mostra seu conteúdo para o usuário antes de mostrar o conteúdo do diretório em si.

Você pode utilizar este arquivo para dar breves explicações sobre os propósitos dos diretórios sendo acessados. Além disso, você poderia ajudar o usuário a encontrar o que ele está procurando.

Por exemplo, digamos que um usuário queira acessar o seu servidor para encontrar uma atualização para um programa. O usuário, porém, não tem muita experiência com servidores FTP e não sabe ao certo como encontrar aquilo de que ele precisa. Assim, você poderia criar arquivos `.message` para guiar o usuário.

Quando o usuário acessa o diretório `/pub` do servidor FTP, por exemplo, você poderia explicar-lhe o que está disponível ali. Um exemplo de como a mensagem é mostrada para o usuário está na Figura 6-9.

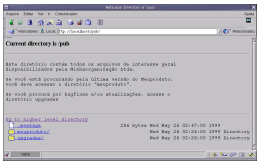


Figura 6-9. Diretório com `.message` Visto no Netscape

Servidor *Proxy*

Nesta seção iremos tratar da implementação de um servidor *proxy* em um Conectiva Linux.

O *software* servidor *proxy* que acompanha o Conectiva Linux é o Squid, e é nele que esta documentação se centralizará.

Caching

Quando você acessa uma página da *web* ou um arquivo de FTP, uma requisição parte de sua máquina até o servidor; só então os dados são transmitidos para a sua máquina. Como muitas vezes a distância entre o servidor e a sua máquina é muito grande e a qualidade das linhas de transmissão muito irregulares, este processo acaba por tornar-se bastante lento.

Além disso, a maioria dos dados requisitados é estática; eles não mudam com o tempo. Os logotipos que as empresas colocam em suas páginas, por exemplo, não tendem a mudar. Entretanto, eles são, muitas vezes, bastante grandes. Isso é um enorme desperdício de recursos da rede, além de tempo.

Uma solução encontrada foi o chamado *caching*. Sempre que é feita uma requisição de algum objeto da Internet, o servidor *proxy* consulta o *cache* para verificar se este objeto já não foi requisitado previamente. Se ele foi, então o servidor *proxy* pode responder à requisição utilizando sua própria cópia local do objeto. Isso acelera significativamente as operações na Internet, já que grande parte dos objetos acaba trafegando apenas localmente.

O servidor *proxy* verifica se a sua cópia é atualizada com o objeto original. Caso não for, o *proxy* atualiza sua cópia. Naturalmente, um servidor de *cache* não poderia guardar todos os objetos acessados para sempre, pois isso iria rapidamente saturá-lo. A solução é simples: o servidor mantém apenas os arquivos utilizados a menos tempo. Isso garante, de uma forma indireta, que os objetos mais freqüentemente utilizados sempre estejam no *cache*.

O Squid

O Squid é o servidor *proxy* do Conectiva Linux. Ele oferece alta performance de *cache* para servidores *web*.

O Squid oferece grandes vantagens em comparação com outros servidores *proxy*:

- ele realiza, além do *cache* de objetos como arquivos de FTP e páginas da *web*, um *cache* de procuras de DNS. Isso quer dizer que ele guarda informações sobre o mapeamento entre endereços IP e nomes de máquinas da Internet. Isso acelera a procura de máquinas;

- ele mantém os objetos mais utilizados na memória RAM (cujo uso pode ser limitado pela configuração);

- ele suporta SSL (acesso a páginas criptografadas) para segurança em transações;

- pode ser organizado em hierarquias de servidores de *cache* para uma melhora signi-

ficativa de performance;

- responde às requisições em um único processo de acesso a disco.

Todo o servidor *proxy* Squid consiste de um programa principal (**Squid**) e de seu próprio programa de resolução de nomes (**dnsserver**). Quando o Squid é inicializado, ele cria o processo do dnsserver, diminuindo o tempo de espera pela resposta do DNS.

Instalação e Configuração

Para instalar o Squid:

1. Acesse o diretório de pacotes do CD do Conectiva Linux:

```
# cd /mnt/cdrom/conectiva/RPMS
```

2. Instale o pacote do Squid:

```
rpm -ivh squid-*
```

```
squid  ################################################
```

3. Inicialize o programa:

```
# cds
atd        gpm       killall          named    pcmcia      single
autofs     halt      kudzu            netfs    portmap     smb
crond      httpd     linuxconf-setup  network  postgresql  snmpd
dhcpd      inet      lpd              nfs      random      squid
functions  keytable  mars-nwe         nfslock  sendmail    sshd
[root@gnu init.d]# ./squid start
creating directories at /var/spool/squid, wait...          [  OK  ]
Iniciando squid                                            [  OK  ]
```

Para realizar configurações no Squid é necessário editar o seu arquivo de configuração que está localizado em `/etc/squid/squid.conf`.

Memória para *Cache*

O Squid armazena os objetos mais utilizados na memória RAM. Isso faz com que a performance seja muito melhor do que se os objetos fossem armazenados em disco.

A quantidade de memória a ser utilizada para *cache* do Squid pode (e deve) ser limitada, de forma a não interferir com outros processos no sistemas. O padrão é 8MB.

> Note que este limite de memória refere-se à memória usada para *cache*, e não a memória total utilizada pelo Squid. Na realidade, a memória utilizada pelo Squid deverá ficar em torno de três vezes este valor.

Para especificar a quantidade de memória máxima a ser utilizada para *cache*, você deve utilizar o parâmetro `cache_mem` no arquivo `/etc/squid/squid.conf`:

```
cache_mem MEM
```

Onde **MEM** é a quantidade de memória máxima a ser utilizada para *cache*.

Exemplo:

```
cache_mem 32 MB
```

Este exemplo especifica que o Squid deverá limitar a 32MB a quantidade de memória utilizada para *cache*.

Arquivos de *Cache*

Os objetos guardados pelo Squid são guardados em arquivos no disco rígido. Você pode especificar algumas opções para definir como o Squid trabalhará com arquivos.

```
cache_dir TIPO NOMEDIR MB N1 N2
```

Onde:

- **TIPO:** você deve especificar o tipo do sistema de armazenamento que o Squid deverá utilizar. Normalmente, você deve utilizar **ufs**. Você pode tentar utilizar **asyncufs** para obter melhor performance. Se, por acaso, o **asyncufs** não funcionar corretamente em seu sistema, volte a usar o **ufs**.

- **NOMEDIR:** especifique o diretório onde os arquivos serão gravados. Note que este diretório não será criado automaticamente pelo Squid.

- **MB:** você pode modificar o espaço máximo a ser utilizado para *cache* neste diretório. O valor padrão é 100 MB.

- **N1:** você pode especificar o número máximo de diretório de primeiro nível que serão criados dentro do diretório de *cache*. O padrão é 16.

- **N2:** número máximo de diretórios de segundo nível que serão criados dentro de cada diretório de primeiro nível. O valor padrão é 256.

Exemplo:

```
cache_dir ufs /var/spool/squid 100 16 256
```

Este exemplo define que o diretório de *cache* será o `/var/spool/squid`, que ele poderá ter até 100MB, 16 diretórios de primeiro nível e 256 diretórios de segundo nível dentro de cada diretório de primeiro nível.

Controle de Acesso

Por razões de segurança, a configuração padrão do Squid do Conectiva Linux é bastante conservadora; ela nega acesso a qualquer máquina.

Você deve alterar este comportamento para poder utilizar o Squid. Deve, portanto, estabelecer regras de acesso ao servidor *proxy*. As regras têm o formato:

```
http_access PERM QUEM
```

Onde:

- **PERM:** indica se a linha é uma permissão ou uma proibição de acesso. Os valores permitidos são: **allow**, para permitir e **deny**, para negar acesso.
- **QUEM:** a quem se refere esta permissão. Pode ser uma máquina ou um domínio ou uma classe. Pode-se ainda usar **ALL** para indicar que a permissão definida na linha se

refere a todas as máquinas.

Exemplo:

```
http_access allow all
```

Este exemplo permite que todas as máquinas da rede possam utilizar este servidor *proxy*.

Note que, como mencionado anteriormente, o Squid é pré-configurado para não permitir acesso de nenhum usuário ou máquina. Assim, você deve procurar a linha do arquivo `/etc/squid/squid.conf` parecida com:

```
http_acces DENY all
```

E removê-la ou editá-la no arquivo.

Capítulo 7. Correio Eletrônico

Introdução

Correio eletrônico[1] sempre foi uma das aplicações chaves na Internet. É considerado garantido por quem usa Internet e utilizado para trafegar informação crucial de maneira rápida, eficiente e segura, aliado, por exemplo, a algum mecanismo de encriptação e/ou autenticação, como o gnupg http://www.gnupg.org. Este capítulo explica em mais detalhes como ocorrem trocas de mensagens eletrônicas, quais os protocolos e ferramentas utilizados e como configurá-los para as tarefas mais usuais.

1. electronic mail ou e-mail

A Teoria

Como Funciona a Troca de Mensagens Eletrônicas

Para melhor compreensão dos conceitos abordados mais adiante, é útil ter uma idéia global do que ocorre durante a transferência de uma mensagem eletrônica entre dois pontos (na prática, duas máquinas, ou ainda dois usuários). Digamos que João, que possui o usuário `joao`, queira mandar uma mensagem para seu irmão Francisco (`francisco`). Não importa se João e Francisco estão se comunicando em uma intranet (rede interna) ou pela Internet, o processo é análogo. Vamos assumir ainda que a máquina de João se chame `capivara` e o servidor de e-mails de Francisco, `saci`. João compõe a mensagem em seu cliente de e-mail, chamado de *Agente de Mensagens do Usuário*[2] preferido, ou simplesmente digita algo como

```
$ echo "Almoço na casa da mãe." | \ >
                mail -s 'Francisco!' francisco@saci
```

A mensagem é entregue ao *MTA*[3] da máquina `capivara`. O MTA é o responsável

2. MUA ou Mail User Agent

3. Mail Transport Agent.

pela entrega de mensagens na caixa postal correta, se está na máquina de destino, ou pelo encaminhamento delas à sua máquina de destino, se está na máquina de origem. Assim, o MTA da máquina `capivara` determina que tem de entregar a mensagem ao usuário, na máquina `saci`. Ele se conecta à porta 25 (normalmente) usando o protocolo SMTP (Simple Mail Transfer Protocol) que entrega a mensagem. O MTA da máquina `saci`, responsável pelo SMTP, recebe a mensagem e a deixa na caixa postal de Francisco (por exemplo, `/var/spool/mail/francisco`). Se Francisco estiver verificando os e-mails em casa, pode usar o protocolo POP (Post Office Protocol) ou IMAP (Internet Message Access Protocol) para receber a mensagem. Se tudo correr bem, Francisco recebe a mensagem poucos segundos após João tê-la enviado e pode tomar as providências necessárias para se proteger.

Os Protocolos Envolvidos na Troca de Mensagens

SMTP

SMTP é o protocolo responsável pelo envio de mensagens da máquina de origem (no exemplo acima, `capivara`) até a máquina de destino (`saci`). Os MTAs das duas máquinas e de alguma outra que possa estar no meio do caminho realizado pela mensagem (se Francisco tiver um redirecionamento de e-mail, por exemplo, haverá mais máquinas envolvidas) são responsáveis pelo tráfego da mensagem

até a caixa postal de Francisco em `saci`. O Sendmail, por exemplo, é um MTA e será explicado em detalhe mais adiante.

Uma vez estabelecida a conexão, o MTA normalmente exibe uma mensagem de apresentação, basicamente dizendo que é ele o responsável pelo SMTP naquela máquina. O MUA (ou o administrador de sistemas que fez telnet para a porta 25 de sua máquina a fim de testar o que está lendo) deve então começar a comunicação enviando o comando HELO:

```
HELO capivara
```

O MTA normalmente responde com uma mensagem simpática como “Muito prazer em conhecê-lo”. Em seguida, o MUA diz quem é o remetente da mensagem a ser transmitida:

```
MAIL FROM: joao@capivara
```

Se tudo correr bem, o MTA aceita o remetente (“250 joao@capivara... Sender ok”). Em seguida, informa-se o destinatário:

```
RCPT TO: francisco@saci
```

Novamente, o servidor deve confirmar que aceitou enviar mensagem para o endereço especificado (“250 francisco@saci... Recipient ok”). A mensagem pode ser recusada, por exemplo, por alguma proteção contra SPAM. Mas, se tudo correr bem, só resta a mensagem em si:

```
DATA
```

A partir daí, o que for digitado será colocado na mensagem, até que se digite uma linha contendo somente um ponto (“.”). Note que é nesse ponto que se definem os cabeçalhos. Assim, a mensagem do exemplo poderia ser escrita como:

```
DATA
354 Enter mail, end with a "." on a line by itself
To: Francisco Pirana <francisco@saci>
From: João Pirana <joao@capivara>
Subject: Francisco!


            Almoço na casa da mãe.

                Abraços do seu irmão,

                     João
```

O servidor imprime na tela uma linha informando que a mensagem foi aceita e colocada na fila de processamento. Para se enviar a mensagem para mais de um endereço, execute o comando **RCPT TO:** para cada destinatário. Quem aparece no campo From:, quem aparece no campo Cc: e quem não aparece (ou seja, que está no campo Bcc: da mensagem) é definido também dentro do comando **DATA**. Supondo que as linhas **RCPT TO:** relevantes já tenham sido definidas:

```
MAIL FROM: joao@capivara
250 joao@capivara... Sender ok
RCPT TO: francisco@saci
250 francisco@saci... Recipient ok
RCPT TO: bruce@woolamalahoo.au
250 bruce@woolamalahoo.au... Recipient ok
RCPT TO: snorman@hedgehog.com
250 snorman@hedgehog.com... Recipient ok
DATA
354 Enter mail, end with a "." on a line by itself
To: Francisco Pirana <francisco@saci>
From: João Pirana <joao@capivara>
Cc: Departamento de Filosofia <bruce@woolamalahoo.au>
Subject: Francisco!
...
```

É sempre bom lembrar que o que separa o cabeçalho do corpo da mensagem é uma linha em branco. Portanto, não deixe linhas em branco entre linhas do cabeçalho.

Para finalizar a sessão, utiliza-se o comando **QUIT**.

Usando o SMTP, portanto, a mensagem é transportada até a máquina de destino. Se Francisco está lendo seus e-mails diretamente no servidor, não há outros proto-

colos envolvidos. Se, porém, ele tem de baixar as mensagens para outra máquina, é necessário outro protocolo para a recuperação das mensagens.

POP

O protocolo POP, inversamente ao SMTP, é utilizado quando se deseja buscar uma mensagem que está no servidor. O leitor atento deve ter notado que não há autenticação no protocolo SMTP. Em princípio, qualquer um pode mandar mensagens para qualquer um. Com recebimento de mensagens, obviamente, é diferente. O usuário, ao se conectar com o servidor POP (usualmente na porta 110) envia os comandos **USER** e **PASS** para assegurar que ele tem direito de ler as mensagens naquele servidor:

```
USER francisco
+OK User name accepted, password please
PASS notlob
+OK Mailbox open, 5 messages
```

Se o servidor confirmar a autenticação, as mensagens na caixa postal podem ser listadas. Note que a senha é passada em texto puro e é visível (ao contrário, por exemplo, do que acontece no processo de login em uma máquina Linux). Portanto, se resolver fazer um teste, certifique-se de que não há ninguém em volta, ou sua senha pode ser comprometida. Além disso, há sempre a possibilidade de

que alguém tenha colocado um *sniffer*[4]. Dependendo da importância das informações que estão sendo transmitidas e recebidas e de quão paranóico se deseja ser, é aconselhável transmitir as mensagens usando criptografia ou mesmo optar por outro protocolo que ofereça mais segurança.

Uma vez autenticado, o servidor POP abre a caixa postal do usuário e lhe diz quantas mensagens estão disponíveis. O usuário pode então listá-las e saber seu tamanho com o comando **LIST**. Com isso, o servidor POP assinala seqüencialmente um número a cada mensagem na caixa postal, e cada mensagem é referenciada por esse número. Por exemplo, para ver o conteúdo de uma mensagem, usa-se:

```
RETR <número da mensagem segundo a saída do  comando LIST>
```

É comum apagarem-se as mensagens do servidor POP após baixá-las para uma máquina local. Ou, uma caixa postal pode estar travada devido a uma mensagem de tamanho desproporcional, por exemplo. O comando para se apagar uma mensagem é:

```
DELE <número da mensagem segundo a saída do comando LIST>
```

Assim como no SMTP, encerra-se uma sessão com um “QUIT”, ou seja, uma

4. Programa que fica observando o tráfego na rede e pode pegar dados que sejam transmitidos em formato texto em sua rede.

sessão padrão usando-se o POP seria algo como:

```
$ telnet saci 110
Trying 200.192.38.238...
Connected to saci.
Escape character is '^]'.
+OK POP3 saci v7.60 server ready
USER francisco
+OK User name accepted, password please
PASS notlob
+OK Mailbox open, 5 messages
RETR 5
+OK 380 octets
Return-Path: <joao@capivara>
Received: (from joao@capivara)
        by capivara (8.9.3/8.9.3) id NAA10331
        for francisco; Fri, 19 May 2000 13:53:05 -0300
Date: Fri, 19 May 2000 13:53:05 -0300
From: João Pirana <joao@capivara>
Message-Id: <200005191653.NAA10331@capivara>
To: Francisco Pirana <francisco@saci>
Subject: Francisco!
Status:
```

```
                Almoço na casa da mãe.

                    Abraços do seu irmão,

                      João

.
DELE 5
+OK Message deleted
QUIT
+OK Sayonara
Connection closed by foreign host.
$
```

IMAP

O POP é relativamente antigo e bastante conhecido. Um protocolo mais novo, o **IMAP**, tem chamado atenção. O grande diferencial do IMAP em relação ao POP é a possibilidade de manipulação das mensagens no próprio servidor. Você pode criar pastas e organizar suas mensagens nelas, fazer buscas nas mensagens,

ver somente os cabeçalhos etc.. Se todas essas funcionalidades são quase padrão em qualquer cliente de e-mail, certamente não o são em um servidor! Essa característica é especialmente atraente quando se acessa a mesma conta de correio eletrônico a partir de mais de uma máquina.

Todo comando de IMAP deve ser precedido por um identificador chamado `tag`, normalmente algo como A0001 (mas não necessariamente). Mensagens de resposta do servidor são precedidas pelo identificador do comando em questão, e o comando **BAD** (no caso de erro como, por exemplo, não especificar todos os parâmetros para um determinado comando), **NO** (no caso de uma falha "legítima", como senha incorreta) ou **OK** (no caso de sucesso). O servidor pode também enviar mensagens que não sejam respostas a um comando do cliente, como por exemplo aviso de que há novas mensagens. Essas mensagens não solicitadas podem também ser forçadas com o comando **NOOP**. Esse comando não faz absolutamente nada. A resposta pode ser um simples **OK**. Mas, se há algo de novo com a caixa postal aberta no momento, ou simplesmente algo que o servidor queira lhe dizer, a oportunidade é aproveitada (uma resposta seria enviada ao cliente de qualquer forma).

O protocolo IMAP trabalha com **estados**. Existem 4 estados: assim que o usuário acessa o servidor, seu estado é *não autenticado*. Logo após a autenticação, como o leitor deve ter inferido, seu estado é chamado *autenticado*. Quando uma caixa postal foi selecionada e aberta, o estado é chamado *selecionado*, e, finalmente, há o estado de *logout*, quando o usuário sai do sistema (por requisição própria ou por imposição do servidor). Os comandos disponíveis variam em cada estado.

Em estado não autenticado, os comandos válidos são: **NOOP**; **CAPABILITY**, que lista as funcionalidades que o servidor implementa; **AUTHENTICATE**, que indica para o servidor o mecanismo de autenticação que se deseja utilizar, se im-

plementado; **LOGIN**, que justamente inicia o estado *autenticado*, e **LOGOUT**, que finaliza a conexão com o servidor. Os dois primeiros e o último, na verdade, podem ser usados em qualquer estado.

Assim que se acessa um servidor IMAP (usualmente na porta 143 do servidor), como no POP, o primeiro passo é normalmente a autenticação. O comando usado é o **LOGIN**, com nome de usuário e senha como parâmetros:

```
$ telnet saci 143
Trying 200.192.38.238...
Connected to saci.
Escape character is '^]'.
* OK saci IMAP4rev1 v12.252 server ready
A0001 LOGIN "francisco" "bolton"
A0001 NO LOGIN failed
A0002 LOGIN "francisco" "notlob"
A0002 OK LOGIN completed
```

Note que os parâmetros estão entre aspas duplas (“”). Além disso, esse exemplo já mostra uma mensagem de erro, como explicado acima: a sintaxe do comando **LOGIN** na primeira tentativa estava correta, mas a senha não.

No estado *autenticado*, os comandos permitidos (além dos três citados no parágrafo anterior) são:

- APPEND
- CREATE
- DELETE
- EXAMINE
- LIST
- LSUB
- RENAME
- SELECT
- STATUS
- SUBSCRIBE
- UNSUBSCRIBE

Todos lidam com caixas postais.

As caixas postais disponíveis podem ser mostradas com o comando **LIST**. Esse comando tem dois argumentos, um caminho inicial a partir do qual procura as caixas postais e um nome de caixa postal que pode conter metacaracteres. Por exemplo:

```
A0016 LIST "mail" *
* LIST (\NoSelect) "/" mail
* LIST (\NoInferiors) "/" mail/joao
A0016 OK LIST completed
```

Nesse caso, foram listados todos os arquivos do diretório `mail`. É interessante notar que, se um caminho absoluto (começando com "/") não for indicado, assume-se que o primeiro argumento deve ser considerado a partir de um caminho padrão, onde podem estar caixas postais do usuário no sistema (nesse caso, `/home/francisco`), ou seja, o comando:

```
A0017 LIST "" *
```

listaria todos os arquivos no diretório home do usuário autenticado. Os arquivos ou diretório para os quais o usuário não tem permissão de leitura simplesmente não são listados para que esse comando não gere falhas de segurança.

Um comando mais comedido é o **LSUB**. Ele lista somente arquivos ou diretórios previamente cadastrados como caixas postais (ou diretórios contendo caixas postais). Cadastramento e descadastramento de caixas postais são feitos com os comandos:

```
SUBSCRIBE <caixa postal ou diretório>
UNSUBSCRIBE <caixa postal ou diretório>
```

Assim, por exemplo:

```
A002 SUBSCRIBE mail
A002 OK SUBSCRIBE completed
A003 LSUB "" *
* LSUB () "/" mail
A003 OK LSUB completed
```

Com o comando **LIST**, como já foi visto acima, o resultado seriam todos os arquivos no diretório do usuário. Com a combinação **SUBSCRIBE/UNSUBSCRIBE + LSUB**, só os diretórios relevantes são mostrados. Isso é útil para se definirem, por exemplo, os diretórios que contêm pastas que podem posteriormente ser acessadas. Além disso, o cadastramento permanece entre sessões do IMAP (na verdade, permanece até que seja feito um descadastramento explícito).

Uma vez determinado o diretório que deverá conter as pastas de mensagens, pode-se efetivamente criar novas pastas. Para isso, usa-se o comando CREATE:

```
CREATE <nome da pasta>
```

Analogamente, o comando **DELETE** apaga a pasta especificada e o comando **RENAME** a renomeia. É importante lembrar que o nome da pasta deve ser relativo, no caso, `/home/francisco`, ou seja, o diretório padrão a partir do qual podem ser criadas pastas. Por exemplo:

```
A0002 CREATE "mail/joao"
A0002 OK CREATE completed
A0003 RENAME "mail/joao" "mail/snorman"
```

```
A0003 OK RENAME completed
A0004 DELETE "mail/joao"
A0004 NO DELETE failed: Can't delete mailbox mail/joao: no such mailbox
A0005 DELETE "mail/snorman"
A0005 OK DELETE completed
```

Para mais informações sobre uma pasta em específico, pode-se utilizar o comando **STATUS:**

```
STATUS <nome da pasta> <lista de itens>
```

A lista de itens deve vir entre parênteses e, dentro deles, os itens devem vir separados por espaço. Eles são: *MESSAGES*, que indica o número de mensagens na caixa postal ou pasta; *RECENT*, que mostra quantas dentre as anteriores são recentes; *UNSEEN*, que exibe o número de mensagens não lidas; *UIDNEXT*, que faz com que cada mensagem receba um identificador, ou **uid** do servidor (*UIDNEXT* é o **uid** que será assinalado à próxima mensagem que chegar àquela pasta) e *UIDVALIDITY* que é um identificador da pasta ou caixa postal. Seguindo nosso exemplo:

```
A0002 STATUS INBOX (MESSAGES RECENT UNSEEN)
* STATUS INBOX (MESSAGES 3 RECENT 0 UNSEEN 3)
A0002 OK STATUS completed
```

O último comando antes de passarmos ao estado *selecionado* mexe diretamente

no conteúdo de uma caixa postal: o comando **APPEND** recebe como parâmetro uma mensagem para ser incluída na caixa postal especificada.

Quando finalmente se decide qual caixa postal deve ser acessada, pode-se fazê-lo com os comandos **SELECT** e **EXAMINE**. Ambos têm a mesma funcionalidade, exceto que, usando-se o **EXAMINE** a pasta em questão será aberta somente para leitura. Nenhuma mudança será permitida, incluindo-se marcar mensagens como lidas, por exemplo. Como a sintaxe de ambos os comandos e as mensagens de resposta são idênticas, somente o **SELECT** será explicado. O mesmo vale para o **EXAMINE**. A sintaxe do comando **SELECT** é:

```
SELECT <nome da pasta ou caixa postal>
```

O valor *INBOX* indica o valor da caixa postal padrão naquele sistema, para aquele usuário. Normalmente, `/var/spool/mail/<nome do usuário>` ou, no nosso exemplo, `/var/spool/mail/francisco`:

```
A0002 SELECT INBOX
* 3 EXISTS
* NO Mailbox vulnerable - directory /var/spool/mail must have 1777 protection
* 1 RECENT
* OK [UIDVALIDITY 958755028] UID validity status
* OK [UIDNEXT 14] Predicted next UID
* FLAGS (\Answered \Flagged \Deleted \Draft \Seen)
* OK [PERMANENTFLAGS (\* \Answered \Flagged \Deleted \Draft \Seen)]
  Permanent flags
```

```
* OK [UNSEEN 1] first unseen message in /var/spool/mail/francisco
A0002 OK [READ-WRITE] SELECT completed
```

Quando pedimos para que o servidor selecionasse a pasta INBOX, sua ação foi abrir o arquivo `/var/spool/mail/francisco` e nos retornar uma série de informações. Três são particularmente interessantes neste momento:

*** 3 EXISTS:** Isso indica que há 3 mensagens na caixa postal `/var/spool/mail/francisco`

*** 1 RECENT:** Mostra quantas mensagens recentes há dentre as existentes.

A0002 OK [READ-WRITE] SELECT completed: Se o comando utilizado tivesse sido o **EXAMINE**, essa linha seria: **A0002 OK [READ-ONLY] SELECT completed**

A linha:

```
* NO Mailbox vulnerable - directory /var/spool/mail must
        have 1777 protection
```

será comentada mais adiante, quando for tratada a configuração do servidor IMAP.

No estado *selecionado*, além de todos os comandos explicados nos estados citados anteriormente, estão disponíveis:

- CHECK
- CLOSE

- COPY
- EXPUNGE
- FETCH
- SEARCH
- STORE
- UID

O comando **CLOSE** simplesmente fecha a pasta que estava selecionada, e o usuário volta ao estado *autenticado*. Para ter acesso a alguma caixa postal novamente, o usuário tem novamente de utilizar o **SELECT** ou o **EXAMINE**.

O comando **CHECK** é, basicamente, um pedido de que as pendências relativas àquela caixa postal sejam resolvidas. Por exemplo, escrita em disco de alguma mudança que tenha sido executada somente na memória do servidor. Se alguma mudança ocorrer no servidor (como por exemplo, uma nova mensagem), isso pode ser avisado, mas o servidor pode também simplesmente responder que o comando foi executado com sucesso.

O comando **EXPUNGE** apaga definitivamente da caixa postal quaisquer mensagens que tenham sido marcadas como apagadas. Essas mensagens não podem mais ser recuperadas, portanto use o comando com cuidado.

Em caixas postais grandes, é comum que se queira determinar quais mensagens satisfazem determinado critério. Por exemplo, pode-se querer saber quais as men-

sagens enviadas por uma determinada pessoa, ou em um determinado dia. O comando **SEARCH** faz uma busca (sem distinção entre maiúsculas e minúsculas) por uma grande variedade de chaves, como, por exemplo, só mensagens apagadas, mensagens maiores do que um certo tamanho, mensagens não respondidas, entre outras:

```
A0003 SEARCH SUBJECT "francisco"
* SEARCH 2 4
A0003 OK SEARCH completed
A0004 SEARCH FROM joao TEXT "porco-espinho"
* SEARCH 4
A0004 OK SEARCH completed
A0005 SEARCH FROM "Spiny Norman"
* SEARCH
A0005 OK SEARCH completed
```

Quando finalmente for hora de baixar as mensagens, usa-se o comando **FETCH**. Esse comando pede dois argumentos, uma lista de mensagens a serem baixadas e as partes das mensagens que devem ser baixadas. Isso quer dizer que você pode primeiro pegar os títulos[5] das mensagens e só baixar completamente as que interessam, ou, combinando **SEARCH** e **FETCH**, ver a data de envio de todas as mensagens de um determinado remetente.

5. subjects

Assim como no POP, todas as mensagens em uma determinada caixa postal são numeradas seqüencialmente. O primeiro argumento para o **FETCH** indica os números das mensagens a serem visualizadas. Essa lista pode ser simplesmente um número (só a mensagem naquela posição vai ser visualizada), uma série de números separados por vírgulas (sem espaço) ou um intervalo, na forma: <**primeiro número**>**:**<**último número**>.

Há muitas formas de se informar qual parte da mensagem querermos visualizar, mas uma forma básica é:

```
BODY[<;seção>]
```

onde <*seção*> pode ser, por exemplo, **TEXT**, **HEADER** ou ainda pode ser utilizada a opção **HEADER.FIELDS**:

```
A0003 FETCH 2:4 BODY[HEADER.FIELDS (Subject)]
* 2 FETCH (BODY[HEADER.FIELDS ("SUBJECT")] {22}
Subject: Francisco!


)
* 3 FETCH (BODY[HEADER.FIELDS ("SUBJECT")] {43}
Subject: My hovercraft is full of eels!


)
* 4 FETCH (BODY[HEADER.FIELDS ("SUBJECT")] {22}
```

```
Subject: Francisco!


)
A0003 OK FETCH completed
A0004 FETCH 1,3 BODY[HEADER]
* 1 FETCH (BODY[HEADER] {310}
[Cabeçalho da primeira mensagem]
* 3 FETCH (BODY[HEADER] {351}
[Cabeçalho da terceira mensagem]
A0004 OK FETCH completed
A0005 FETCH 2 (BODY[HEADER.FIELDS (Subject)] BODY[TEXT])
* 2 FETCH (BODY[HEADER.FIELDS ("SUBJECT")] {22}
Subject: Francisco!

 BODY[TEXT] {38}
       Almoço na casa da mãe.

         Abraços do seu irmão,

                 João
)
A0005 OK FETCH completed
```

Para se movimentar mensagens entre pastas, pode-se usar o comando **COPY**:

```
COPY <mensagens> <pasta>
```

Por exemplo:

```
A0003 CREATE "mail/snorman"
A0003 OK CREATE completed
A0004 COPY 2:4 "mail/snorman"
A0004 OK COPY completed
A0005 STATUS INBOX (MESSAGES)
* STATUS INBOX (MESSAGES 5)
A0005 OK STATUS completed
A0006 STATUS "mail/snorman" (MESSAGES)
* STATUS mail/snorman (MESSAGES 3)
A0006 OK STATUS completed
```

Quando se precisa alterar os atributos de uma mensagem (o caso mais comum é marcá-la como apagada, mas pode-se marcá-la como não lida, por exemplo), usa-se o comando **STORE**. Esse comando recebe como argumentos uma lista de números de mensagens (no mesmo formato do comando **FETCH**) sobre as quais deve agir. Esta opção diz se é preciso especificar exatamente os atributos da men-

sagem (**FLAGS**), quais atributos devem ser somados aos já existentes (**+FLAGS**) e quais atributos devem ser subtraídos (**-FLAGS**). Os possíveis atributos são:

\Answered: mensagem respondida.

\Deleted: mensagem marcada para ser apagada, ver o comando **EXPUNGE**.

\Draft: mensagem cuja composição ficou interminada.

\Flagged: mensagem simplesmente "marcada", normalmente para chamar atenção posteriormente.

\Seen: mensagem já lida.

:

Há um atributo, `\Recent` (mensagem nova na caixa postal), que não pode ser alterado, porque é intrínseco a um determinado instante na sessão de um usuário autenticado no servidor IMAP.

```
A0003 STATUS INBOX (MESSAGES)
* STATUS INBOX (MESSAGES 4)
A0003 OK STATUS completed
A0004 STORE 1 +FLAGS (\Deleted)
* 1 FETCH (FLAGS (\Seen \Deleted))
A0004 OK STORE completed
```

```
A0005 EXPUNGE
* 1 EXPUNGE
* 3 EXISTS
* 0 RECENT
A0005 OK Expunged 1 messages
A0006 STATUS INBOX (MESSAGES)
* STATUS INBOX (MESSAGES 3)
A0006 OK STATUS completed
```

Os comandos **COPY**, **FETCH**, **STORE** e **SEARCH** recebem argumentos especificando sobre quais mensagens eles devem agir. Nos exemplos, foi utilizado o número seqüencial que cada mensagem recebe ao entrar na caixa postal, mas cada mensagem recebe também um identificador único (não necessariamente seqüencial). As mensagens podem ser referenciadas de acordo com esse identificador pelo comando UID, que leva como parâmetros um dos comandos acima e seus argumentos, com os números das mensagens substituídos pelos identificadores.

Finalmente, quando não houver mais nada a ser feito em sua caixa postal, encerra-se a conexão:

```
A0002 LOGOUT
* BYE saci IMAP4rev1 server terminating connection
A0013 OK LOGOUT completed
Connection closed by foreign host.
[francisco ~]$
```

A Prática

Configuração do POP e do IMAP

Há vários servidores de POP e IMAP pela Internet. Entre eles, destacam-se o Qpopper, o GNU pop3d (servidores POP) e o WU-IMAPd (que, apesar do nome, tem um servidor IMAP e um POP). Este último, desenvolvido na Universidade de Washington, é o pacote que implementa ambos os protocolos em uma configuração padrão do Conectiva Linux. A configuração dos serviços não traz grandes dificuldades: deve-se instalar o pacote *imap*, descomentar as linhas relevantes em `/etc/inetd.conf`:

```
pop-3   stream  tcp     nowait  root    /usr/sbin/tcpd  ipop3d
imap    stream  tcp     nowait  root    /usr/sbin/tcpd  imapd
```

Em seguida, deve-se reiniciar o inetd:

```
# /etc/rc.d/init.d/inet restart
```

E, finalmente, certificar-se de que os serviços (ou o serviço escolhido) estejam habilitados em `/etc/services`:

```
pop-3           110/tcp                     # POP version 3
pop-3           110/udp
imap2           143/tcp         imap        # Interim Mail Access Proto v2
```

```
imap2           143/udp         imap
```

Configuração do SMTP

Como já foi citado, o SMTP é implementado por um MTA. A implementação do protocolo SMTP é bem mais crítica do que a do POP e do IMAP, pois se esses últimos falharem, as mensagens ficam esperando no servidor até que o usuário possa recebê-las de alguma forma. Se o SMTP falhar, mensagens podem ser perdidas no caminho entre um servidor e outro. Dentre os MTAs disponíveis, alguns dos mais comumente usados são Qmail, Postfix e o Sendmail (o padrão utilizado no Conectiva Linux).

O Sendmail é talvez o MTA mais conhecido de todos. Parte dessa fama se deve a falhas de segurança que, no passado, permitiam até acesso à máquina como superusuário[6]. Esses problemas em razão de o software ser muito complexo. Quem já mexeu com o arquivo de configuração do Sendmail (`sendmail.cf`) sabe o que isso significa. Hoje em dia, porém, seu desenvolvimento é ativo; um método de configuração mais amigável foi desenvolvido e o Sendmail continua a ser um padrão como MTA.

Dois métodos de configuração do sendmail serão discutidos: através do Linuxconf (o configurador gráfico utilizado no Conectiva Linux) e o m4 (o método "mais amigável" citado).

6. root

O m4 não é um método de configuração em si, mas um processador de macros. Ele permite que você use uma sintaxe mais amigável ao invés de ter de entender o rebuscado arquivo de configuração do Sendmail. Um arquivo de configuração pode ser gerado a partir de uma série de regras usando-se o m4. Assumindo-se que o arquivo com as regras em m4 seja `/usr/lib/sendmail-cf/cf/arquivo.mc` e se deseje criar um arquivo chamado sendmail.cf:

```
# cd /usr/lib/sendmail-cf/cf
# /usr/bin/m4 ../m4/cf.m4 arquivo.mc > sendmail.cf
```

No Linuxconf, as configurações do Sendmail estão dentro do menu Ambiente de Rede, sob o nome Sendmail - sistema de envio de e-mails.

Um arquivo em m4 utilizado para se gerar um `sendmail.cf` mínimo, porém funcional, seria algo como:

```
divert(-1)
include('../m4/cf.m4')
OSTYPE('linux')
FEATURE(redirect)
FEATURE(always_add_domain)
FEATURE(use_cw_file)
FEATURE(local_procmail)
MAILER(procmail)
MAILER(smtp)
```

```
FEATURE(access_db)
FEATURE(relay_hosts_only)
```

Linhas começando com “#” são consideradas comentários, tanto no arquivo m4 quanto no arquivo final de configuração. Comentários feitos no arquivo m4 são repassados para o `sendmail.cf`, a não ser que estejam no começo do arquivo e sob a diretiva

```
divert(-1)
```

A diretiva

```
divert(0)
```

reverte para o funcionamento normal.

Capítulo 8. Segurança no Servidor

Segurança é um tópico bastante abrangente, que poderia render um livro inteiro. Justamente por isto, o propósito deste capítulo não é ser um *guia absoluto de segurança*, mas mostrar como aumentar a segurança de seu Conectiva Linux.

Visão Geral sobre Segurança

Atualmente, conectar redes locais à Internet é algo bastante comum e, embora isto possa trazer vantagens, também pode trazer vários problemas. Infelizmente, fazer parte da Internet significa estar exposto a uma grande variedade de ameaças, o que obriga todo e qualquer administrador a preocupar-se com a segurança de seus sistemas. Enquanto redes existem para facilitar o acesso a computadores, procedimentos de segurança existem para controlar este acesso.

O primeiro conceito relacionado a segurança é: “não existe sistema completamente seguro”. O que é possível fazer é dificultar a invasão em sua máquina. O trabalho necessário para proteger o seu sistema dependerá basicamente do que você tem para proteger e o quão importante é proteger este sistema.

Note que, de um modo geral, quanto mais seguro você tornar o seu sistema, mais

complexa será sua utilização, pois existirão várias restrições de uso. É imprescindível usar o bom senso na hora de aplicar as medidas de segurança, para evitar que a cura seja pior que a doença.

Antes de tomar qualquer atitude relacionada a aumentar a segurança de seu sistema, você deve saber o que está sendo protegido, por que e quanto vale esta informação. Além disso, é necessário verificar a que tipo de ameaças seu sistema está exposto. A RFC 1244, intitulada *Site Security Handbook*, por Holbrook Reynold e outros, identifica três tipos distintos de ameaças de segurança geralmente associadas à conectividade em rede:

Acesso não autorizado:

Acesso ao sistema por uma pessoa não autorizada.

Revelação de informações:

Qualquer problema relacionado ao acesso a informações valiosas ou confidenciais por pessoas que não deveriam acessá-las.

Negação de Serviço:

Também conhecido como *Denial of Service* - DoS - é qualquer problema que torne impossível ou bastante difícil continuar utilizando o sistema de maneira produtiva.

Dependendo do sistema em questão, estas ameaças podem ser mais ou menos importantes. Por exemplo, para um órgão governamental ou empresa da área de

tecnologia, acessos não autorizados podem desacreditá-los perante o público e/ou clientes. Já para a grande maioria das empresas, acesso não autorizado não é um grande problema, se não envolver uma das ameaças: revelação de informações e negação de serviço.

A extensão do problema em casos de revelação de informação varia de acordo com a informação que pode ser comprometida. Embora seja fato notório que informações sigilosas jamais devam permanecer armazenadas em máquinas conectadas à Internet, em alguns casos certos tipos de informação, como informações pessoais de clientes e/ou números de cartões de crédito, podem ser necessárias em aplicações de comércio eletrônico, por exemplo. Neste tipo de caso, o cuidado deve ser redobrado.

A negação de serviço pode causar grandes prejuízos a empresas que conectam sistemas de missão crítica a Internet. Na verdade, as vantagens devem ser muito bem avaliadas antes de conectar este tipo de sistema à Internet, pois, dependendo do caso, esta conexão pode parar uma empresa por inteiro. Geralmente servidores *menores* são conectados à Internet, possivelmente acessando informações de um servidor principal através de um modo mais seguro.

Obviamente que, se a necessidade é justamente prestar um serviço na Internet, todos estes riscos existirão. Para diminuí-los, é preciso tomar algumas precauções, como desabilitar os serviços desnecessários, utilizar controle de acesso através de ferramentas como o tcp_wrappers, instalar e configurar um *firewall* entre sua rede local e redes externas (geralmente entre sua rede local e a Internet). É também importante analisar constantemente os *logs* e a integridade de arquivos importantes do sistema. O Conectiva Linux conta com as ferramentas necessárias para ajudá-lo na tarefa de tornar seu sistema mais seguro.

Finalizando esta introdução, manter um sistema seguro envolve vários procedimentos, sendo que o mais importante é manter uma monitoração constante do sistema, para notar qualquer anormalidade antes que ela se torne um problema grave.

Desabilitando Serviços Desnecessários

Os serviços normalmente habilitados no seu Conectiva Linux dependem do perfil utilizado na instalação do sistema. Portanto, após instalar o sistema, você deve verificar quais deles realmente precisam estar habilitados. Existem, basicamente, dois tipos de serviços: aqueles que rodam no modo *standalone* e aqueles que rodam através do inetd.

Serviços *Standalone*

Serviços que rodam no modo *standalone* são geralmente executados durante a inicialização do sistema, através dos chamados *scripts* de inicialização. O Apache, o Sendmail e o Samba são exemplos de serviços que costumam ser executados durante o *boot* do sistema.

Uma das ferramentas que podem ser utilizadas para configurar os serviços a

serem executados é o ntsysv. Verifique se o mesmo está instalado com o comando a seguir:

```
# rpm -q ntsysv
```

Caso a resposta para este comando seja “pacote ntsysv não está instalado”, você deve instalá-lo a partir do CD 1 do Conectiva Linux. Com o CD montado em `/mnt/cdrom`, execute o comando a seguir, como superusuário, para instalar o programa:

```
    # rpm -ivh /mnt/cdrom/conectiva/RPMS/ntsysv*
```

Com o programa instalado, como superusuário, execute-o, digitando o comando:

```
# ntsysv
```

A Figura 8-1 ilustra a tela do programa ntsysv. Através desta tela você pode (e deve) desabilitar todos os serviços que não são utilizados. Para obter uma descrição de um serviço, selecione-o e pressione a tecla de função **F1**. Note que outros tipos de serviços são iniciados automaticamente, e não apenas serviços de rede. O *gpm*, por exemplo, é um serviço que adiciona suporte a *mouse* para aplicações que rodam no modo texto. Tome o cuidado de desabilitar apenas os serviços que não devem ser utilizados na máquina. Por exemplo, não desabilite o serviço *httpd* se for necessário rodar um servidor *web* na máquina.

Figura 8-1. Configuração da Inicialização de Serviços

O ntsysv configura apenas o nível de execução atual. Se você deseja configurar outros níveis de execução, estes níveis podem ser especificados na linha de comando, através da opção `--levels`. É possível configurar vários níveis de execução simultaneamente. Executando o comando `# ntsysv --levels 345`, por exemplo, seriam configurados os níveis 3, 4 e 5 simultaneamente. Neste caso, se um serviço for marcado como habilitado, ele será habilitado em todos os níveis de execução especificados. De maneira análoga, ao desabilitar um serviço, o mesmo será desabilitado em todos os níveis de execução especificados.

Existem duas opções para sair do programa. Se for utilizado o botão Ok, as alterações serão salvas. Caso seja utilizado o botão Cancelar, nenhuma alteração efetuada será considerada.

Serviços Executados Através do inetd

O inetd, também conhecido como "*internet super-server*", é um *daemon* geral-

mente executado na inicialização do sistema e que espera por conexões em alguns *sockets internet* específicos. Quando uma conexão é estabelecida em algum destes *sockets*, ele verifica a qual serviço o *socket* corresponde e invoca o programa capaz de servir a requisição em questão. Resumidamente, o inetd invoca *daemons* sob demanda, reduzindo a carga da máquina. Obviamente, este tempo necessário para invocar um *daemon* sob demanda pode ser prejudicial em serviços muito utilizados e é por isto que muitos serviços não podem ser executados através do inetd.

A configuração do inetd reside no arquivo `/etc/inetd.conf`, embora o arquivo `/etc/services` também seja utilizado para mapear nomes de serviços para suas respectivas portas e protocolos. Estes arquivos podem ser alterados através de um editor de textos, ou então através do Linuxconf. Configurar o inetd através do Linuxconf costuma eliminar erros grosseiros, pois ele faz uma validação dos dados antes de adicionar as informações aos arquivos correspondentes.

A configuração do inetd no Linuxconf é efetuada através da configuração de Configuração →Ambiente de Rede → Tarefas de servidor → Serviços Internet. Esta configuração compreende a administração do arquivo `/etc/services` (opção *Serviços de rede para Internet*) e a administração do arquivo `/etc/inetd.conf` (opção *Base de dados dos servidores*).

Através da opção *Serviços de rede para Internet* é possível adicionar, modificar ou remover o mapeamento do nome de um serviço para sua respectiva porta e protocolo. A Figura 8-2 ilustra a configuração do serviço chamado *pop-3*.

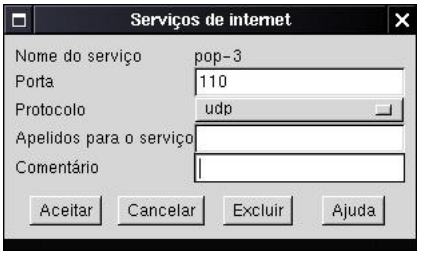


Figura 8-2. Configuração do `/etc/services`

O que realmente nos interessa na configuração de "Serviços Internet" encontra-se na opção *Base de dados dos servidores*. É neste local que é possível desabilitar todos os serviços desnecessários (ou habilitar os necessários, se for o caso).

Para desabilitar um serviço, basta selecioná-lo na lista e, na janela que aparece em seguida, marcá-lo como *Inativo*, como ilustrado na Figura 8-3.

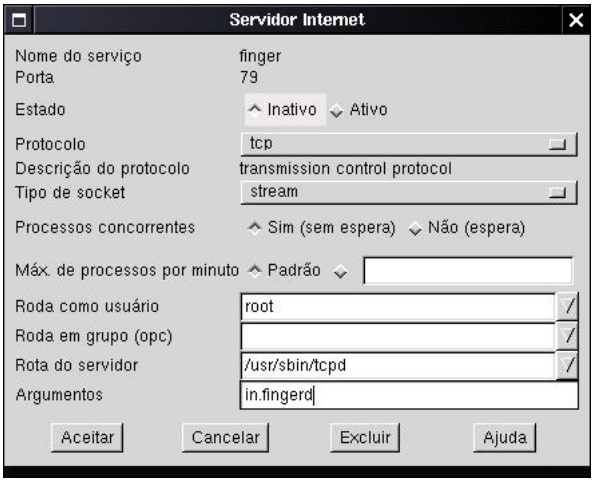


Figura 8-3. Desabilitando um Serviço

Como regra geral, mantenha desabilitados os serviços:

- echo;
- discard;
- daytime;
- chargen;
- shell;

- login;
- exec;
- talk (e similares);
- tftp;
- bootps;
- finger (e similares);
- systat;
- netstat;
- time.

Estes serviços dificilmente são necessários em sua máquina e possíveis invasores costumam utilizá-los como amostra do que está habilitado na máquina que pretendem invadir. Além destes, desabilite todos aqueles que não serão utilizados. Por exemplo, se não for necessário um servidor FTP na máquina, desabilite-o e, preferencialmente, desinstale do sistema o pacote correspondente.

Utilizando TCP_Wrappers

O pacote tcp_wrappers pode ser utilizado para controlar o acesso a alguns serviços, como por exemplo finger, telnet e ftp, entre outros. Como nem todos os *daemons* suportam o uso do tcpd [1], para controle de acesso, você deve sempre consultar a documentação dos programas antes de tentar configurá-los para utilizar o tcp_wrappers. Alguns destes programas têm seu próprio sistema de monitoração e controle de acesso, que poderia ser utilizado ao invés do tcpd.

O Conectiva Linux já vem configurado para utilizar o tcpd em todos os *daemons* possíveis e recomendados. Contudo, configurar um *daemon* para utilizar o tcpd é extremamente simples, considerando que o *daemon* em questão suporte a utilização de tcp_wrappers. A Figura 8-4 mostra a configuração de um servidor FTP sem a utilização de tcp_wrappers e a Figura 8-5 ilustra o mesmo servidor, mas desta vez, com a utilização de tcp_wrappers. Esta configuração encontra-se em Configuração →Ambiente de Rede→ Tarefas de servidor → Serviços Internet → Base de dados dos servidores → ftp.

1. Este é o nome do programa responsável pela monitoração dos serviços, no pacote tcp_wrappers.

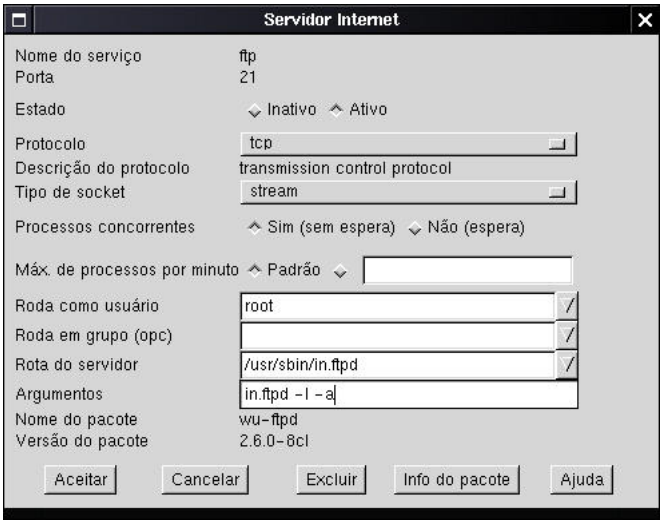


Figura 8-4. Servidor FTP sem tcp_wrappers

Compare a configuração *Rota do servidor Path* entre a Figura 8-4 e a Figura 8-5, a seguir.

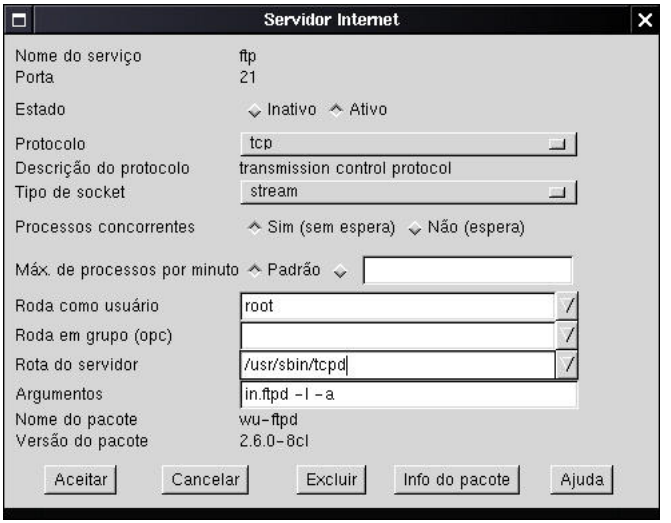


Figura 8-5. Servidor FTP Utilizando tcp_wrappers

Após configurar um *daemon* para utilizar o pacote tcp_wrappers é necessário configurar o controle de acesso propriamente dito. Esta configuração pode ser efetuada através dos arquivos `/etc/hosts.allow` e `/etc/hosts.deny`. No arquivo `/etc/hosts.deny` configuram-se regras para negar serviços a determinados clientes, ao mesmo tempo em que no arquivo `/etc/hosts.allow` configuram-se regras para permitir que determinados clientes tenham acesso a serviços.

Existem dezenas de possibilidades de configuração para o tcp_wrappers e você pode estudá-las em extensão através das páginas de manual *hosts_access(5)* e

hosts_options(5). Portanto, iremos ilustrar apenas alguns casos interessantes do uso desta ferramenta.

As regras de controle de acesso, existentes nestes dois arquivos, têm o seguinte formato:

```
lista_de_daemons : lista_de_clientes [ : comando ]
```

lista_de_daemons

: Lista de um ou mais nomes de *daemons* como especificados no `/etc/inetd.conf`, ou curingas.

lista_de_clientes

: Lista de um ou mais endereços ou nomes de máquinas, padrões ou curingas utilizados para especificar quais clientes podem e quais não podem acessar o serviço.

comando (opcional)

: É possível executar um comando sempre que uma regra casa com um padrão e é utilizada. Veja exemplos a seguir.

Como citado anteriormente, curingas podem ser utilizados tanto na lista de *daemons* quanto nas lista de clientes. Entre os existentes, podemos destacar os seguintes:

ALL

Significa todos os *daemons* ou todos os clientes, dependendo apenas do campo em que se encontra.

LOCAL

Este curinga casa com qualquer nome de máquina que não contenha um caractere ponto ".", isto é, uma máquina local.

PARANOID

Casa com qualquer nome de máquina que não case com seu endereço. Isto geralmente ocorre quando algum servidor DNS está mal configurado ou quando alguma máquina está tentando se passar por outra.

Na lista de clientes podem ser utilizados nomes ou endereços de máquinas, ou então padrões que especificam um conjunto de máquinas. Se a cadeia de caracteres que identifica um cliente inicia com um ponto ".", um nome de máquina irá casar com este padrão sempre que o final do mesmo casar com padrão especificado. Por exemplo, se fosse utilizada a cadeia de caracteres ".conectiva.com.br", o nome de máquina "gateway.conectiva.com.br" casaria com o padrão.

Similarmente, se a cadeia de caracteres termina com um ponto ".", um endereço de máquina irá casar com o padrão quando seus campos numéricos iniciais casarem com a cadeia de caracteres especificada. Para exemplificar, se fosse utilizada a cadeia de caracteres "192.168.220.", todas as máquinas que tenham um endereço IP que inicie com estes 3 conjuntos de números irão casar com o padrão

(192.168.220.0 ao 192.168.220.255).

Além destes métodos, é possível identificar um cliente através do IP/máscara de rede. Você pode especificar, por exemplo, “192.168.220.0/255.255.255.128”, e qualquer máquina com endereço IP entre 192.168.220.0 e 192.168.220.127 casaria com o padrão.

Nada melhor do que exemplos práticos para facilitar o entendimento. Uma boa política é fechar completamente o acesso de todos os serviços a quaisquer clientes, através do arquivo `/etc/hosts.deny`, e seletivamente liberar o acesso aos serviços necessários através do arquivo `/etc/hosts.allow`. No Exemplo 8-1, temos uma configuração em que liberamos o acesso a FTP apenas ao domínio “rede.net”, o acesso ao servidor POP3 a qualquer máquina, todos os serviços para “localhost” e negamos os demais serviços para qualquer máquina que seja.

Exemplo 8-1. Exemplo de Configuração do tcp_wrappers

Segue abaixo o arquivo `/etc/hosts.deny`.

```
# hosts.deny
# Este arquivo lista os nomes das máquinas que _NÃO_ têm
# permissão para usar os serviços oferecidos por esta
# máquina através do INET, usando o servidor
# /usr/sbin/tcpd (tcp_wrapper) para checar permissões.
# Recomendamos a leitura do manual hosts_access, na seção
# 5; para tanto execute:
```

```
# man 5 hosts_access
#
# Lembre-se de que o novo portmap utiliza este arquivo para decidir quais
# máquinas podem acessar os serviços de NFS oferecidos por esta máquina.
ALL:ALL
```

Arquivo `/etc/hosts.allow`.

```
# hosts.allow
# Este arquivo lista os nomes das máquinas que têm
# permissão para usar os serviços oferecidos por esta
# máquina através do INET, usando o servidor
# /usr/sbin/tcpd (tcp_wrapper) para checar permissões.
# Recomendamos a leitura do manual hosts_access, na seção
# 5; para tanto execute:
# man 5 hosts_access
ALL: localhost
in.ftpd: .rede.net
ipop3d: ALL
```

No Exemplo 8-2, considere o mesmo arquivo `/etc/hosts.deny` do exemplo anterior.

Exemplo 8-2. Configuração do tcp_wrappers Menos Restritiva

Arquivo `/etc/hosts.allow`.

```
# hosts.allow
# Este arquivo lista os nomes das máquinas que têm
# permissão para usar os serviços oferecidos por esta
# máquina através do INET, usando o servidor
# /usr/sbin/tcpd (tcp_wrapper) para checar permissões.
# Recomendamos a leitura do manual hosts_access, na seção
# 5; para tanto execute:
# man 5 hosts_access
ALL: localhost
in.ftpd: .rede.net 200.234.123.0/255.255.255.0 200.248.
ipop3d: ALL EXCEPT hackerboys.org
```

Neste último caso, máquinas da rede “200.234.123.0/255.255.255.0” e máquinas em que o endereço IP inicie por “200.248.” também podem acessar o serviço FTP. Note que utilizamos um operador novo para o serviço ipop3d: EXCEPT. Isto permitiu que o acesso a este serviço fosse liberado para todos, exceto para máquinas da rede “hackerboys.org”.

O operador EXCEPT pode ser utilizado tanto da lista de clientes quanto na lista de *daemons*. Por exemplo, a linha:

```
ALL EXCEPT in.ftpd: ALL
```

no arquivo `/etc/hosts.allow`, permite o acesso a todos os serviços, exceto FTP, para qualquer máquina.

Todos os acessos, bem sucedidos ou não, são registrados através do syslog. No Conectiva Linux, estas informações são registradas no arquivo `/var/log/secure`. É recomendado que este arquivo seja periodicamente analisado à procura de tentativas de invasão.

Vários outros exemplos de configuração estão descritos nas páginas de manual da seção 5 citadas anteriormente (*hosts_access* e *hosts_options*).

Firewall Através de Filtro de Pacotes

Um *firewall* é um sistema que isola redes distintas e permite que se controle o tráfego entre elas. Um exemplo típico onde a utilização de um *firewall* é recomendada é na conexão de uma rede local à Internet. Embora o conceito de *firewall* seja bastante amplo e possa envolver servidores *proxy*, analisadores de *logs* e filtros de pacotes, entre outras características, iremos, nesta seção, deter-nos no filtro de pacotes fornecido pelo kernel do Linux.

O kernel do Linux conta com um filtro de pacotes bastante funcional, que permite que sua máquina descarte ou aceite pacotes IP, baseando-se na origem, no destino e na interface pela qual o pacote foi recebido. A origem e o destino de um pacote são caracterizados por um endereço IP, um número de porta e pelo protocolo.

Todo o tráfego através de uma rede é enviado no formato de pacotes. O início de cada pacote informa para onde ele está indo, de onde veio e o tipo do pacote, entre outros detalhes. A parte inicial deste pacote é chamada cabeçalho. O restante do pacote, contendo a informação propriamente dita, costuma ser chamado de corpo do pacote.

Um filtro de pacotes analisa o cabeçalho dos pacotes que passam pela máquina e decide o que fazer com o pacote inteiro. Possíveis ações a serem tomadas em relação ao pacote são:

aceitar: o pacote pode seguir até seu destino.

rejeitar: o pacote será descartado, como se a máquina jamais o tivesse recebido.

bloquear: o pacote será descartado, mas a origem do pacote será informada de que esta ação foi tomada.

O filtro de pacotes do kernel é controlado por *regras de firewall*, as quais podem ser divididas em 4 categorias: a cadeia de entrada (*input chain*), a cadeia de saída (*output chain*), a cadeia de reenvio (*forward chain*) e cadeias definidas pelo usuário (*user defined chain*). Para cada uma destas cadeias é mantida uma tabela de regras separada.

Uma regra de *firewall* especifica os critérios de análise de um pacote e o seu alvo (*target*). Se o pacote não casa com o padrão especificado pela regra, a regra

seguinte da cadeia é analisada. Se desta vez o pacote casar com o padrão, a regra seguinte é definida pelo alvo, que pode ser o nome de uma cadeia definida pelo usuário, ou um dos seguintes valores especiais:

ACCEPT

Significa que o filtro de pacotes deve deixar o pacote passar.

DENY

Significa que o filtro de pacotes deve impedir que o pacote siga adiante.

REJECT

Assim como *DENY*, significa que o pacote não deve seguir adiante, mas uma mensagem ICMP é enviada ao sistema originador do pacote, avisando-o de que o pacote foi rejeitado. Note que *DENY* e *REJECT* têm o mesmo significado para pacotes ICMP.

MASQ

Este alvo somente é válido para a cadeia de reenvio e para cadeias definidas pelo usuário, e somente pode ser utilizado quando o kernel é compilador com suporte a IP Masquerade. Neste caso, pacotes serão mascarados como se eles tivessem sido originados pela máquina local.

REDIRECT

Este alvo somente é válido para a cadeia de entrada e para cadeias definidas pelo usuário e somente pode ser utilizado se o kernel foi compilado com a opção de *Transparent proxy*. Com isto, pacotes serão redirecionados para um *socket* local, mesmo que eles tenham sido enviados para uma máquina remota. Obviamente isto só faz sentido se a máquina local é utilizada como *gateway* para outras máquinas. Se a porta especificada para redirecionamento é "0", que é o valor padrão, a porta de destino dos pacotes será utilizada como porta de redirecionamento. Se for especificada uma outra porta qualquer, esta será utilizada, independentemente daquela especificada nos pacotes.

RETURN

Se a regra contendo o alvo *RETURN* foi chamada por uma outra regra, a regra seguinte da cadeia que a chamou é analisada. Caso ela não tenha sido chamada por outra regra, a política padrão da cadeia é utilizada para definir o destino do pacote.

A configuração do filtro de pacotes no kernel 2.2 é efetuada através do programa de linha de comando ipchains. Contudo, o Linuxconf tem um módulo de configuração do filtro de pacotes que facilita bastante a configuração. Antes de tentar configurar o filtro de pacotes, certifique-se de que o o pacote ipchains está instalado e de que o módulo *firewall* está habilitado no Linuxconf[2]. Para verificar se o ipchains está instalado, execute o comando:

2. Este módulo é habilitado por padrão, no Conectiva Linux.

```
# rpm -q ipchains
```

Caso a resposta para este comando seja “pacote ipchains não está instalado”, você deve instalá-lo a partir do CD 1 do Conectiva Linux. Com o CD montado em `/mnt/cdrom`, execute o comando a seguir, como superusuário, para instalar o programa:

```
# rpm -ivh /mnt/cdrom/conectiva/RPMS/ipchains*
```

Já para verificar se o módulo do Linuxconf está habilitado, siga os passos descritos no capítulo do Linuxconf.

Configuração do Filtro de Pacotes Pelo Linuxconf

A configuração do filtro de pacotes no Linux é bastante flexível e pode facilmente tornar-se uma tarefa complicada. O Linuxconf propõe uma lógica simples que facilita a configuração das regras de *firewall*. Ao mesmo tempo que esta lógica ajuda a criar e manter configurações de um *firewall* básico, ela impede que algumas configurações mais sofisticadas sejam criadas com o Linuxconf.

Dentro desta lógica, quando você ativa qualquer uma das três cadeias (entrada, saída ou reenvio), o Linuxconf irá configurar a política padrão da cadeia como *DENY*. Todas as regras que você adicionar são aberturas no *firewall*. Se você não adicionar regra alguma, sua máquina ficará completamente isolada. Note que,

por causa desta filosofia, o Linuxconf não suporta cadeias definidas pelo usuário, entre outras funcionalidades.

Em geral, configurando apenas a cadeia de entrada, chamada de *firewall por entrada* no Linuxconf, já temos um bom controle sobre o que pode ser acessado na máquina. Para habilitar a cadeia de entrada, marque a opção “Regras de entrada” em Configuração →Ambiente de Rede→ Firewall → Padrões do firewall.

Como citado anteriormente, isto fará com que a política padrão da cadeia de entrada seja *DENY*. Portanto, você deve adicionar regras para *reduzir* esta restrição, de maneira que seja possível acessar *alguma coisa* na máquina.

Supondo que se queira permitir apenas o acesso a um servidor *web* que escuta na porta 80 da máquina, e barrar todo o resto, uma única regra seria suficiente.

Você deve, então, adicionar uma regra de *firewall por entrada* (Configuração →Ambiente de Rede→ Firewall → Firewall por entrada). A Figura 8-6 ilustra a janela de configuração de regras de entrada.

Figura 8-6. Configuração de Regras de Entrada

Nesta janela existe um *checkbox* que permite ativar ou desativar a regra. Em seguida, existem os seguintes campos:

Comentário

Local para descrever a regra de maneira sucinta

Protocolo

Local para especificar para quais protocolos a regra em questão é válida. Valores possíveis são: *all*, para todos os protocolo; *tcp*; *udp* e *icmp*.

Política de regras

Define a política da regra, especificando o que será feito com aqueles pacotes que chegarem até a regra. A política pode ser *aceitar*, *rejeitar* ou *bloquear* (ACCEPT, REJECT ou DENY, respectivamente).

O restante das informações necessárias para configurar uma regra estão dispostas em três guias. A Figura 8-7 ilustra a guia “Para”, que como pode ser observado, é idêntica à guia “De”, ilustrada na Figura 8-6. Contudo, os dados inseridos na guia “De” são referentes à origem do pacote, enquanto que na guia “Para” os dados são referentes ao destino do mesmo.

Figura 8-7. Configuração de Guias

Os campos existentes em ambas as guias (De e Para) estão descritos a seguir:

Máquina ou rede

Local para especificar a origem (guia De) ou destino (guia Para) de um pacote. Especifique preferencialmente um endereço IP, embora seja possível especificar um nome de máquina, que será posteriormente resolvido pelo DNS.

Máscara

Local para definir a máscara de rede referente ao endereço IP (ou nome de máquina) utilizado no campo acima. Procure sempre informar uma máscara de rede, para evitar que o Linuxconf pense por você.

Faixa de portas

Local para especificar uma faixa de portas de origem (guia From) ou de destino (guia To) do pacote a que a regra se refere.

Outras portas

Local para especificar outras portas de origem (guia From) ou de destino (guia To) do pacote a que a regra se refere.

Accept *TCP Syn Packet*

Se esta opção for desabilitada (sendo que o padrão é estar habilitada), pacotes que solicitam o início de uma conexão não serão aceitos. Só faz sentido desabilitar esta opção quando a regra especifica o protocolo TCP e a política da regra é “aceitar”.

Interface de entrada

Local para especificar a interface pela qual o pacote deve estar entrando.

A guia seguinte é a guia “Características” (Figura 8-8).

Figura 8-8. Configuração da Guia *Características*

Esta guia conta com os seguintes campos:

Esta regra é bidirecional

Se esta opção estiver marcada (padrão), a regra será repetida com origem e destino invertidos. É por isto que o Linuxconf lhe permite especificar a interface duas vezes.

Se você não gosta deste comportamento, apenas desative a opção

Fator de ordenação

Permite que você atribua um valor para cada regra, de maneira que você possa ordená-las como desejar. Regras com fator menor são avaliadas primeiro.

Registrando está ativo

Se habilitada, esta opção fará com que o kernel imprima informações sobre o pacote através da função `printk`(), sempre que um pacote casar com a regra em questão. No Conectiva Linux, isto significa que estas informações serão gravadas no arquivo `/var/log/messages`.

Redirecione para porta local

Se habilitada, esta opção fará com que os pacotes que casarem com a regra em questão sejam redirecionados para a máquina local. Você poderia, por exemplo, redirecionar todos os pacotes destinados a um servidor FTP da sua rede para uma porta local da máquina utilizada como *gateway*.

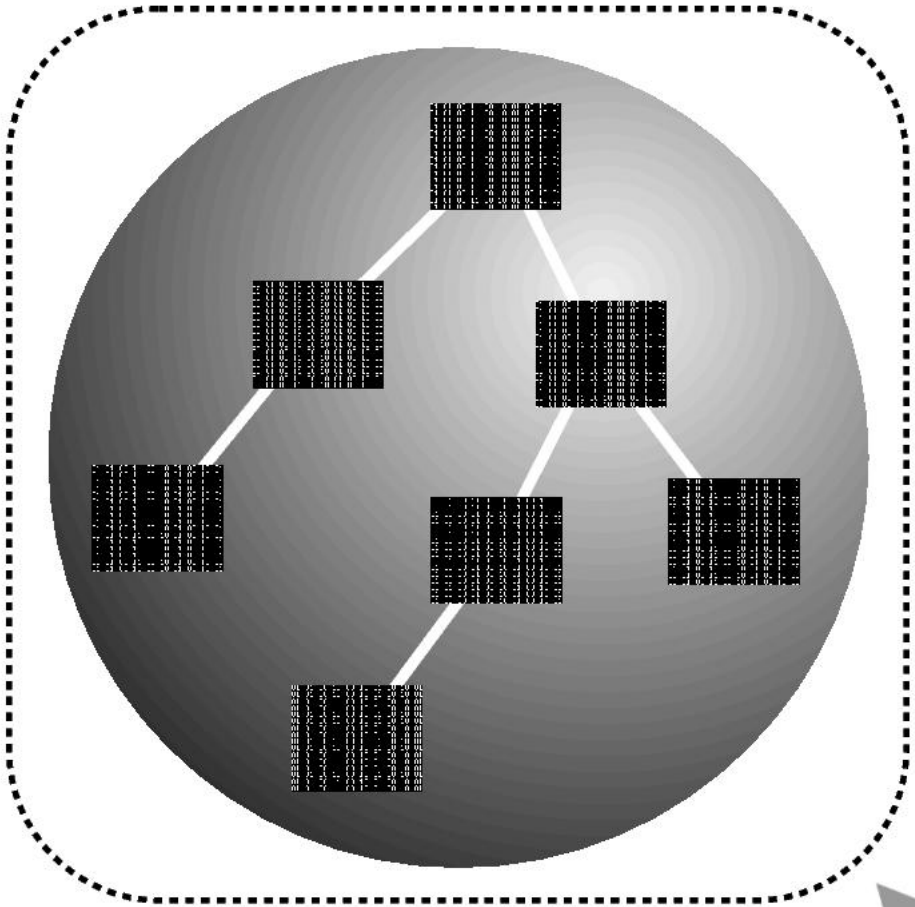
Porta de redirecionamento

Se não for especificada porta alguma neste campo, a porta de destino do pacote será utilizada como porta de redirecionamento. Caso alguma porta seja especificada, esta será utilizada como porta de redirecionamento.

> É possível que, ao adicionar uma regra errada, sua máquina pare de funcionar corretamente. Neste caso, utilize o comando `netconf --resetfw`, que todas as regras do filtro de pacotes serão temporariamente desativadas.

Além de adicionar regras para pacotes que entram na máquina, é possível adicionar regras para pacotes que saem da máquina e para pacotes que passam *através* da máquina, de uma interface de rede para outra. O Linuxconf utiliza os termos "Firewall para saída" e "Firewall por reenvio", respectivamente, para definir estes dois tipos de regras. Enquanto que, regras de saída não têm um uso muito grande em grande parte dos casos, regras de reenvio são comumente utilizadas quando se tem uma máquina como *gateway* entre uma rede local e a Internet (ou outra rede qualquer).

Por este motivo, nos deteremos na explicação do "Firewall por reenvio". Além disto, a configuração de regras de entrada e de saída são semelhantes, embora a lógica seja invertida. Na Figura 8-9, pode ser observado um exemplo típico de utilização de "Firewall por reenvio".



Nesta gravura, considere que os endereços IP da rede local são públicos, isto é, podem ser utilizados na Internet e foram designados pela empresa que fornece a conexão.

Para permitir que as máquinas da rede local possam acessar máquinas existentes na Internet não é necessária qualquer regra de reenvio. A única exigência é que o kernel esteja compilado com "IP firewalling" e que o mesmo esteja habilitado. A maneira de habilitar esta característica do kernel é efetuar o seguinte comando, como superusuário:

```
# echo 1 > /proc/sys/net/ipv4/ip_forward
```

O Conectiva Linux pode habilitar esta característica automaticamente, durante a inicialização do sistema. Para que isto ocorra, deve existir uma linha com:

```
IP_FORWARD="yes"
```

ou

```
IP_FORWARD="true"
```

no arquivo `/etc/sysconfig/network`. Se o valor desta variável for "no" ou "false", o Conectiva Linux não habilitará esta característica durante a inicialização do sistema.

Embora nenhuma regra de reenvio seja necessária para possibilitar que as máquinas da rede local acessem a Internet, pode ser interessante bloquear o acesso a alguns serviços. Por exemplo, pode ser útil bloquear a repassagem de pacotes que destinam-se à porta 80 (HTTP, geralmente), para forçar a utilização de um servi-

dor proxy para acesso à *web*. A configuração desta regra está ilustrada nas figuras a seguir.

Figura 8-10. Firewall Reenvio - Origem do Pacote

Figura 8-11. Firewall Reenvio - Destino do Pacote

Figura 8-12. Firewall Reenvio - Features

Como o Linuxconf coloca a política padrão da cadeia como “DENY”, assim que a mesma é habilitada, será necessário adicionar mais uma regra, explicitamente liberando o acesso nos demais casos (quando o destino do pacote não for a porta 80 de uma máquina qualquer). Adicione então, uma regra de reenvio, conforme ilustram as figuras a seguir.

Figura 8-13. Adicionando uma Regra de Origem de Pacote

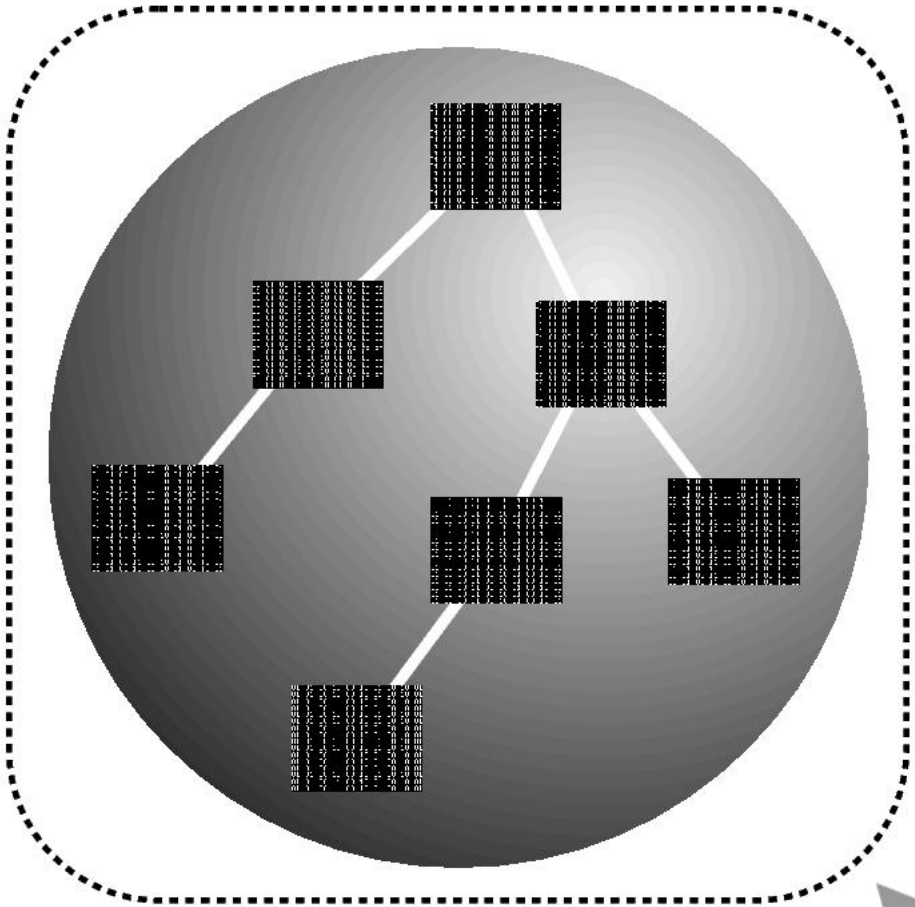
Figura 8-14. Adicionando uma Regra de Destino de Pacote

Figura 8-15. Firewall Reenvio - Adicionando uma Regra

Note que, nesta última regra, o *Ordering factor* foi definido como “100”, para que esta regra seja avaliada por último. Qualquer pacote bloqueado pela regra anterior não chegará até esta última.

> Não esqueça de habilitar as “Regras de reenvio” (Configuração → Ambiente de Rede → Firewall → Padrões do firewall), ou estas regras não serão avaliadas.

Uma outra situação bastante típica está ilustrada na Figura 8-16.



Int

Nesta situação, os endereços IP da rede local são privados, isto é, as máquinas não fazem parte da Internet. Estas máquinas somente podem acessar a Internet através de um servidor *proxy* ou se o *gateway* fizer algum tipo de NAT (*Network Address Translation*). O kernel do Linux proporciona esta funcionalidade através da característica conhecida como "IP Masquerade" (mascaramento de IP). Configurar esta funcionalidade no Conectiva Linux é tão simples quanto configurar as regras de reenvio demonstradas anteriormente. A única diferença é que deve ser marcada a opção *mascarar* existente na janela de configuração da regra. Observe o exemplo da Figura 8-17.

Figura 8-17. Configurando o IP Masquerade

O restante da regra deve ser configurado normalmente (origem do pacote, destino e *features*). Resumindo o funcionamento do "IP Masquerade", ele faz com que o kernel traduza os IPs da rede local, que são privados, para o IP da interface que tem um IP público. Quando uma máquina da rede faz uma requisição, esta vai através do *gateway*, que faz esta *tradução* de endereços, refaz a requisição para a máquina de destino e, quando recebe a resposta, envia-a para a máquina que fez a solicitação.

Esta técnica não funciona em todos os casos, pois alguns protocolos exigem que a máquina remota abra uma conexão com o cliente, e quando utiliza-se "IP Mas-

querade" isto geralmente não é possível. É por este motivo que alguns programas não funcionam perfeitamente em uma rede que utiliza mascaramento de IP. Contudo, serviços simples como WWW e e-mail funcionam perfeitamente. O kernel do Linux conta com alguns módulos especiais que aumentam a capacidade do "IP Masquerade", para que ele possa funcionar com mais protocolos e programas. Através do Linuxconf, em Configuração → Ambiente de Rede → Firewall → Padrões do Firewall, você pode habilitar estes módulos (CuSeeMe, FTP e IRC, entre outros). A Figura 8-18 ilustra esta tela de configuração.

Figura 8-18. Firewall - IP Masquerade

Consulte outras informações na Internet no site Linux IP Masquerade Resource (http://ipmasq.cjb.net); você pode encontrar informações sobre configuração do "IP Masquerade" no site Masq Apps (http://www.tsmservices.com/masq/).

Verificando a Integridade do Sistema

Uma das primeiras ações de um invasor costuma ser substituir arquivos e programas do sistema com o intuito de mascarar sua *visita* atual e, principalmente, facilitar as *visitas* futuras. Portanto, se houver a possibilidade de verificar a integridade de arquivos do sistema, há uma grande possibilidade de detectar uma invasão. E o melhor é que este recurso permite que se saiba *quais* arquivos foram modificados, possibilitando que o administrador decida entre reinstalar o sistema ou apenas substituir o arquivos alterados pelos originais.

Após perceber que a máquina foi invadida, o administrador costuma analisar o sistema utilizando programas como ps, ls, netstat e who. Ocorre que estes programas são os primeiros a serem substituídos, ocultando, assim, a invasão e o invasor propriamente dito. Mesmo que se tenha a informação de data e tamanho dos arquivos originais, estas informações, sozinhas, não podem ser utilizadas como parâmetro, pois podem ser facilmente modificadas. Contudo, se além destas informações estiver disponível algo como o *checksum* MD5 dos arquivos, torna-se bem mais simples encontrar arquivos indevidamente modificados.

O AIDE (*Advanced Intrusion Detection Environment*) é um programa que tem justamente a finalidade de verificar a integridade dos arquivos do sistema. Ele constrói uma base de dados com várias informações dos arquivos especificados em seu arquivo de configuração. Esta base de dados pode conter vários atributos dos arquivos, como:

- permissões;
- número do *inode*;

- dono;
- grupo;
- tamanho;
- data e hora de criação, último acesso e última modificação.

Além disso, o AIDE também pode gerar e armazenar nesta base de dados o *checksum* criptográfico dos arquivos, utilizando um, ou uma combinação dos seguintes algoritmos: md5, sha1, rmd160 e tiger.

O procedimento recomendado é que você crie esta base de dados em um sistema recém-instalado, antes de conectá-lo a uma rede. Esta base de dados será a *fotografia* do sistema em seu estado normal e o parâmetro a ser utilizado para medir alterações no sistema de arquivos. Obviamente, sempre que você modificar o seu sistema, como por exemplo através da instalação, atualização ou remoção de programas, uma nova base de dados deve ser gerada. Esta nova base de dados é que deve ser utilizada doravante como parâmetro. A base de dados deve conter informações sobre binários, bibliotecas e arquivos de cabeçalhos importantes do sistema, já que estes não costumam ser alterados durante o uso normal do sistema. Informações sobre arquivos de *log*, filas de correio eletrônico e de impressão, diretórios temporários e de usuários não devem ser armazenados na base de dados, já que são arquivos e diretórios freqüentemente alterados.

Configuração do AIDE

A configuração do AIDE reside no arquivo `/etc/aide.conf`. Este arquivo tem três tipos de linhas:

linhas de configuração: utilizadas para definir parâmetros de configuração do AIDE.

linhas de seleção: utilizadas para indicar quais arquivos terão suas informações adicionados à base de dados.

linhas de macro: utilizadas para definir variáveis no arquivo de configuração.

Apenas as *linhas de seleção* são essenciais ao funcionamento do AIDE. Existem, por sua vez, três tipos de linhas de seleção. Estas linhas são interpretadas como expressões regulares. Linhas que começam com uma barra "/" indicam que os arquivos que casarem com o padrão terão suas informações adicionadas ao banco de dados. Se a linha iniciar com um ponto de exclamação "!", ocorre o contrário: os arquivos que casam com o padrão são desconsiderados. Linhas iniciadas por um sinal de igualdade "=" informam ao AIDE que somente arquivos que sejam exatamente iguais ao padrão devem ser considerados.

Através das *linhas de configuração* é possível definir alguns parâmetros de funcionamento do AIDE. Estas linhas tem o formato parâmetro=valor. Os parâmetros de configuração estão descritos a seguir:

database

A URL do arquivo de banco de dados de onde as informações são lidas. Pode haver somente uma linha destas. Se houver mais de uma, apenas a primeira é considerada. O valor padrão é `./aide.db`.

database_out

A URL do arquivo de banco de dados onde são escritas as informações. Assim como *database*, deve haver apenas uma linha destas. No caso de haver várias, somente a primeira ocorrência é considerada. O valor padrão é `./aide.db.new`.

report_url

A URL onde a saída do comando é escrita. Se existirem várias instâncias deste parâmetro, a saída será escrita em todas as URLs. Se você não definir este parâmetro, a saída será enviada para a saída padrão (*stdout*).

verbose

Define o nível de mensagens que é enviado à saída. Este valor pode estar na faixa entre 0 e 255 (inclusive) e somente a primeira ocorrência deste parâmetro será considerada. É possível sobrescrever este valor através das opções `--version` ou `-V` na linha de comando.

gzip_dbout

Informa se o banco de dados deve ser compactado ou não. Valores válidos para esta opção são *yes*, *true*, *no* e *false*.

Definições de grupos

Se o parâmetro não for nenhum dos anteriores então ele é considerado uma definição de grupo. Embora existam alguns grupos predefinidos que informam ao AIDE quais as informações do arquivo que devem ser armazenadas na base de dados, você pode criar suas próprias definições. A Tabela 8-1 mostra os grupos predefinidos.

Tabela 8-1. Grupos Predefinidos

p	permissões
i	*inode*
n	número de *links*
u	dono
g	grupo
s	tamanho
m	data e hora da última modificação
a	data e hora do último acesso

c	data e hora da criação do arquivo
S	verifica o aumento do tamanho do arquivo
md5	*checksum md5*
sha1	*checksum sha1*
rmd160	*checksum rmd160*
tiger	*checksum tiger*
R	p+i+n+u+g+s+m+c+md5
L	p+i+n+u+g
E	grupo vazio
>	arquivo de *log (aumenta o tamanho)* - *p+u+g+i+n+S*

Você poderia definir um grupo que verifica apenas o dono e o grupo do arquivo, da seguinte maneira:

```
trivial=u+g
```

As *linhas de macro* podem ser utilizadas para definir variáveis e tomar decisões baseadas no valor das mesmas. Informações detalhadas podem ser encontradas na página de manual `aide.conf(5)`.

O termo URL, utilizado na configuração dos parâmetros *database*, *database_out* e *report_url*, pode assumir um dos seguintes valores:

stdout: a saída é enviada para a saída padrão.

stderr: a saída é enviada para a saída padrão de erros.

stdin: a entrada é lida da entrada padrão.

file:/arquivo: a entrada é lida de `arquivo` ou a saída é escrita em `arquivo`.

fd:número: a entrada é lida do *filedescriptor número* ou a saída é escrita no *filedescriptor número.*

Note que URLs de entrada não podem ser utilizadas como saídas e vice-versa.

O Exemplo 8-3 ilustra uma configuração básica para o AIDE.

Exemplo 8-3. Arquivo de Configuração do AIDE

```
# Localização da base de dados
database=file:/var/aide/aide.db
# Local onde é criada uma base de dados nova
database_out=file:/var/aide/aide.db.new
# Arquivo onde será salva a saída do programa
report_url=/var/aide/report.aide

# Grupo para verificação de dono, grupo e permissões
trivial=u+g+p
```

```
/bin R
/sbin R
/boot R
/etc R
# Verifica apenas dono, grupo e permissões
/etc/passwd trivial
/etc/shadow trivial
# Ignora o diretório /etc/X11
!/etc/X11
/lib R

# Incluido /var
/var R
# Ignora /var/log, /var/spool e /var/lock
!/var/log/.*
!/var/spool/.*
!/var/lock/.*
# Ignora o arquivo /var/run/utmp
!/var/run/utmp$
```

Normalmente, o ideal é ignorar diretórios que são modificados com muita freqüência, a não ser que você goste de *logs* gigantescos. É um procedimento re-

comendado excluir diretórios temporários, filas de impressão, diretórios de *logs* e quaisquer outras áreas freqüentemente modificadas. Por outro lado, é recomendado que sejam incluídos todos os binários, bibliotecas e arquivos de cabeçalhos do sistema. Muitas vezes é interessante incluir diretórios que você não costuma observar, como o `/dev/` e o `/usr/man`.

> Se você deseja referir-se a um único arquivo, você deve colocar um *$* no final da expressão regular. Com isto, o padrão casará apenas com o nome exato do arquivo, desconsiderando arquivos que tenham o início do nome similar.

O pacote do AIDE que acompanha o Conectiva Linux tem um arquivo de configuração padrão funcional, mas nada o impede de modificá-lo para refletir suas necessidades.

Utilização do AIDE

Como o arquivo de configuração padrão deverá servir para a maioria dos casos, para gerar o banco de dados, basta executar os comandos:

```
# /usr/bin/aide -i

# mv /var/aide/aide.db.new /var/aide/aide.db
```

Após esta operação, você deve executar o comando:

```
# /usr/bin/aide-md5 [dispositivo de boot]
```

O parâmetro *dispositivo de boot* é opcional, e corresponde ao dispositivo de armazenamento utilizado para inicialização do sistema (`/dev/hda`, por exemplo).

O aide-md5 foi desenvolvido pela Conectiva e supre a falta de assinatura do banco de dados do AIDE. Ele informa os somatórios MD5 de alguns componentes críticos ao funcionamento do AIDE, inclusive do próprio banco de dados recém-gerado. Você deve tomar nota desses somatórios para verificação posterior.

Se o dispositivo de boot for informado ao aide-md5, o MD5 do setor de boot também será calculado, portanto é interessante informar esse parâmetro.

Para verificar a integridade do sistema, execute o próprio AIDE, desta forma:

```
# /usr/bin/aide -C
```

Os arquivos que sofreram qualquer mudança, seja no tamanho, conteúdo, permissões ou data de criação, serão listados.

É provável que, na maioria das vezes que o AIDE apontar diferenças em arquivos, elas tenham sido provocadas por atos legítimos, por exemplo, atualização de pacotes ou intervenção do administrador do sistema. Nesses casos, o administrador deve, após uma conferência, reconstruir o banco de dados.

Para verificar a integridade do próprio AIDE, deve-se novamente utilizar o programa aide-md5, mas desta vez, de uma *mídia removível*, como por exemplo, de um disquete:

```
# /mnt/floppy/aide-md5 /dev/hda
```

Se algum dos códigos MD5 não bater com aqueles gerados anteriormente, o(s) respectivo(s) componentes podem estar comprometidos, e isto é um problema *muito* sério.

Obviamente que, se você alterou as configurações do AIDE, regerou o banco de dados ou atualizou o kernel, os códigos serão diferentes. Logo após efetuar quaisquer destas alterações, você deve executar novamente o aide-md5 e anotar os códigos.

> É altamente recomendável copiar o aide-md5 para um meio removível, protegido contra gravação, e uma vez que o sistema tenha entrado em produção, deve-se executá-lo sempre a partir daquele meio, eventualmente removendo o aide-md5 original do disco rígido. Pois, se você fizer uso do aide-md5 do disco rígido, e este for comprometido, o invasor pode forjar somatórios MD5 falsamente *perfeitos*.

Capítulo 9. Alta Disponibilidade

Introdução

Este capítulo descreverá os conceitos e a terminologia por trás da Alta Disponibilidade, bem como as aplicações e programas de sistema que objetivam aumentar a disponibilidade de servidores Linux, que são parte integrante do Conectiva Linux. Também pode ser usado como um manual para a configuração destas aplicações.

Definição

Para que se entenda a Alta Disponibilidade faz-se necessário, antes de mais nada, perceber que a Alta Disponibilidade não é apenas um produto ou uma aplicação que se instale, e sim uma característica de um sistema computacional. Existem mecanismos e técnicas, blocos básicos, que podem ser utilizados para aumentar a disponibilidade de um sistema. A simples utilização destes blocos, entretanto, não garante este aumento se não for acompanhado de um completo estudo e projeto de configuração.

A Disponibilidade de um sistema computacional, indicada por A(t), é a probabilidade de que este sistema esteja funcionando e pronto para uso em um dado

instante de tempo `t`. Esta disponibilidade pode ser enquadrada em três classes, de acordo com a faixa de valores desta probabilidade. As três classes são: Disponibilidade Básica, Alta Disponibilidade e Disponibilidade Contínua.

Disponibilidade Básica

A Disponibilidade Básica é aquela encontrada em máquinas comuns, sem nenhum mecanismo especial, em software ou hardware, que vise de alguma forma mascarar as eventuais falhas destas máquinas. Costuma-se dizer que máquinas nesta classe apresentam uma disponibilidade de 99% a 99,9%. Isto equivale a dizer que em um ano de operação a máquina pode ficar indisponível por um período de 9 horas a quatro dias. Estes dados são empíricos e os tempos não levam em consideração a possibilidade de paradas planejadas (que serão abordadas mais adiante), porém são aceitas como o senso comum na literatura da área.

Alta Disponibilidade

Adicionando-se mecanismos especializados de detecção, recuperação e mascaramento de falhas, pode-se aumentar a disponibilidade do sistema, de forma que este venha a se enquadrar na classe de Alta Disponibilidade. Nesta classe as máquinas tipicamente apresentam disponibilidade na faixa de 99,99% a 99,999%, podendo ficar indisponíveis por um período de pouco mais de 5 minutos até uma hora em um ano de operação. Aqui se encaixam grande parte das aplicações com-

erciais de Alta Disponibilidade, como centrais telefônicas.

Disponibilidade Contínua

Com a adição de noves se obtém uma disponibilidade cada vez mais próxima de 100%, diminuindo o tempo de inoperância do sistema de forma que este venha a ser desprezível ou mesmo inexistente. Chega-se então na Disponibilidade Contínua, o que significa que todas as paradas planejadas e não planejadas são mascaradas, e o sistema está sempre disponível.

Objetivos

Como já pode ser percebido de sua definição, o principal objetivo da Alta Disponibilidade é buscar uma forma de manter os serviços prestados por um sistema a outros elementos, mesmo que o sistema em si venha a se modificar internamente por causa de uma falha. Aí está implícito o conceito de mascaramento de falhas, através de redundância ou replicação (termos que serão conceituados mais tarde). Um determinado serviço, que se quer altamente disponível, é colocado por trás de uma camada de abstração, que permita mudanças em seus mecanismos internos mantendo intacta a interação com elementos externos.

Este é o coração da Alta Disponibilidade, a sub-área da Tolerância a Falhas, que

visa manter a disponibilidade dos serviços prestados por um sistema computacional, através da redundância de hardware e reconfiguração de software. Vários computadores juntos agindo como um só, cada um monitorando os outros e assumindo seus serviços caso perceba que algum deles falhou.

Outra possibilidade importante da Alta Disponibilidade é fazer isto com computadores simples, como os que se pode comprar até num supermercado. A complexidade pode estar apenas no software. Mais fácil de desenvolver que o hardware, o software de Alta Disponibilidade é quem se preocupa em monitorar outras máquinas de uma rede, saber que serviços estão sendo prestados, quem os está prestando, e o que fazer quando uma falha é percebida.

Cálculo da Disponibilidade

Em um sistema real, se um componente falha, ele é reparado ou substituído por um novo componente. Se este novo componente falha, é substituído por outro e assim por diante. O componente reparado é tido como no mesmo estado que um componente novo. Durante sua vida útil, um componente pode ser considerado como estando em um destes estados: *funcionando* ou *em reparo*. O estado *funcionando* indica que o componente está operacional e o estado *em reparo* significa que ele falhou e ainda não foi substituído por um novo componente.

Em caso de defeitos, o sistema vai de *funcionando* para *em reparo*, e quando a substituição é feita ele volta para o estado *funcionando*. Sendo assim, pode-se dizer que o sistema apresenta ao longo de sua vida um tempo médio até apresentar falha (MTTF) e um tempo médio de reparo (MTTR). Seu tempo de vida é uma

sucessão de MTTFs e MTTRs, à medida que vai falhando e sendo reparado. O tempo de vida útil do sistema é a soma dos MTTFs nos ciclos MTTF+MTTR já vividos.

De forma simplificada, diz-se que a disponibilidade de um sistema é a relação entre o tempo de vida útil deste sistema e seu tempo total de vida. Isto pode ser representado pela fórmula abaixo:

```
Disponibilidade = MTTF / (MTTF + MTTR)
```

Ao avaliar uma solução de Alta Disponibilidade, é importante levar em consideração se na medição do MTTF são observadas como falhas as possíveis paradas planejadas. Mais considerações sobre este assunto serão tecidas em seções posteriores.

Conceitos

Para se entender corretamente do que se está falando quando se discute uma solução de Alta Disponibilidade, deve-se conhecer os conceitos envolvidos. Não são muitos, porém estes termos são muitas vezes utilizados de forma errônea em literatura não especializada. Antes de mais nada, deve-se entender o que é falha, erro e defeito. Estas palavras, que parecem tão próximas, na verdade designam a ocorrência de algo anormal em três universos diferentes de um sistema computa-

cional.

Falha

Uma falha acontece no universo físico, ou seja, no nível mais baixo do hardware. Uma flutuação da fonte de alimentação, por exemplo, é uma falha. Uma interferência eletromagnética também. Estes são dois eventos indesejados, que acontecem no universo físico e afetam o funcionamento de um computador ou de partes dele.

Erro

A ocorrência de uma falha pode acarretar um erro, que é a representação da falha no universo informacional. Um computador trabalha com bits, cada um podendo conter 0 ou 1. Uma falha pode fazer com que um (ou mais de um) bit troque de valor inesperadamente, o que certamente afetará o funcionamento normal do computador. Uma falha, portanto, pode gerar um erro em alguma informação.

Defeito

Já esta informação errônea, se não for percebida e tratada, poderá gerar o que se conhece por defeito. O sistema simplesmente trava, ou mostra uma mensagem de erro, ou ainda perde os dados do usuário sem maiores avisos. Isto é pecebido no universo do usuário.

Recapitulando, uma falha no universo físico pode causar um erro no universo informacional, que por sua vez pode causar um defeito percebido no universo do usuário. A Tolerância a Falhas visa exatamente acabar com as falhas, ou tratá-las enquanto ainda são erros. Já a Alta Disponibilidade permite que máquinas travem ou errem, contanto que exista outra máquina para assumir seu lugar.

Para que uma máquina assuma o lugar de outra, é necessário que descubra de alguma forma que a outra falhou. Isso é feito através de testes periódicos, cujo período deve ser configurável, nos quais a máquina secundária testa não apenas se a outra está ativa, mas também fornecendo respostas adequadas a requisições de serviço. Um mecanismo de detecção equivocado pode causar instabilidade no sistema. Por serem periódicos, nota-se que existe um intervalo de tempo durante o qual o sistema pode estar indisponível sem que a outra máquina o perceba.

Failover

O processo no qual uma máquina assume os serviços de outra, quando esta última apresenta falha, é chamado failover. O failover pode ser automático ou man-

ual, sendo o automático o que normalmente se espera de uma solução de Alta Disponibilidade. Ainda assim, algumas aplicações não críticas podem suportar um tempo maior até a recuperação do serviço, e portanto podem utilizar failover manual[1]. Além do tempo entre a falha e a sua detecção, existe também o tempo entre a detecção e o reestabelecimento do serviço. Grandes bancos de dados, por exemplo, podem exigir um considerável período de tempo até que indexem suas tabelas, e durante este tempo o serviço ainda estará indisponível.

Para se executar o failover de um serviço, é necessário que as duas máquinas envolvidas possuam recursos equivalentes. Um recurso pode ser uma placa de rede, um disco rígido, ainda mais importante, os dados neste disco, e todo e qualquer elemento necessário à prestação de um determinado serviço. É vital que uma solução de Alta Disponibilidade mantenha recursos redundantes com o mesmo estado, de forma que o serviço possa ser retomado sem perdas.

Dependendo da natureza do serviço, executar um failover significa interromper as transações em andamento, perdendo-as, sendo necessário reiniciá-las após o failover. Em outros casos, significa apenas um retardo até que o serviço esteja novamente disponível. Nota-se que o failover pode ou não ser um processo transparente, dependendo da aplicação envolvida.

1. feito por um administrador ou operador

Failback

Ao ser percebida a falha de um servidor, além do failover é obviamente necessário que se faça manutenção no servidor falho. Ao ser recuperado de uma falha, este servidor será recolocado em serviço, e então se tem a opção de realizar o processo inverso do failover, que se chama failback. O failback é portanto o processo de retorno de um determinado serviço de uma outra máquina para sua máquiana de origem. Também pode ser automático, manual ou até mesmo indesejado. Em alguns casos, em função da possível nova interrupção na prestação de serviços, o failback pode não ser atraente.

Missão

Quando se calcula a disponibilidade de um sistema, é importante que se observe o conceito de missão. Missão de um sistema é o período de tempo no qual ele deve desempenhar suas funções sem interrupção. Por exemplo, uma farmácia, que funcione das 8h às 20h, não pode ter seu sistema fora do ar durante este período de tempo. Se este sistema vier a apresentar defeitos fora deste período, ainda que indesejados, estes defeitos não atrapalham em nada o andamento correto do sistema quando ele é necessário. Uma farmácia 24h obviamente tem uma missão contínua, de forma que qualquer tipo de parada deve ser mascarada.

A Alta Disponibilidade visa eliminar as paradas não planejadas. Porém, no caso da primeira farmácia, as paradas planejadas não devem acontecer dentro do período de missão. Paradas não planejadas decorrem de defeitos, já paradas planejadas

são aquelas que se devem a atualizações, manutenção preventiva e atividades correlatas. Desta forma, toda parada dentro do período de missão pode ser considerada uma falha no cálculo da disponibilidade.

Uma aplicação de Alta Disponibilidade pode ser projetada inclusive para suportar paradas planejadas, o que pode ser importante, por exemplo, para permitir a atualização de programas por problemas de segurança, sem que o serviço deixe de ser prestado.

A Solução Conectiva para Alta Disponibilidade

A Conectiva tem participado de projetos internacionais de Alta Disponibilidade, colaborando com a elaboração de diversos programas que suprem funcionalidades básicas na construção de ambientes de Alta Disponibilidade. O interesse em trabalhar na integração de diversas tecnologias e estendê-las individualmente vem do objetivo de prover uma solução simples e flexível, que possa ser otimimizada para as particularidades de cada aplicação. Todos estes projetos seguem a filosofia do Software Livre, assim como a solução apresentada pela Conectiva em seu Conectiva Linux.

Neste espírito, a solução é baseada em quatro blocos básicos, que são: replicação

de disco, monitoração de nodos, monitoração de serviços e sistema de arquivos robusto. Estes quatro blocos podem ser utilizados em conjunto ou individualmente, possibilitando a criação de soluções com failover e failback, automáticos ou manuais, com ou sem replicação de dados, e mesmo suportando paradas planejadas. Esta solução foi idealizada para um cluster de dois nodos.

Monitoração de nodos

A monitoração de nodos é realizada pelo heartbeat. Ele é o responsável por testar periodicamente os nodos do cluster, coordenando as ações de failover e failback. As soluções que utilizam reativação automática de serviços serão baseadas neste pacote. O heartbeat permite que se execute programas no processo de failover e failback, controlando qualquer recurso que se deseje.

Replicação de disco

A replicação de disco é de responsabilidade do DRBD, um driver de bloco para o kernel que cria um dispositivo de bloco[2] virtual, consistindo tanto de um disco real local quanto de uma conexão de rede, que terá na outra ponta outro driver DRBD atuando como secundário. Tudo aquilo que é escrito no dispositivo virtual

2. disco

é escrito no disco local e também enviado para o outro driver, que fará a mesma operação em seu disco local. Com isto se obtém dois nodos com discos exatamente iguais, até o instante da falha. As aplicações que trabalham com dados dinâmicos ou atualizados com muita freqüência se beneficiam deste driver.

Sistema de arquivos

Dados replicados ou não, é importante que o sistema de arquivos esteja consistente. Nem todos os sistemas de arquivos garantem isso, portanto para esta solução se escolheu trabalhar com o Reiser Filesystem[3]. Este sistema de arquivos trabalha com journal, o que significa que todas as alterações de dados são antes registradas no disco para que, caso o sistema venha a falhar durante este processo, a transação possa ser recuperada quando o sistema voltar. Isto confere agilidade ao processo de recuperação de falhas, bem como aumenta muito a confiabilidade das informações armazenadas.

Monitoração de serviços

A monitoração de serviços é feita através do Mon, um super escalonador de testes

3. ReiserFS

que pode verificar centenas de máquinas e serviços de forma rápida e ágil, enviando alertas para endereços de correio eletrônico, pagers ou telefones celulares, garantindo que os administradores dos serviços estejam sempre bem informados sobre seu estado de operação. Suporta dependências entre testes, portanto não perde tempo verificando se um servidor de HTTP está respondendo em uma máquina que sabe estar inoperante. Um alerta pode até mesmo tentar recuperar a situação automaticamente ou reiniciar uma máquina, caso a falha ocorra em um horário de difícil manutenção.

Configuração do DRBD

Tendo dois computadores, chamados aqui de `ha1` e `ha2`, efetue estas configurações de forma idêntica nos dois. Instale o pacote de utilitários do DRBD:

```
# rpm -ivh drbd*
drbd-utils        ##############################
drbdconf          ##############################
#
```

Configuração via Linuxconf

Abra o Linuxconf e acesse Configuração→Ambiente de Rede→Tarefas de servidor→Disp. DRBD→Adicionar. Observe a Figura 9-1.

Figura 9-1. Configuração do DRBD

No campo Nó: coloque o hostname do Master, e no campo Partição: a partição para o DRBD. Efetue estas configurações também para o Slave, através da orelha Configurando para Slave. Clicando em Aceitar surgirá o arquivo `drbd0`, Figura 9-2.

Figura 9-2. Arquivo de configuração

Clicando em Sair o módulo irá perguntar se você deseja reinicializar os serviços, clique em Sim.

Configuração pelo modo texto

No diretório `/etc/sysconfig/drbd` você encontrará o exemplo de um arquivo descritivo para um dispositivo DRBD, o `drdb.example`. Copie este arquivo com o nome de `/etc/sysconfig/drbd/drbd0`, e efetue as seguintes configurações:

```
# endereço do master e do slave end[:porta]
# porta padrão: 7788
# Importante: não use nomes de domínio aqui, apenas
```

```
# os hostnames da forma reportada pelo hostname -s
MASTER_NODE="ha1:7788"
SLAVE_NODE="ha2:7788"

# Aqui você poderá colocar um endereço IP específico das interfaces se
# for necessário. Caso seja utilizado, a definição de porta
# (7788, 7779, ...) deve estar aqui. Se não for utilizado, deve
# permanecer em branco (vazio "")  mas nunca comentado (#).
MASTER_IF=""
SLAVE_IF=""

OPTIONS=""

# Protocolo usado para este dispositivo o protocolo de confirmação
# pode ser A, B ou C.
PROTOCOL="B"

# Dispositivos usados no master e no slave (podem ser diferentes em
# cada máquina)
MASTER_DEVICE="/dev/nb0"
SLAVE_DEVICE="/dev/nb0"
```

```
# Partições para o drdb (pode ser uma partição diferente em cada
# máquina), elas devem ter um tamanho similar.
MASTER_PARTITION="/dev/hda6"
SLAVE_PARTITION="/dev/hda6"
```

Inicialize o DRBD:

```
# /etc/rc.d/init.d/drbd start
Loading DRBD module [ OK ]
Configuring DRBD resource drbd0                  [  OK  ]
Waiting for DRBD resource drbd0 to resynchronize [  OK  ]
#
```

Através do comando:

```
# /etc/rc.d/init.d/drbd status
version : 55

0: cs:WFConnection st:Secondary ns:0 nr:0 dw:0 dr:0 of:0
#
```

Você poderá verificar o estado do DRBD no sistema. Ou ainda verificar o arquivo `/var/log/messages` com o comando **# tm** e observar o que houve durante a inicialização do DRBD.

Monte a unidade através do script **datadisk** da seguinte forma:

```
# /etc/ha.d/resource.d/datadisk start
#
```

Não se pode montar simultaneamente a partição nos dois nodos.

Sistema de arquivos Reiserfs

Instale o pacote de utilitários do Reiserfs:

```
# rpm -ivh reiserfs-utils*
reiserfs-utils ############################### #
```

Inicie a partição com o comando:

```
# dd if=/dev/zero of=/dev/hda6
```

Crie um sistema de arquivos Linux Reiserfs utilizando o comando:

```
# mkreiserfs /dev/hda6



<-------MKREISERFS, 1999------->
ReiserFS version 3.5.21
Block size 4096 bytes
Block count 257032
First 16 blocks skipped
Super block is in 16
Bitmap blocks are :
    17, 32768, 65536, 98304, 131072, 163840, 196608, 229376
Journal size 8192 (blocks 18-8210 of device 0x3:0x6)
Root block 8211
Used 8219 blocks
Hash function "tea" ATTENTION: ALL DATA WILL BE LOST ON ’/dev/hda6’! (y/n)y
Initializing journal - 0%....20%....40%....60%....80%....100%
Syncing..
```

Configuração do Heartbeat

Instale o pacote do Heartbeat:

```
# rpm -ivh heartbeat*
heartbeat ##############################
heartbeatconf ##############################
#
```

Configuração pelo Linuxconf

As configurações do heartbeat podem ser feitas através do módulo *Configuração do heartbeat* do Linuxconf. Este módulo você encontrará acessando menu em Configuração→Ambiente de rede→Tarefas de servidor→Configuração do heartbeat. Veja a Figura 9-3.

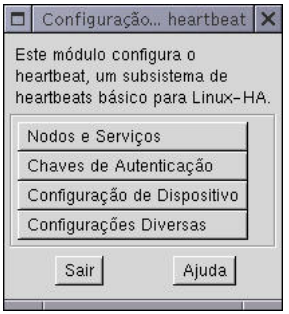


Figura 9-3. Configuração do Heartbeat

Em Nodos e Serviços clique em Adicionar e adicione um nome para o novo nodo, no nosso exemplo `ha1`. Clicando em aceitar surgirá o nodo que você adicionou, Figura 9-4.

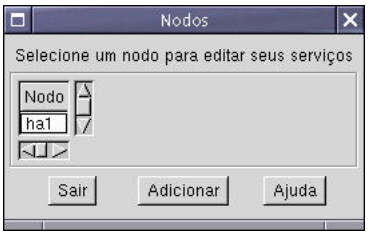


Figura 9-4. Nodos

Clique sobre o nome do nodo (ha1), surgirá a janela Editando nodo com o botão IPs e Serviços. Através deste botão escolha Adicionar e digite um IP[4] para este nodo e os recursos que devem ser monitorados, no campo Serviços. A Figura 9-5 contém um exemplo utilizando um IP para este nodo e alguns recursos separando-os por um espaço em branco.

Figura 9-5. IPs e Serviços

Vamos definir agora a chave de autenticação, clicando no botão Chaves de Autenticação da Figura 9-3, surgirá uma janela com três métodos de autenticação e um campo para definição de uma chave. Preencha de forma similar a Figura 9-6.

4. *virtual*

Figura 9-6. Chaves de Autenticação

Neste caso o método escolhido foi o md5 e a chave de autenticação `Olá!`.

Para configurar um dispositivo do tipo UDP, por exemplo, clique em Configuração de Dispositivo→Adicionar→udp. Digite um nome para o dispositivo, no nosso caso da Figura 9-7 digitamos no campo Nome do Dispositivo `eth0`.

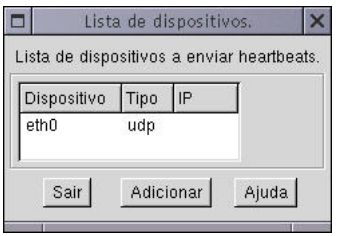


Figura 9-7. Lista de dispositivos

E por último faremos mais algumas configurações personalizadas através do botão

Configurações Diversas. Aqui configuramos nomes para arquivos de mensagens, implementação para o syslog, tempos opcionais em segundos e a porta UDP. Note que deixamos a opção Nice failback habilitada. Veja a figura de exemplo Figura 9-8.

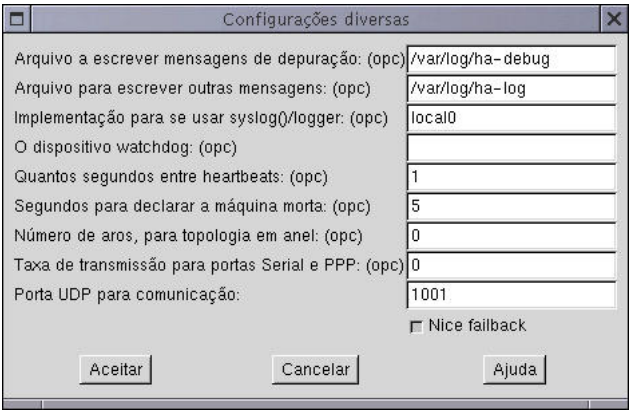


Figura 9-8. Configurações diversas

Mais detalhes sobre estas configurações poderão ser vistas à seguir, em configuração pelo modo texto.

Configuração pelo modo texto

Edite o arquivo `haresources`.

Este arquivo contém uma lista de recursos que são movidos de máquina para máquina conforme os nós caem e levantam no cluster. Não inclua endereços de IP fixos ou administrativos neste arquivo.

Exemplo para o arquivo `/etc/ha.d/haresources`:

```
#nome-do-nó endereço-IP-virtual recurso1 recurso2 ... recursoN
ha1 10.0.17.26 mysql httpd datadisk
```

Outro arquivo a ser modificado é o `ha.cf`, este arquivo tem muitas opções. Tudo o que você precisa é de uma lista de conjunto de nós (node ...) e uma lista interfaces.

Exemplo de configuração para o arquivo `/etc/ha.d/ha.cf`:

```
# keepalive: tempo em segundos entre heartbeats
keepalive 1

# deadtime: tempo em segundos para declarar o host caído
deadtime 5

# porta UDP usada para a comunicação udp
udpport 1001
```

```
# interface para o heartbeat, uma ou várias
udp eth0

# Se o cluster estiver executando quando o primário iniciar ele atuará
# como um secundário.
nice_failback on

# Arquivo para gravar mensagens de debug debugfile
/var/log/ha-debug

# Arquivo para escrever outras mensagens
logfile /var/log/ha-log

# facility usada para o syslog
logfacility local0

# Máquinas que estão no cluster nó nome-do-nó ... (nome obtido por
# uname -n).
node ha1
node ha2
```

O arquivo de autenticação deve estar no modo 600 (-rw——-), somente leitura e

escrita para o dono, escolha o método e a chave que irá com este identificador de método.

Exemplo para o arquivo `/etc/ha.d/authkeys`:

```
# Deve-se especificar apenas uma diretiva auth
# no início.
# auth método-de-autenticação
auth 3


# O método md5 é considerado o mais seguro para este caso.
3 md5 Olá!
```

Capítulo 10. Redes Mistas

Neste capítulo apresentaremos informações sobre instalação, configuração e manutenção de redes heterogêneas. Você poderá ver como fazer seu servidor Conectiva Linux agir como um servidor Windows® ou um servidor Netware®, fazendo com que estações não-Conectiva Linux possam ser utilizadas de maneira transparente. Além disso, você verá como fazer um servidor de arquivos. Você aprenderá como configurar suas máquinas clientes para acessar estes serviços.

NFS

Introdução e Conceitos

A maior vantagem do uso de redes de computadores é o compartilhamento de informações e recursos. Na verdade, este é o próprio propósito de se utilizar uma rede. O compartilhamento de informações pode ser feito de diversas maneiras, entre elas está o uso de FTP, web, etc.. Já o compartilhamento de recursos por vários computadores em uma rede, como discos, pode ser realizado através do NFS.

O NFS é um acrônimo para *Network File System*, ou, em português, Sistema

de Arquivos de Rede. O NFS foi criado para permitir o acesso transparente a discos remotos. Ele também permite uma maior centralização da administração de discos, pois é possível ter diretórios em uma única máquina (o servidor NFS) e compartilhados em todos os sistemas conectados à rede. Além disso, o NFS abre a possibilidade de existirem clientes sem disco.

Um esquema NFS bem configurado será totalmente transparente ao usuário. Não será relevante para o usuário saber em qual servidor um diretório realmente está. Basta que seus programas funcionem corretamente sem que ele tenha de realizar qualquer tipo de configuração especial.

Instalando o NFS

Instale o servidor NFS

1. Acesse o CD 1 do Conectiva Linux:

```
# cd /mnt/cdrom/conectiva/RPMS/
#
```

2. Instale os pacotes do NFS:

```
# rpm -ivh nfs-*
```

```
nfs-server ################################################
nfs-utils  ################################################
#
```

Configurando o Servidor NFS

A configuração de um servidor NFS é muito simples e pode ser feita tanto com o Linuxconf quanto através da edição de arquivos de configuração.

Na verdade, só o que você terá de fazer é definir os diretórios a serem exportados.

Para configurar o seu servidor, entre no Linuxconf e dirija-se ao menu Ambiente de Rede→Tarefas de Servidor→NFS para que a tela de configuração lhe seja mostrada tal como na Figura 10-1.

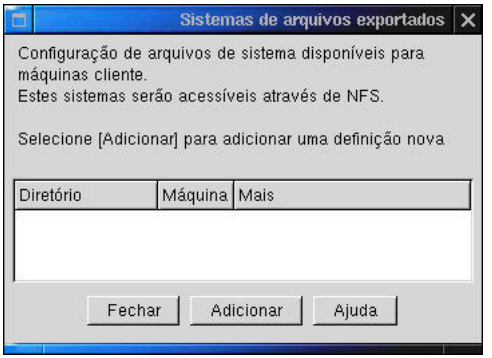


Figura 10-1. Tela de configuração do servidor NFS

Nesta tela você pode definir um caminho a ser exportado. As opções disponíveis são:

Rota para exportar: aqui você define o diretório a ser exportado. Este diretório poderá ser montado por um cliente.

Comentário: apenas um comentário ilustrativo. Pode ser usado para documentar alguma observação sobre o diretório.

Nome do cliente: neste campo você pode definir quais máquinas-clientes (separadas por vírgula) poderão acessar este diretório. Se nenhum cliente for especificado, então qualquer máquina poderá conectar-se. Você pode ainda utilizar coringas para definir as máquinas-clientes. Por exemplo, se você quer dar acesso a todas as máquinas de seu domínio, você pode especificar algo como: `*.minhaorganizacao.com.br`

Pode escrever: indica se o diretório será exportado apenas para leitura ou se será possível para os usuários gravarem nele.

Privilégios de superusuário: normalmente, o superusuário acessa diretórios remotos com privilégios de `nobody`. Você pode especificar esta opção para que o superusuário continue tendo acesso de superusuário quando acessar o diretório.

Seguir links simbólicos: quando esta opção está ativa, os links simbólicos absolutos (aqueles iniciados por /) são convertidos em links relativos, de forma a atingir a raiz do servidor.

Requisitar acesso da porta segura: você pode especificar que apenas conexões seguras (com número baixo de porta de origem) possam montar o diretório.

Como mencionado anteriormente, a configuração pode também ser feita através da edição de arquivos de configuração. Esta edição é bastante simples, envolvendo apenas a edição do arquivo `/etc/exports`.

O arquivo `/etc/exports` é bastante simples. Cada linha representa um diretório exportado e as informações são separadas por espaços. Por exemplo:

```
/share kepler(rw) copernico
```

Este exemplo exporta o diretório `/share` especificando duas máquinas (`kepler` e `copernico`) com opções diferentes (`kepler` pode gravar no diretório, enquanto que `copernico` só pode ler).

Tabela 10-1. Correspondência entre Opções do Linuxconf e do `/etc/exports`

`/etc/exports`	Linuxconf
rw	Marcar "pode escrever"
no_root_squash	Marcar "privilégios de superusuário"
link_relative	Marcar "seguir links simbólicos"
insecure	Desmarcar "requisitar acesso da porta segura"

Após feitas as configurações, você deve iniciar o serviço **nfs**. Para fazê-lo, é necessário abrir um terminal e digitar o comando (o serviço portmap já deverá estar rodando):

```
# /etc/rc.d/init.d/nfs start
Inicializando serviços NFS :            [ OK ]
Inicializando quotas (NFS)              [ OK ]
Inicializando mountd (NFS)              [ OK ]
Inicializando rpc.nfsd (NFS)            [ OK ]
```

Configurando um cliente NFS

É muito simples fazer uma máquina utilizar um disco remoto. Na verdade, não é necessário qualquer tipo de configuração para tornar uma máquina um cliente NFS. Você só precisa montar o diretório remoto da mesma maneira como monta um diretório local.

1. Antes de mais nada, crie um diretório na máquina local. Vamos montar o diretório remoto neste diretório local. Em nosso exemplo, montaremos o diretório `/usr/local` da máquina `asterix` dentro do diretório local `/mnt/asterix`

   ```
   # mkdir /mnt/asterix #
   ```

2. Agora monte o diretório remoto com o comando **mount**.

   ```
   # mount asterix:/usr/local /mnt/asterix
   #
   ```

   Feito isso, você poderá perceber que o conteúdo do diretório local `/mnt/asterix` é o mesmo do diretório `/usr/local` do servidor `asterix`.

É claro que, em muitos casos, você desejará que os diretórios remotos sejam automaticamente montados quando da inicialização da máquina-cliente. Para fazê-lo, você deve utilizar o Linuxconf e entrar em Sistemas de Arquivos→Acessar volumes NFS→Adicionar para que a tela de adição de volumes NFS lhe seja mostrada (Figura 10-2).

Figura 10-2. Tela de acesso a volumes NFS

Samba

O SMB é o protocolo utilizado em redes Windows® para compartilhamento de recursos, como impressoras e discos. É através do SMB que o Windows® permite que uma máquina acesse o disco e a impressora de outra na rede.

Com o crescimento do Linux, tornou-se necessário fazer com que máquinas Windows® e as redes Unix trabalhassem de maneira harmoniosa. Infelizmente, isso não era muito simples, já que as duas plataformas vinham de culturas muito diferentes e tinham dificuldades em trabalhar de maneira conjunta sem o auxílio do *Samba*.

O Samba, então, é uma implementação livre do protocolo SMB. Com o Samba será possível simular, de maneira transparente, um servidor Windows®. Isso torna possível o uso de estações Windows® em uma rede Conectiva Linux utilizando o protocolo NetBIOS.

Configurando o Servidor Samba

Figura 10-3. Configuração do Samba

A configuração de um servidor Samba é um tópico bastante abrangente. Tudo depende do tipo de serviços que você deseja executar.

Por exemplo, você deve decidir se deseja que o servidor Samba seja um controlador de domínio ou não.

Instalando o Samba

A instalação do Samba é simples:

1. Acesse o CD 1 da distribuição do Conectiva Linux:

```
# cd /mnt/cdrom/conectiva/RPMS
```

2. Instale o pacote do Samba:

```
# rpm -ivh samba-*
samba         ########################################
samba-clients ########################################
```

Configuração

Esta seção concentrar-se-á na configuração do Samba através do Linuxconf. Porém, existem outras maneiras de fazê-la, como através da edição do arquivo `/etc/smb.conf` e, ainda, através do SWAT. Cobriremos o SWAT no final desta seção. Os exemplos de configuração será sempre sobre o Linuxconf, não sendo necessária qualquer edição direta do arquivo `/etc/smb.conf`.

Senhas Criptografadas

O problema mais comum durante a instalação do Samba é relacionado com as senhas dos usuários.

A partir da versão 98, o Windows® começou a fazer a transmissão de senhas criptografadas pela rede NetBIOS. O Windows 95® e as versões iniciais do Windows NT®, porém, transmitiam sem encriptar as senhas. Essa falta de padronização entre estes sistemas torna a configuração do Samba um tanto mais complexa.

A encriptação de senhas visa proteger as mesmas de tentativas primitivas de descoberta. Infelizmente, os algoritmos de encriptação utilizados não são particularmente fortes.

Senhas Descriptografadas no Windows® 95

O padrão do Windows® 95 é não encriptar as senhas. Assim, é provável que esta configuração não seja necessária para você. Porém, versões mais recentes do Windows® 95 (como, por exemplo, o Windows® 95 OSR2) mudaram seu comportamento. Se você tiver problemas com senhas, siga o procedimento descrito nesta seção.

A configuração do Windows 95® pode ser feita de duas maneiras. Uma delas seria a utilização do arquivo `Win95_PlainPassword.reg` que acompanha o Samba. Este arquivo pode ser localizado no diretório `docs/` da documentação *on-line* do Samba:

```
# cd /usr/doc/samba*/docs
```

Você pode copiá-lo para as estações Windows 95®. Depois, basta abrir o arquivo (dar dois cliques sobre o mesmo) para que ele seja instalado.

Outra maneira de habilitar senhas é editar o registro através do utilitário **regedit** do Windows® para alterar ou incluir a chave:

```
[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\VxD\VNETSUP]
              "EnablePlainTextPassword"=dword:00000001
```

Senhas Descriptografadas no Windows® 98

Como padrão, o Windows® 98 encripta todas as senhas que trafegam pela rede. Para poder utilizar estações Windows® 98 com sua rede, siga o procedimento descrito nesta seção.

A configuração de senhas não encriptadas no Windows 98® pode ser feita de duas maneiras. Uma delas seria a utilização do arquivo `Win98_PlainPassword.reg` que acompanha o Samba. Este arquivo pode ser localizado no diretório `docs/` da documentação *on-line* do Samba:

```
# cd /usr/doc/samba*/docs
```

Você pode copiá-lo para as estações Windows 98®. Depois, basta abrir o arquivo (dar dois cliques sobre o mesmo) para que ele seja instalado.

Outra maneira de habilitar senhas é editar o registro através do utilitário **regedit** do Windows® para alterar ou incluir a chave:

```
[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\VxD\VNETSUP]
              "EnablePlainTextPassword"=dword:00000001
```

Senhas Descriptografadas no Windows NT®

O Windows® NT encripta senhas em algumas versões e não encripta em outras.

Notadamente, após o terceiro pacote de consertos (*Service Pack 3*, ou *SP3*), ele passou a encriptar todas as senhas trafegadas pela rede. Assim, recomenda-se seguir os procedimentos descritos nesta seção para assegurar que ele funcione como cliente de uma rede Samba. Além disso, recomendamos que você tenha, pelo menos, o Windows® NT SP3 instalado.

A configuração de senhas não encriptadas no Windows® 98 pode ser feita de duas maneiras. Uma delas seria a utilização do arquivo `NT4_PlainPassword.reg` que acompanha o Samba. Este arquivo pode ser localizado no diretório `docs/` da documentação *online* do Samba:

```
# cd /usr/doc/samba*/docs
```

Você pode copiá-lo para as estações Windows® NT. Depois, basta abrir o arquivo (dar dois cliques sobre o mesmo) para que ele seja instalado.

Outra maneira de habilitar senhas é editar o registro através do utilitário **regedit** do Windows® para alterar ou incluir a chave:

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Rdr\Parameters]

             "EnablePlainTextPassword"=dword:00000001
```

Configurações Básicas

Figura 10-4. Tela de configurações Globais do Samba

Uma das primeiras configurações que você provavelmente desejará fazer é definir o grupo de trabalho. Para isso, abra o Linuxconf e vá para as Tarefas de Servidor no Ambiente de Rede e entre em Samba para começar a configuração. Neste momento, você deve ver uma tela semelhante à Figura 10-3.

Clique em Padrões para configurar o grupo de trabalho.

No campo Grupo de Trabalho, digite o nome desejado.

Como o Windows® normalmente utiliza o método de segurança por recurso, você deve alterar o comportamento padrão do Samba, que é o de fazer a autenticação por usuário. Para fazer isso, apenas altere a opção Modo de Autenticação para Compartilhar. Esta opção pode ser encontrada na pasta Senhas.

Compartilhando um diretório

Nesta seção, vamos mostrar como compartilhar o diretório `/home/samba` para que o mesmo possa ser montado em uma estação Windows®.

1. Abra a caixa de diálogo Compartilhamento de Disco (Figura 10-5).

Compartilhando um diretório através do Samba

Figura 10-5. Compartilhamento de Discos

Note que estamos compartilhando o diretório `/home/samba`, com o nome de compartilhamento (aquele que aparecerá no Ambiente de Redes do Windows®) de "publico". Permitimos, também, que o usuário, qualquer usuário, possa gravar no diretório. Além disso, definimos que apenas máquinas em nosso domínio possam acessá-lo.

Para compartilhar um diretório, você só precisa especificar um nome de compartilhamento, o diretório a ser exportado e definir opções de acesso simples.

Montando um volume Samba

Você pode ter a necessidade de acessar um volume de uma máquina Windows® a partir do seu Conectiva Linux. Fazer isto não só é possível como é muito simples.

O processo deve ser feito através da linha de comando. Imaginando que você queira montar o disco `c:` da máquina `copernico`, que foi compartilhado com o nome `c`, em seu diretório Conectiva Linux `/mnt/copernico`:

```
# smbmount //copernico/c /mnt/copernico
#
```

Note que em alguns casos (você está montando um volume de um servidor Windows NT®, por exemplo), será necessário que você informe um usuário e uma senha para poder utilizar o comando **smbmount**.

```
# smbmount //copernico/c /mnt/copernico -o username=mara,password=selva
```

Isso funcionará se o usuário `mara` estiver cadastrado na máquina `jaguatirica` com a senha `selva`.

Iniciando o Samba

Para que o seu servidor Conectiva Linux possa funcionar como um servidor Samba, o serviço **smbd** deve ser inicializado. Para tanto, abra um terminal e digite:

```
# /etc/rc.d/init.d/smb start
Inicializando serviços SMB :                  [  OK  ]
Inicializando serviços NMB :                  [  OK  ]
```

Configuração do cliente

Esta seção descreve a configuração passo a passo de um cliente Windows® 98.

A instalação nas outras versões do Windows® deverá ter uma lista de passos semelhantes. Em caso de dúvidas, você deverá consultar a documentação do Windows® ao que se refere aos passos de instalação de uma rede ponto a ponto.

1. Instale normalmente a sua placa de rede conforme a documentação do Windows®. Você precisará do protocolo TCP/IP e do serviço **Cliente para Redes Microsoft**. Novamente, consulte a documentação do Windows® para informações sobre como instalar este serviço.

   Após a instalação, as propriedades da sua rede deverão se parecer com Figura 10-6.

   Figura 10-6. Propriedades da Rede Windows®

2. Clique na pasta Identificação na tela de configuração de redes e digite o nome de sua máquina e o nome do grupo de trabalho. Em nosso exemplo, a máquina se chamará `kepler` e fará parte do grupo de trabalho `minhaorganizacao`.

   Figura 10-7. Configuração da Identificação da Máquina

3. Clique na pasta Controle de Acesso e verifique que a tela está configurada como Figura 10-8.

Figura 10-8. Configurações do Controle de Acesso

4. Voltando para a tela de configuração de redes, abra a tela de propriedades do protocolo TCP/IP; clique em Configuração DNS e adicione o endereço IP do servidor Samba à lista de servidores DNS. Se já não o tiver feito, ative o DNS (opção Ativar DNS na mesma tela). Note que esta configuração somente se aplica a redes que possuem um servidor DNS. A tela de configuração do DNS é mostrada na Figura 10-9. Você deverá, também, editar a pasta Endereço IP, informando o endereço de IP a ser utilizado pela estação (se sua rede possuir um servidor DHCP, você não precisará desta configuração).

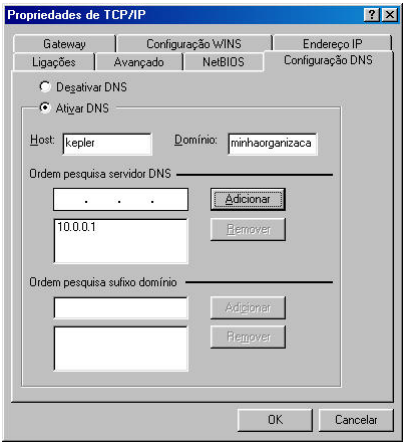


Figura 10-9. Configuração do DNS

5. Clique em OK e deixe a configuração de rede. O Windows® não pode ser configurado imediatamente e, assim, você terá de reiniciá-lo quando ele assim o solicitar.

Esses passos deverão permitir-lhe colocar uma estação Windows® 98 em sua rede Linux. Após a máquina ter reiniciado, você poderá abrir o Ambiente de rede para navegar pelas máquinas disponíveis na rede. A tela do Ambiente de rede de nosso exemplo se parecerá com a Figura 10-10.

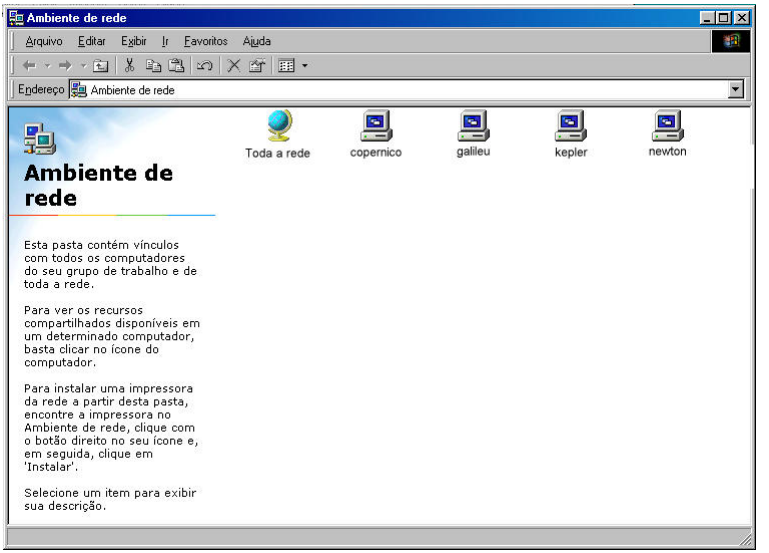


Figura 10-10. Ambiente de Rede

Utilizando o SWAT

Além do Linuxconf, é possível configurar o Samba através de uma outra interface amigável: o SWAT. O SWAT é uma interface *web* para a configuração. Uma grande vantagem do SWAT é a de que ele permite a configuração remota de um servidor Samba, já que só é necessário acessar a máquina pela Internet.

Para habilitar o SWAT a partir de seu servidor, é necessário editar o arquivo `/etc/inetd.conf` e descomentar (retirar o "#" inicial) da linha:

```
swat stream tcp nowait.400 root /usr/sbin/swat swat
```

que está, normalmente, no final do arquivo. Caso você não encontre uma linha semelhante, pode-se adicionar a linha acima.

Após feita a edição, o serviço **inetd** deve ser reiniciado:

```
killall -HUP inetd
```

ou ainda:

```
/etc/rc.d/init.d/inet restart
```

A diferença entre os dois comandos é que o segundo irá iniciar o serviço, caso não esteja iniciado.

A partir do momento em que o **inetd** for reiniciado, o SWAT será acessível através da porta 901 de seu servidor. Você pode acessar o SWAT http://localhost:901 através de qualquer navegador (veja Figura 10-11).

Figura 10-11. SWAT

Mars-NWE

O Mars-NWE é um emulador de Netware®, ou seja, é um programa que define um subconjunto do protocolo NCP da Novell®, de forma que estações o reconheçam como um servidor Netware®.

O Mars é uma boa opção ao Netware em redes em que há pelo menos um administrador com bom conhecimento de Linux. Além disso, empresas que iniciaram um processo de migração para Linux e possuem algumas estações DOS podem também utilizar o Mars-NWE.

Como o Mars-NWE é um emulador, alguns utilitários de configuração da Novell® não funcionam com ele e a sua configuração deve ser feita dentro do Linux.

Introdução e Conceitos

O protocolo IPX

O IPX é um protocolo de transporte[1]. O gerenciamento de sessão é realizado por outros protocolos. No caso do Netware®, este protocolo é o NCP.

Ao contrário do TCP/IP, no protocolo IPX não há a necessidade da especificação de números de rede, já que os mesmos são sempre os números identificadores da

1. Protocolo que se encarrega de transportar um pacote da rede de uma origem para um destino.

placa de rede[2].

Além disso, o protocolo IPX é roteável. Isso faz com que os servidores Netware®, inclusive o Mars-NWE, automaticamente desempenhem a função de roteadores, sempre que estiverem ligados a mais de uma rede. Estes servidores constantemente "anunciam-se" através de pacotes de *broadcast* de forma que é possível a criação de tabelas de roteamento dinâmicas.

O *Bindery*

É importante salientar que o Mars-NWE não honra a maioria dos objetos *bindery* do próprio servidor, como *trustees* e limitações de horário. Assim, as configurações de permissões devem ser feitas através do próprio Linux. Os únicos objetos *bindery* reconhecidos pelo Mars-NWE são as senhas dos usuários. De qualquer modo, todos os objetos *bindery* são armazenados no diretório `/var/mars_nwe`, sendo, assim, uma boa idéia manter cópias de segurança do mesmo. Existem planos para que outros objetos de *bindery* sejam suportados em versões futuras do Mars.

2. Número atribuído a cada placa na fábrica. Estes números de 48 *bits* jamais deveriam conflitar.

Scripts de *Logon*

Os *scripts* ficam armazenados no diretório SYS:MAIL\, tal como num servidor Netware®. Além disso, você será capaz de criar/alterar esses arquivos via **SYSCON**.

Às vezes o **SYSCON** não consegue gravar o *script* de *logon*; ele grava um arquivo LOGIN.BAK no diretório do usuário e não consegue renomeá-lo para LOGIN. Geralmente isso é problema de permissão em diretórios ou arquivos velhos (ou seja, arquivos copiados de um servidor Netware® pré-existente). Renomeie manualmente no Linux e atribua as permissões do usuário. É certo que isso não acontecerá uma segunda vez.

Se você estiver migrando do Netware® para o Mars, certamente vai montar o volume Netware® com **ncpmount** e copiar os dados para um diretório como, por exemplo, `/home/netware/sys`. É bom que, uma vez feita a cópia, você apague os subdiretórios do diretório SYS:MAIL. Se você não o fizer, ali ficarão os diretórios antigos, criados pelo servidor Netware®. E é certo que os números de usuário atribuídos pelo Netware® (que são justamente os nomes dos diretórios) não vão bater com os números criados pelo Mars; e você terá de ficar descobrindo "quem é quem" e atribuir as permissões corretas com **chown** e **chmod** etc.. Recomenda-se apagar tudo e iniciar o Mars de modo que todos os diretórios sejam criados automaticamente.

Autenticação de Usuários

Cada um dos usuários Netware® deve corresponder a um usuário Linux cadastrado

no arquivo `/etc/passwd`. Porém, a autenticação dos usuários do Mars não é feita através do arquivo `/etc/passwd` ou do `/etc/shadow`, mas sim através do arquivo `/etc/nwserv.conf`.

Como os *trustees* não são honrados pelo Mars, é necessário estabelecer as permissões no próprio Linux através dos comandos **chmod**, **chgrp** e **chown**.

Já vimos que o arquivo de configuração do Mars estabelece uma relação entre usuários Netware® e usuários UNIX. Os comandos citados acima trabalham apenas com usuários UNIX, portanto as permissões têm de ser "pensadas" em termos de usuários UNIX. É certo que se os usuários UNIX tiverem os mesmos nomes dos usuários Netware®, fica tudo mais fácil.

O usuário UNIX associado ao "supervisor" pode ser o root, ou um usuário comum. Se for um usuário comum, ele deve ter um grupo primário só seu, e também deve participar de todos os grupos onde haja usuários UNIX associados com usuários Netware®. Isso garante que o supervisor possa de fato ler e gravar qualquer arquivo dos volumes exportados.

Associar o root ao supervisor economiza bastante tempo. No entanto, se o servidor estiver num ambiente inseguro (exposto à Internet, ou com usuários desconhecidos, etc.) é melhor associar o supervisor a um usuário Unix comum.

Basicamente, os seguintes pontos têm de ser observados:

- Os diretórios e arquivos `SYS:SYSTEM`, `SYS:PUBLIC` e `SYS:LOGIN` devem ser possuídos por root:root, e com permissões de leitura para todo mundo;

- O diretório `SYS:MAIL` deve ser possuído por root:root (ou pelo usuário e grupo associado ao supervisor), mas com permissão de leitura para todos;

- Os demais diretórios e arquivos devem ser possuídos pelos respectivos usuários e grupos;

- As permissões de todos os diretórios devem ser 2775, se legíveis a todos os usuários, e 2770 se legíveis apenas aos usuários do grupo. O dígito "2" aciona o bit SGID do diretório; assim, quaisquer arquivos e diretórios novos criados dentro do diretório serão possuídos pelos usuários que os criaram, mas o grupo será sempre o mesmo do diretório-mãe. Assim, os demais usuários do grupo também terão acesso garantido aos novos arquivos e diretórios. Note que isso complementa a configuração das máscaras de permissão do arquivo `/etc/nwserv.conf`;

- O diretório-raiz de cada volume (como no arquivo-exemplo, o diretório `/home/netware/sys`) deve ter permissões 775 e ser possuído pelo usuário supervisor, salvo no caso de os usuários terem permissão de criar arquivos e diretórios na raiz do volume. Nesse caso as permissões devem ser 777;

- Os diretórios dentro de `MAIL/` devem ser possuídos pelos respectivos usuários e grupos. Os arquivos `LOGIN` podem ser possuídos pelo usuário ou ainda possuídos pelo root (neste último caso o arquivo está protegido contra tentativas de alteração que partam do próprio usuário). Note que o arquivo e o diretório precisam ser, ao menos, legíveis pelo usuário, assim como o diretório MAIL;

- Note que, se você deixou o Mars criá-los sozinho, as permissões dos diretórios sob `SYS:MAIL` já estarão todas corretas, sem necessidade de qualquer intervenção do usuário;

  Quando um usuário não tiver permissão de leitura a algum diretório, este lhe aparecerá vazio.

- Se, por exemplo, um usuário necessita ter acesso ao arquivo `VOLUME:DIR1\ARQUIVO`, ele precisará ter, pelo menos, acesso de leitura ao diretório-raiz de VOLUME, bem como a todos os diretórios do caminho. Se não puder ler o diretório, o usuário não enxergará subdiretórios e arquivos.

Utilitários DOS

Muitas operações (cadastro de usuários, senhas, etc.) podem ser feitas através do próprio Linux com os utilitários `/usr/bin/nw*`. Mas é certo que você precisará de um ou outro utilitário da Novell® (**IPX20**, **SYSCON**, **LOGIN**, **SLIST** etc.) Existem umas poucas versões gratuitas de alguns desses utilitários (**LOGIN** e **SLIST**), o que é insuficiente para uma rede com estações DOS. Será difícil manter uma rede Novell® totalmente livre de software comercial.

Se você tem um Netware® licenciado, simplesmente copie os diretórios `SYS:PUBLIC` e `SYS:SYSTEM` para o servidor Mars.

Note que este problema apenas se aplica ao caso de redes com estações DOS. Como as estações Windows® 95/98 incluem um cliente para redes Netware® que não depende de nenhum utilitário DOS, você será capaz de constituir uma rede totalmente livre de software comercial Netware® se todas as suas estações forem Windows®.

Se suas estações forem todas Linux, também não haverá necessidade dos utilitários DOS. Porém, não há necessidade do Mars-NWE em uma rede assim, já que é possível, e muito mais lógico, construir uma rede baseada em protocolo

TCP/IP.

Performance

Segundo o próprio autor do Mars, “a performance do Mars-NWE é ligeiramente inferior ao Netware® 3.12, no mesmo *hardware*, mas é superior ao Netware® 4”. Testes demonstraram que o Mars-NWE é mais rápido (10-15%) que o Netware® 3.12 para operações comuns em arquivos (leitura e gravação de pequenos trechos, etc.).

Porém, o Mars é cerca de 50% mais lento em operações de leitura/escrita de grandes trechos, como por exemplo um **COPY** do DOS. Essa performance pode ser melhorada através de um recurso chamado de *packet burst*, que está ainda em estado experimental. Para mais informações sobre como habilitar este recurso, vide a seção *Versão do Netware®*.

Problemas Conhecidos

Além do fato de que alguns procedimentos são um tanto complexos para quem está acostumado com Netware®, o Mars-NWE tem uma característica indesejável. Se um usuário abrir um arquivo em modo exclusivo, e depois tentar abrir novamente o mesmo arquivo, terá sucesso, enquanto o comportamento de um servidor Netware® seria negar quaisquer tentativas de reabertura.

Note que isso acontece apenas se o arquivo é aberto múltiplas vezes através da mesma conexão. Se um usuário entrar no sistema com o mesmo nome em diferentes estações, e tentar abrir um mesmo arquivo em modo exclusivo em todas elas, não terá sucesso a partir da segunda estação. O impacto desse bug do Mars varia em função dos programas utilizados.

Se os usuários costumam abrir múltiplas instâncias de um mesmo aplicativo, e esse aplicativo usa abertura de arquivos em modo exclusivo para garantir integridade de certas operações, pode haver problemas. Se você tiver problemas com isso, você pode proibir os usuários com estações Windows® de abrir múltiplas instâncias do mesmo aplicativo.

Um outro possível problema é que o Mars não vai carregar/executar suas NLMs. Uma extensão eventualmente encontrada em servidores Netware® 3 é o BTrieve®. Já existe BTrieve® para Linux, porém é um produto comercial.

Configuração

A configuração do Mars ainda não pode ser feita através do Linuxconf. Assim sendo, o processo de configuração de um servidor Mars deve ser realizado através da edição do arquivos de configuração `/etc/nwserv.conf`.

O arquivo `/etc/nwserv.conf` controla todo o comportamento de seu servidor Mars-NWE. Perceba que as opções são sempre precedidas por um número identificador. Este número é utilizado pelo Mars para reconhecer a função de cada linha.

Nesta seção, vamos mostrar-lhe como configurar as opções mais comuns (note que existem várias outras, mas que elas são pouco utilizadas). Você poderá encontrar informações sobre as mesmas no próprio arquivo `/etc/nwserv.conf` padrão que acompanha a instalação.

Volumes do Servidor

Você deve especificar quais serão os volumes do servidor Mars. Para especificar um volume do servidor, você deverá incluir uma linha para cada volume no arquivo de configuração. Esta linha tem a seguinte sintaxe:

```
1 VOLUME DIR_LINUX OPCOES MASC_DIR MASC_ARQ
```

onde:

VOLUME: nome do volume como será visto pelas estações.

DIR_LINUX: diretório do Conectiva Linux onde este volume será armazenado.

OPCOES: as opções são: **opção k**, que permite nomes em letras minúsculas no Conectiva Linux. Estes nomes serão automaticamente convertidos para letras maiúsculas para estações DOS. Se esta opção não for especificada, os nomes têm de ter letras maiúsculas no Conectiva Linux; **opção o:** especifica que os subdiretórios estão no mesmo sistema de arquivos. Isso permite ao Mars fazer algumas otimizações.

MASC_DIR: aqui você pode especificar as permissões padrão de diretórios. Novos diretórios serão criados com estas permissões.

MASC_ARQ: aqui você pode especificar as permissões padrão para arquivos. Todos os novos arquivos serão criados com estas permissões.

Não esqueça que a presença do volume SYS é obrigatória.

Exemplo:

```
1       SYS     /home/netware/sys       ko  775 775
1       FABRICA /home/netware/fabrica   ko  775 775
1       PESSOAL /home/netware/pessoal   ko  775 775
```

Nome do Servidor Netware®

Para definir o nome do servidor Netware®, basta incluir uma linha contendo o nome desejado:

```
2 NOME_SERVIDOR
```

Onde **NOME_SERVIDOR**

Exemplo:

```
2 FABRICA
```

Isso define o nome do servidor como sendo `FABRICA`.

Rede Interna

Você pode especificar o número de sua rede interna. Pode-se especificar a opção `auto`, para que o Mars escolha automaticamente o número da rede interna (ele simplesmente utiliza o número IP da interface de rede).

```
3 NUM_REDE
```

Onde **NUM_REDE** é o número da sua rede interna (opcionalmente, utilize `auto`).

Exemplo:

```
3 auto
```

Placas de Rede

Os parâmetros para a configuração das placas de rede são:

```
4 NUM_REDE INTERFACE PADRAO_PACOTE TEMPO
```

onde:

NUM_REDE: é o número da rede.

INTERFACE: é a *interface* de rede do Linux.

PADRAO_PACOTE: é o padrão de empacotamento utilizado pelo servidor. Este padrão pode ser `802.2`, `802.3`, `ethernet_ii`, `snap`, `token` ou `auto`. Obviamente, este padrão de empacotamento deve ser o mesmo utilizado pelas estações. O *boot* remoto do Netware® exige `802.3`.

TEMPO: é o tempo levado por uma pacote para ser transmitido pela *interface*. Para placas de rede, utilize sempre 1.

Todas as interfaces de rede devem ter números de IP, mesmo que o servidor não esteja servindo nenhum protocolo baseado em TCP/IP.

Exemplo:

```
4 0x01 eth0 802.3 1
```

Salvamento de Rotas

Como padrão, o Mars não salva as rotas quando é desativado. Assim, sempre que o Mars é ativado ele passa de 1 a 2 minutos procurando as mesmas. Isso pode ser modificado, fazendo com que o Mars salve as rotas no momento em que é

desativado.

```
5 SALVAR
```

Onde **SALVAR** é um valor numérico. "0" faz com que o Mars não salve as rotas "1" faz com que o Mars salve as rotas no momento da desativação, acelerando a inicialização posterior.

Exemplo:

```
5 0
```

Neste exemplo, o Mars está configurado para não salvar as rotas.

Versão do Netware®

Você pode indicar a versão do Netware® que o Mars vai aparentar ser. Isso é importante para alguns programas que só funcionam com versões específicas do Netware®.

```
6 VERSAO PACKET_BURST
```

Onde:

VERSAO: é um código especificando a versão do Netware®. Este código pode ser: 0

para Netware® 2.15, 1 para Netware® 3.11 e 2 para Netware® 3.12.

PACKET_BURST: é um código para habilitar ou desabilitar o *packet burst*. Este recurso ainda é experimental no Mars, mas é capaz de aumentar consideravelmente a performance do servidor. O código pode ser 0x1 para habilitar ou 0x0 para desabilitar o recurso.

Exemplo:

```
6 2 0x0
```

Isso define o servidor como Netware® 3.12 sem *packet burst.*

Tratamento de Senhas

Você pode definir como as senhas dos clientes DOS serão tratadas.

```
7 MODO
```

Onde **MODO** é um código que indica como tratar as senhas:

0: força a encriptação de todas as senhas.

1: força a encriptação de todas as senhas, mas suporta a rotina não encriptada de mudança de senha.

7: permite senhas não encriptadas, mas não permite senhas vazias.

8: permite senhas não encriptadas e senhas vazias.

9: permite apenas senhas não encriptadas.

Exemplo:

```
7 0
```

Define o comportamento padrão.

Segurança de Arquivos durante o Processo de *Login*

Existem muitas opções que controlam a parte de segurança dos arquivos durante a fase de *login*.

0: os clientes só podem acessar o diretório `SYS:LOGIN`. Esta é a opção padrão.

1: os clientes podem acessar outros arquivos além dos `SYS:LOGIN/*`, mas ainda sujeitos às permissões do Linux.

2: este modo permite acesso a arquivos da seguinte forma: se o cliente tenta abrir um arquivo para escrita, mas o mesmo é apenas leitura, o Mars permite a abertura, mas apenas para leitura.

4: permite que diretórios sejam renomeados através de uma chamada NCP que normalmente só funcionaria com arquivos.

8: ignorar restrições de estação e de tempo no caso do supervisor. Atualmente, esta opção não faz nada, já que o Mars ainda não suporta este tipo de objeto *bindery*.

16: permite que um arquivo em utilização por outro usuário seja apagado.

32: armazena entradas de arquivos para uso posterior. Normalmente, apenas os diretórios são armazenados. Isso é necessário caso você utilize ncpfs como cliente Mars.

64: limita o espaço livre alegado em 2GB. Isso é necessário para alguns clientes antigos do DOS.

```
8 MODO
```

Onde **MODO** é a soma dos códigos das opções desejadas.

Exemplo:

```
8 20
```

Isso define que diretórios podem ser renomeados via NCP (4) e que arquivos em uso podem ser apagados (16).

Usuário *Convidado*

Você deve especificar um usuário do Linux para corresponder ao usuário "convidado" (*guest*). Durante o processo de *boot* remoto e *login*, o servidor dará essa

permissão para o cliente, portanto é importante verificar que este usuário tenha acesso aos arquivos necessários (`SYS:LOGIN\LOGIN.exe` e `SYS:LOGIN\NET$DOS.SYS`)

```
10 UID 11 GID
```

Onde:

UID: é o número do usuário "convidado".

GID: é o número do grupo do usuário "convidado".

Você pode especificar o usuário:grupo `nobody:nobody` (99:99) para ser o usuário "convidado".

Exemplo:

```
10 99 11 99
```

Isso define o usuário `nobody:nobody` como usuário convidado.

Usuários com Poder de Supervisor

Você deve definir quais serão os usuários com poderes de supervisor.

```
12 USU_NW USU_LINUX SENHA
```

Onde:

USU_NW: é o nome do usuário "supervisor"no Netware®.

USU_LINUX: é a conta do usuário no Linux.

SENHA: é a senha do usuário no Linux. Note que é uma boa idéia mudar as permissões do arquivo `/etc/nwserv.conf` para 700 de forma que ninguém possa ler o arquivo e descobrir a senha do supervisor.

Exemplo:

```
12 SUPERVISOR root !92oi28#
```

Isso define que o usuário `root` será o supervisor e que sua senha é `!92oi28#`

Usuários do Netware®

Você pode cadastrar os usuários do Netware®. Há duas maneiras de se cadastrar as senhas dos mesmos: como parâmetro desta linha no arquivo de configuração ou através do **SYSCON**.

```
13
        USU_NW:USU_LINUX:[SENHA]
```

Onde:

USU_NW: é o nome do usuário no Netware®.

USU_LINUX: é o nome do usuário Linux associado.

SENHA: é a senha do usuário. Note que este parâmetro é opcional, já que a senha pode ser configurada pelo supervisor via **SYSCON**.

Se a senha for configurada através do **SYSCON**, o usuário pode alterar a senha temporariamente atribuída pelo administrador.

Um mesmo usuário Linux pode ser associado a vários usuários Netware®, facilitando a implementação da segurança.

Exemplo:

```
13 CLARA chefia
13 JORGE chefia
13 MARCIO producao
13 DEMERVAL demerval
```

Estas linhas cadastram alguns usuários. Note que `CLARA` e `JORGE` são mapeados para um mesmo usuário Linux (`chefia`).

Mapeamento Automático de Usuários

É possível mapear automaticamente os usuários Linux e os usuários do Netware®.

```
15 MAPEAMENTO_AUTOMATICO
```

Onde **MAPEAMENTO_AUTOMATICO** é 0 para desabilitar e 1 para habilitar o mapeamento automático de usuários.

Exemplo:

```
15 0
```

Desabilita o mapeamento automático. Note que desabilitar esta opção é altamente desaconselhável.

Criação dos Diretórios Essenciais

Com a opção 16, o Mars sempre testará a existência dos diretórios essenciais (`MAIL`, diretórios de usuários, etc..) e os criará, se houver necessidade.

```
16 TESTAR
```

Onde **TESTAR** é 0 para não testar e 1 para testar a existência dos arquivos (isso,

obviamente, implica na criação dos mesmos em caso de necessidade).

Script de *Login* Padrão

Existe um problema quando o **SYSCON** tenta gravar o primeiro *script* de *login*: ele não consegue fazê-lo. Se você habilitar essa opção, este problema estará resolvido e um *script* de *login* padrão (vazio) será criado.

```
17 CRIAR
```

Onde **CRIAR** é 0x0 para não criar, e 0x1 para criar.

Exemplo:

```
17 0x1
```

Esse exemplo instrui o Mars a sempre criar um *script* de *login* padrão, quando o usuário não possuir um.

Desligamento do *Banner* de Impressão

Com esta opção, você pode desligar a impressão do *banner* incondicionalmente. Isso é útil principalmente quando se está utilizando estações Windows 95® antigas, já que as mesmas não oferecem essa importantíssima opção.

```
18 BANNER
```

Onde **BANNER** é 0 para não imprimir, e 1 para permitir a impressão. Note que, se for especificado o valor 1, a impressão do *banner* ainda pode ser evitada através de opções do Netware®.

Exemplo:

```
18 0
```

Jamais imprimir o *banner* nas impressões.

Filas de Impressão

Você pode especificar as filas de impressão para utilização das estações. Cada fila ocupa uma linha:

```
21 NOME DIRETORIO COMANDO
```

Onde:

NOME: é o nome da fila de impressão do Netware®.

DIRETORIO: é o diretório onde as tarefas de impressão serão gravadas. Note que este diretório tem de existir e que ele não pode ser o diretório da fila do Linux (`/var/spool/lpd/*`).

Exemplo:

```
21 LASER   SYS:/PRINT/LP    lpr -P text
```

Neste mesmo guia vamos apresentar outro protocolo para trabalhar com redes mistas, veja no apêndice B.

Apêndice A. *Appletalk*

O Conectiva Linux oferece o pacote Netatalk em sua distribuição. Este pacote contém o protocolo *Appletalk*, que permite ao servidor Conectiva Linux servir impressoras e arquivos para estações Macintosh®.

Note que o caminho inverso não é possível, ou seja, o Macintosh não pode ser servidor de uma rede Linux. Isto depende da criação de um módulo do *kernel* que ainda está em seus estágios iniciais de desenvolvimento.

O Netatalk aceita conexões via protocolo *Ethertalk* e TCP/IP. Os computadores Macintosh mais novos privilegiam o TCP/IP como protocolo de transporte.

O pacote Netatalk consiste de 3 serviços que atuam em conjunto, embora possam ser ativados e desativados independentemente:

- **atalkd:** serve o *Appletalk* via *Ethertalk*;
- **afpd:** serve o *Appletalk* via TCP/IP;
- **papd:** intermedia os serviços de impressão para os outros dois serviços.

Se você não compartilhar impressoras e nem necessitar do *Ethertalk*, pode iniciar apenas o afpd e, assim, economizar um pouco de memória.

Instalando o Netatalk

Para instalar o Netatalk:

- Acesse o diretório de pacotes do CD 1 do Conectiva Linux

```
# cd /mnt/cdrom/conectiva/RPMS
```

- Instale os pacotes do Netatalk:

```
# rpm -ivh netatalk-*
netatalk       ##########################################
netatalk-devel ##########################################
```

Configurando o Netatalk

O Netatalk do Conectiva Linux já vem pré-configurado para as aplicações simples. Tudo o que você tem de fazer é especificar os diretórios a serem exportados como volumes para as estações Macintosh.

O Netatalk concentra todos os seus arquivos de configuração no diretório `/etc/atalk`.

Exportando Diretórios

Para especificar quais diretórios serão exportados como volumes para os clientes Macintosh, você deve editar o arquivo `/etc/atalk/AppleVolumes.default` e adicionar as linhas correspondentes aos diretórios.

As linhas de `/etc/atalk/AppleVolumes.default` tem o seguinte formato:

```
PATH [NOME] [casefold=X] [codepage=X] [options=X,Y,Z] \
     [access=X,@Y,Z] [dbpath=X] [password=X]
```

Onde:

- **NOME:** é uma descrição do volume;
- **casefold:** são opções de caixa do texto dos nomes de arquivos e diretórios. Pode ser:
  - **tolower:** converte as letras para minúsculas no servidor e nos clientes;
  - **toupper:** converte as letras para maiúsculas no servidor e nos clientes;
  - **xlatelower:** converte para minúsculas no cliente e para maiúsculas;
  - **xlateupper:** converte para maiúsculas no cliente e para maiúsculas.

- **codepage:** indica a página de códigos a ser utilizada. O parâmetro é o nome de um arquivo do diretório `nls`;
- **options:** são opções diversas divididas por vírgulas. Pode ser qualquer combinação de:
  - **prodos:** permite compatibilidade com clientes AppleII®;
  - **crlf:** habilita a conversão dos caracteres de nova linha dos arquivos textos entre os dois ambientes;
  - **noadouble:** não cria os arquivos .AppleDouble a não ser que uma divisão dos recursos se faça necessária. Os arquivos .AppleDouble são arquivos criados para cada arquivo em um diretório. O Macintosh guarda informações como ícone, tipo de arquivo, etc, nestes arquivos. Isoladamente eles são bastante pequenos (589 *bytes*), mas podem ocupar bastante espaço devido ao grande número de arquivos gerados.

- **access:** é uma lista de nomes de usuários e/ou grupos que não podem acessar o volume. Os grupos devem ser precedidos por uma arroba ("@");
- **dbpath:** diretório onde o banco de dados será gravado;
- **password:** é uma senha para proteger o diretório.

Configurando Permissões de Acesso

Usuários

Para acessar o servidor Netatalk, o cliente Macintosh deve fornecer um nome de usuário e uma senha, que deve estar cadastrados no servidor Conectiva Linux.

Você pode criar um usuário único que será utilizado por todas as estações Macintosh ao mesmo tempo. Embora isso facilite a administração, prejudica a segurança já que qualquer usuário terá acesso total aos arquivos dos outros.

Permissões no Diretório dos Volumes

Os usuários precisam ter permissão de escrita nos diretórios dos volumes que forem acessar via *Appletalk*.

Isso porque o Netatalk precisa guardar ali algumas informações referentes ao cliente Macintosh. Além disso, será criada nestes diretórios as suas respectivas "Lixeiras".

Como a criação de um diretório com todas as permissões para todos os usuários não é algo desejável no servidor Conectiva Linux, você pode criar um grupo `atalk`, colocar os usuários do Macintosh neste grupo e somente permitir escrita

aos arquivos aos membros deste grupo.

Na Estação

Para acessar os volumes, utilize o *Network Browser*. Expanda a seção *AppleTalk*. Se estiver tudo configurado de acordo, o nome do servidor Conectiva Linux já deve aparecer na lista.

Expanda o servidor Conectiva Linux para visualizar os volumes exportados. Nesse instante, o MacOS® solicitará um nome de usuário e uma senha, que você já deverá ter cadastrado no Conectiva Linux.

Clicando-se duas vezes sobre qualquer volume, uma nova janela será aberta, mostrando os arquivos e diretórios do volume em forma de ícones ou em forma de lista.

Se você clicar duas vezes em um volume e seu conteúdo não for mostrado, isso é sintoma de falta de permissões (vide a a seção *Configurando Permissões de Acesso*). Por outro lado, se você consegue acessar o volume, mas tiver permissões insuficientes para manipular determinado arquivo, o MacOS® notificar-lhe-á explicitamente do problema.

O MacOS® tem a característica indesejável de manter em *cache* as permissões negativas. Ou seja, ele continuará reportando falha de acesso mesmo que as permissões tenham sido modificadas no Conectiva Linux. Você terá de forçar o MacOS® desconectar-se do servidor Linux de alguma forma - seja resetando o Mac,

reiniciando o serviço Netatalk, ou quebrando a conexão TCP/IP.

Inicializando o Netatalk

Para inicializar o Netatalk:

```
# cds
atalk   dhcpd      httpd     kudzu            mysql    nfs      postgresql
atd     functions  inet      linuxconf-setup  named    nfslock  random
autofs  gpm        keytable  lpd              netfs    pcmcia   sendmail
crond   halt       killall   mars-nwe         network  portmap  single
# ./atalk start
Starting AppleTalk Services:                   [  OK  ]
Starting papd service:                         [  OK  ]
Starting afpd service:                         [  OK  ]
```

Você pode utilizar o ntsysv para configurar estes serviços para serem inicializados automaticamente.

Apêndice B. Licenças Gerais

Introdução

Praticamente todos os softwares contidos no CD-ROM do Conectiva Linux são de livre distribuição. Poucos requerem algum tipo de autorização especial para utilização, obtidos pela Conectiva S.A. (http://www.conectiva.com.br) e alguns softwares desenvolvidos pela própria Conectiva são disponibilizados sob licença comercial de uso.

A maioria dos softwares é distribuída sob uma das três licenças apresentadas neste capítulo. Por favor verifique em cada software quais são os seus componentes e quais os termos de sua distribuição.

Todos os softwares no CD-ROM produzido pela são copyright da ® Conectiva S.A. (http://www.conectiva.com.br). A menos que exista manifestação expressa, os softwares contidos no CD são de livre distribuição sob a Licença Pública GNU (GPL).

Os termos Red Hat® e rpm®são marcas de propriedade da *Red Hat Software, Inc*. Os termos Conectiva e WebBatch são marcas de propriedade da Conectiva S.A. (http://www.conectiva.com.br).

O BSD Copyright

Copyright ® 1991, 1992, 1993, 1994 The Regents of the University of California. Todos os direitos reservados.

Redistribuição e uso nas formas de código-fonte ou binários, com ou sem modificação são permitidos dentro das seguintes condições:

1. A redistribuição do software deve conter todas as informações sobre direitos autorais, esta lista de condições e o aviso abaixo;

2. A redistribuição de binários ou executáveis deve conter todas as informações sobre direitos autorais, listas de condições e o aviso abaixo, na documentação e/ou em outros materiais constantes da distribuição;

3. Todos os comerciais e anúncios mencionando funcionalidades deste software devem apresentar o seguinte texto: **Este produto inclui software desenvolvido pela Universidade da Califórnia, Berkeley e seus contribuintes**;

4. O nome da Universidade ou de seus contribuintes não pode ser utilizado para endossar ou promover produtos derivados deste software sem expressa autorização por escrito.

ESTE SOFTWARE É DISTRIBUÍDO POR SEUS MONITORES E CONTRIBUINTES NA FORMA EM QUE SE ENCONTRA, E QUALQUER GARANTIA EXPRESSA OU IMPLÍCITA, INCLUINDO, MAS NÃO LIMITADAS, ÀS GARANTIAS COMERCIAIS E ATENDIMENTO DE DETERMINADOS PROPÓSITOS, NÃO SÃO RECONHECIDAS. EM NENHUMA

HIPÓTESE OS MONITORES OU SEUS CONTRIBUINTES SERÃO RESPONSÁVEIS POR QUALQUER DANO DIRETO, INDIRETO, ACIDENTAL, ESPECIAL, INCLUINDO, MAS NÃO LIMITADO, À SUBSTITUIÇÃO DE MERCADORIAS OU SERVIÇOS, IMPOSSIBILIDADE DE USO, PERDA DE DADOS, LUCROS CESSANTES OU INTERRUPÇÃO DE ATIVIDADES COMERCIAIS, CAUSADOS EM QUALQUER BASE PELO USO DESTE SOFTWARE.

X Copyright

Copyright® 1987 X Consortium

É concedida e garantida a qualquer pessoa, livre de custos, a obtenção de cópia deste software e dos arquivos de documentação associados (o Software), podendo lidar com o Software sem restrições, incluindo os direitos de uso, cópia, modificação, unificação, publicação, distribuição, sublicenciamento e/ou venda de cópias do Software, e a permissão para as pessoas às quais o Software for fornecido, dentro das seguintes condições:

As informações de direitos autorais a seguir devem estar presentes em todas as cópias ou partes substanciais do Software:

O SOFTWARE SERÁ DISPONIBILIZADO NA FORMA EM QUE SE ENCONTRA, SEM GARANTIAS DE QUALQUER ESPÉCIE, EXPRESSAS OU ÍMPLICITAS, INCLUÍDAS, MAS NÃO LIMITADAS, ÀS GARANTIAS

COMERCIAIS, O ATENDIMENTO A DETERMINADOS FINS E O ATENDIMENTO DE DETERMINADA FUNCIONALIDADE. DE FORMA ALGUMA O CONSÓRCIO X (X CONSORTIUM) SERÁ RESPONSÁVEL POR QUALQUER RECLAMAÇÃO, DANO OU OUTRAS PERDAS, A MENOS QUE EXPRESSO EM CONTRATO, ACORDO OU OUTRAS FORMAS, NO QUE SE REFERE A UTILIZAÇÃO, COMERCIALIZAÇÃO, CONEXÃO OU OUTROS CONTATOS COM ESTE SOFTWARE.

Exceto pelo contido nesse aviso, o nome do Consórcio X (X Consortium) não poderá ser utilizado em qualquer comercial ou outra forma de promoção de vendas, uso ou outras negociações deste Software, sem a expressa autorização do X Consortium.

Copyright ® 1987 Digital Equipment Corporation, Maynard, Massachusetts. Todos os direitos reservados.

Permissão de uso, cópia, modificação e distribuição deste software e sua documentação com qualquer objetivo e sem ônus é garantida, desde que o copyright abaixo apareça em todas as cópias e que tanto o copyright, como este aviso e o nome da Digital apareçam, não podendo ser usados em anúncios, publicidade referentes à distribuição do software sem autorização expressa por escrito.

A DIGITAL NÃO FORNECE QUALQUER TIPO DE GARANTIA NO USO DESTE SOFTWARE, INCLUINDO TODAS AS COMERCIAIS E DE ATENDIMENTO A DETERMINADOS PROPÓSITOS, E EM HIPÓTESE ALGUMA A DIGITAL SERÁ RESPONSÁVEL POR QUALQUER RECLAMAÇÃO, DANO OU OUTRAS PERDAS, A MENOS QUE EXPRESSO EM CONTRATO, ACORDO OU OUTRAS FORMAS, NA UTILIZAÇÃO, COMERCIALIZAÇÃO, CONEXÃO OU OUTROS CONTATOS COM ESTE SOFT-

WARE.

Apêndice C. Licença de Uso e Garantia de Produto

Por favor leia este documento cuidadosamente antes de instalar o Conectiva Linux, ou qualquer um de seus pacotes, ou qualquer programa incluído com este produto em seu computador. Este documento contém informações importantes sobre seus direitos legais. Nós fortemente lhe encorajamos a considerar os pontos apresentados aqui, e a entender e aceitar os termos e condições pelos quais este programa está licenciado a você. Instalando qualquer programa incluído com este produto, você aceita os termos e condições a seguir.

Geral

O Sistema Operacional Conectiva Linux tem seu direito autoral baseado na Licença Pública Geral GNU (“GPL”). Nós acreditamos que a GPL disponibiliza os melhores mecanismos para todos os benefícios e liberdades disponibilizados pelos programas de “livre distribuição”. Uma cópia da GPL pode ser encontrada no manual de instalação do Conectiva Linux, em http://www.conectiva.com.br e em diversos sites na Internet. O Conectiva Linux é um sistema operacional modular feito de centenas de outros programas componentes, cada um destes escrito por pessoas diferentes e com seu próprio direito autoral. Neste documento eles são

referenciados, individualmente e coletivamente, como “Programas”. Vários Programas têm seu direito autoral baseados na GPL e outras licenças que permitem a cópia, modificação e redistribuição. Por favor, verifique a documentação online que acompanha cada um dos Programas inclusos no Conectiva Linux para verificar sua licença específica. Nós sugerimos ler estas licenças cuidadosamente para entender seus direitos e utilizar melhor os benefícios disponibilizados pelo Conectiva Linux.

Licença Restrita de Produtos

Adicionalmente aos Programas de livre distribuição, a Conectiva pode incluir neste produto diversos Programas que não estão sujeitos a GPL ou outras licenças que permitem modificação e redistribuição. Alguns destes programas estão citados abaixo:

- AcrobatReader®
- AcuCobol-4.3®
- Aker®
- Arkeia®

- BR®
- Dataflex®
- Domino®
- FlagShip®
- JRE®
- Jade®
- MZS®
- Oracle8i®
- SpoolBiew®
- db2®
- oss®
- vmware®
- xni®

e diversas aplicações do CD aplicativos comerciais. Geralmente, cada um destes componentes é licenciado a você unicamente em sua forma binária de maneira re-

strita, ou seja, você poderá instalar estes componentes em um único computador para seu uso individual. A cópia, redistribuição, engenharia reversa e/ou modificação destes componentes é proibida. Qualquer violação dos termos das licenças, imediatamente cancela sua licença. Para saber os termos precisos das licenças destes componentes, por favor, verifique a documentação on-line que acompanha cada um destes componentes. Se você não concorda em aceitar os termos da licença destes componentes, então não os instale em seu computador. Se você gostaria de instalar estes componentes em mais que um computador, por favor, contate o distribuidor dos programas para adquirir licenças adicionais.

Antes da Instalação

LEIA ATENTAMENTE OS TERMOS E CONDIÇÕES A SEGUIR ANTES DE INSTALAR O CONECTIVA LINUX OU QUALQUER UM DOS PROGRAMAS INCLUÍDOS COM ELE. INSTALAR QUALQUER UM DESTES PROGRAMAS INDICA SUA ACEITAÇÃO AOS TERMOS E CONDIÇÕES A SEGUIR. SE VOCÊ NÃO CONCORDA COM ESTES TERMOS E CONDIÇÕES NÃO INSTALE ESTES PROGRAMAS.

OS PROGRAMAS, INCLUINDO OS CÓDIGOS-FONTE, DOCUMENTAÇÃO, APARÊNCIA, ESTRUTURA E ORGANIZAÇÃO, SÃO PRODUTOS PROPRIETÁRIOS DA CONECTIVA S.A.; INC; ORACLE, SUN E OUTROS E SÃO PROTEGIDOS PELO DIREITO AUTORAL E OUTRAS LEIS. ESTES PROGRAMAS E QUALQUER CÓPIA, MODIFICAÇÃO OU PARTE ORIGINADA

DESTES PROGRAMAS, DEVEM A QUALQUER TEMPO PERMANECER COM OS ACIMA MENCIONADOS, SUBMETIDOS AOS TERMOS E CONDIÇÕES DA GPL OU OUTRA LICENÇA RELACIONADA COM OS PROGRAMAS EM CONSIDERAÇÃO.

Garantia Limitada

EXCETO SE ESPECIFICAMENTE DITO NESTE ACORDO, OS PROGRAMAS SÃO DISPONIBILIZADOS E LICENCIADOS “COMO ESTÃO”, SEM GARANTIA DE QUALQUER TIPO SEJA ELA EXPRESSA OU IMPLÍCITA, INCLUINDO, MAS NÃO LIMITADA, PARA AS GARANTIAS DE COMERCIALIZAÇÃO E CONVENIÊNCIA PARA UM PROPÓSITO PARTICULAR.

A Conectiva S.A. (http://www.conectiva.com.br) garante que a mídia na qual os Programas estão gravados é livre de defeitos de fabricação e manufatura sob uso normal durante um período de 30 dias da data da compra. A Conectiva S.A. (http://www.conectiva.com.br)& não garante que as funções contidas nos Programas serão compatíveis com os requisitos que você espera delas ou que a operação dos Programas será inteiramente livre de erros ou aparecerão precisamente como descritos na documentação que acompanha o produto.

Limitação de Reparação e Responsabilidade

Pelo máximo permitido pelas leis aplicáveis, as reparações descritas a seguir são aceitas por você como únicas, e devem ser disponíveis somente se você registrou este produto com a Conectiva S.A., de acordo com as instruções disponibilizadas com este produto, até dez dias depois de ter recebido o mesmo. A inteira responsabilidade da Conectiva S.A. (http://www.conectiva.com.br), e sua reparação exclusiva, devem ser: se a mídia que disponibiliza os Programas estiver com defeito, você pode retorná-la dentro de 30 dias da data da compra, juntamente com uma cópia da nota fiscal e a Conectiva S.A. (http://www.conectiva.com.br), a seu critério, irá trocá-la ou proceder a devolução do dinheiro.

PELO MÁXIMO PERMITIDO PELAS LEIS APLICÁVEIS, EM NENHUM EVENTO OU MOMENTO A CONECTIVA S.A. SERÁ RESPONSÁVEL POR QUALQUER DANO, INCLUINDO LUCROS CESSANTES, PERDAS ECONÔMICAS OU OUTROS DANOS ACIDENTAIS OU DANOS CONSEQÜENTES, PELO USO OU INAPTIDÃO PARA O USO DOS PROGRAMAS, MESMO QUE A CONECTIVA S.A. OU QUALQUER DISTRIBUIDOR AUTORIZADO NÃO TENHA ADVERTIDO ESTES TIPOS DE PROBLEMAS.

Bug do Ano 2000

O Conectiva Linux tem sido testado desde seu início para trabalhar sem problemas no Ano 2000 bem como depois dele. A certificação para o bug do Ano 2000 refere-se mais sobre testes, boas práticas e a educação do usuário do que a garantia do produto. Nós continuaremos a disponibilizar informações detalhadas aos clientes sobre a compatibilidade com o Ano 2000, mas garantias contratuais específicas para o problema do Ano 2000 não são apropriadas dada a natureza do bug do Ano 2000 e pelo simples fato que uma única tecnologia, mesmo uma bem preparada para o Ano 2000 como o Conectiva Linux, não pode resolver todos os itens relacionados à transição para o Ano 2000. A informação que disponibilizamos sobre a compatibilidade com o Ano 2000 não constitui uma extensão à qualquer garantia para os produtos da Conectiva. A Conectiva S.A. (http://www.conectiva.com.br) disponibiliza esta informação para assistir você na avaliação e correção de potenciais conseqüências do uso de datas para o próximo século.

Geral

Se qualquer cláusula deste Acordo for considerada inválida, as outras cláusulas não deverão ser afetadas pela mesma. Este Acordo deve ser legislado pelas leis Brasileiras.

direitos reservados. Conectiva e Conectiva Linux são marcas registradas da Conectiva S.A. (http://www.conectiva.com.br). Linux é uma marca registrada de Linus Torvalds em diversos países.

Apêndice D. Licença Pública Geral GNU

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

This is an unofficial translation of the GNU General Public License into Portuguese. It was not published by the Free Software Foundation, and does not legally state the distribution terms for software that uses the GNU GPL – only the original English text of the GNU GPL does that. However, we hope that this translation will help Portuguese speakers understand the GNU GPL better.

Introdução

As licenças de muitos softwares são desenvolvidas para cercear a liberdade de uso, compartilhamento e mudanças. A GNU Licença Pública Geral, ao contrário,

pretende garantir a liberdade de compartilhar e alterar softwares de livre distribuição - tornando-os de livre distribuição também para quaisquer usuários. A Licença Pública Geral aplica-se à maioria dos softwares da Free Software Foundation e a qualquer autor que esteja de acordo com suas normas em utilizá-la (alguns softwares da FSF são cobertos pela GNU Library General Public License).

Quando nos referimos a softwares de livre distribuição, referimo-nos à liberdade e não ao preço. Nossa Licença Pública Geral foi criada para garantir a liberdade de distribuição de cópias de softwares de livre distribuição (e cobrar por isso caso seja do interesse do distribuidor), o qual recebeu os códigos-fonte, que pode ser alterado ou utilizado em parte em novos programas.

Para assegurar os direitos dos desenvolvedores, algumas restrições são feitas, proibindo a todas as pessoas a negação desses direitos ou a solicitação de sua abdicação. Essas restrições aplicam-se ainda a certas responsabilidades sobre a distribuição ou modificação do software.

Por exemplo, ao se distribuir cópias de determinado programa, por uma taxa determinada ou gratuitamente, deve-se informar sobre todos os direitos incidentes sobre aquele programa, assegurando-se que os fontes estejam disponíveis assim como a Licença Pública Geral GNU.

A proteção dos direitos envolve dois passos: (1) copyright do software e (2) licença que dá permissão legal para cópia, distribuição e/ou modificação do software.

Ainda para a proteção da FSF e do autor, é importante que todos entendam que não há garantias para softwares de livre distribuição. Caso o software seja modificado por alguém e passado adiante, este software não mais refletirá o trabalho original do autor não podendo portanto ser garantido por aquele.

Finalmente, qualquer programa de livre distribuição é constantemente ameaçado pelas patentes de softwares. Buscamos evitar o perigo de que distribuidores destes programas obtenham patentes individuais, tornado-se seus donos efetivos. Para evitar isso foram feitas declarações expressas de que qualquer solicitação de patente deve ser feita permitindo o uso por qualquer indivíduo, sem a necessidade de licença de uso.

Os termos e condições precisas para cópia, distribuição e modificação seguem abaixo.

Termos e Condições para Cópia, Distribuição e Modificação

1. Esta licença se aplica a qualquer programa ou outro trabalho que contenha um aviso colocado pelo detentor dos direitos autorais dizendo que aquele poderá ser distribuído nas condições da Licença Pública Geral. O Programa refere-se a qualquer software ou trabalho e a um trabalho baseado em um Programa e significa tanto o Programa em si como quaisquer trabalhos derivados de acordo com a lei de direitos autorais, o que significa dizer, um trabalho que contenha o Programa ou uma parte deste, na sua forma original ou com modificações ou traduzido para uma outra língua (tradução está incluída sem limitações no termo modificação).

Atividades distintas de cópia, distribuição e modificação não estão cobertas por esta Licença, estando fora de seu escopo. O ato de executar o Programa não está restringido e a saída do Programa é coberta somente caso seu conteúdo contenha trabalhos baseados no Programa (independentemente de terem sidos gerados pela execução do Programa). Se isso é verdadeiro depende das funções executadas pelo Programa.

2. O código-fonte do Programa, da forma como foi recebido, pode ser copiado e distribuído, em qualquer media, desde que seja providenciado um aviso adequado sobre os copyrights e a negação de garantias, e todos os avisos que se referem à Licença Pública Geral e à ausência de garantias estejam inalterados e que qualquer produto oriundo do Programa esteja acompanhado desta Licença Pública Geral.

   É permitida a cobrança de taxas pelo ato físico de transferência ou gravação de cópias, e podem ser dadas garantias e suporte em troca da cobrança de valores.

3. Pode-se modificar a cópia ou cópias do Programa de qualquer forma que se deseje, ou ainda criar-se um trabalho baseado no Programa, copiá-lo e distribuir tais modificações sob os termos da seção 1 acima e do seguinte:

[a.] Deve existir aviso em destaque de que os dados originais foram alterados nos arquivos e as datas das mudanças;

[b.] Deve existir aviso de que o trabalho distribuído ou publicado é, de forma total ou em parte derivado do Programa ou de alguma parte sua, e que pode ser licenciado totalmente sem custos para terceiros sob os termos desta Licença.

[c.] Caso o programa modificado seja executado de forma interativa, é obri-

gatório, no início de sua execução, apresentar a informação de copyright e da ausência de garantias (ou de que a garantia corre por conta de terceiros), e que os usuários podem redistribuir o programa sob estas condições, indicando ao usuário como acessar esta Licença na sua íntegra.

Esses requisitos aplicam-se a trabalhos de modificação em geral. Caso algumas seções identificáveis não sejam derivadas do Programa, e podem ser consideradas como partes independentes, então esta Licença e seus Termos não se aplicam àquelas seções quando distribuídas separadamente. Porém ao distribuir aquelas seções como parte de um trabalho baseado no Programa, a distribuição como um todo deve conter os termos desta Licença, cujas permissões estendem-se ao trabalho como um todo, e não a cada uma das partes independentemente de quem os tenha desenvolvido.

Mais do que tencionar contestar os direitos sobre o trabalho desenvolvido por alguém, esta seção objetiva propiciar a correta distribuição de trabalhos derivados do Programa.

Adicionalmente, a mera adição de outro trabalho ao Programa, porém não baseado nele nem a um trabalho baseado nele, a um volume de armazenamento ou media de distribuição não obriga a utilização desta Licença e de seus termos ao trabalho.

São permitidas a cópia e a distribuição do Programa (ou a um trabalho baseado neste) na forma de código-objeto ou executável de acordo com os termos das Seções 1 e 2 acima, desde que atendido o seguinte:

[a.] Esteja acompanhado dos códigos-fonte legíveis, os quais devem ser distribuídos na forma da Seções 1 e 2 acima, em mídia normalmente utilizada para manuseio de softwares ou;

[b.] Esteja acompanhado de oferta escrita, válida por, no mínimo 3 anos, de disponibilizar a terceiros, por um custo não superior ao custo do meio físico de armazenamento, uma cópia completa dos códigos-fonte em meio magnético, de acordo com as Seções 1 e 2 acima;

[c.] Esteja acompanhado da mesma informação recebida em relação à oferta da distribuição do código-fonte correspondente (esta alternativa somente é permitida para distribuições não comerciais e somente se o programa recebido na forma de objeto ou executável tenha tal oferta, de acordo com a subseção 2 acima).

O código-fonte de um trabalho é a melhor forma de produzirem-se alterações naquele trabalho. Códigos fontes completos significam todos os fontes de todos os módulos, além das definições de interfaces associadas, arquivos, scripts utilizados na compilação e instalação do executável. Como uma exceção excepcional, o código-fonte distribuído poderá não incluir alguns componentes que não se encontrem em seu escopo, tais como compilador, cerne, etc. para o sistema operacional onde o trabalho seja executado.

Caso a distribuição do executável ou objeto seja feita através de acesso a um determinado ponto, então oferta equivalente de acesso deve ser feita aos códigos-fonte, mesmo que terceiros não sejam obrigados a copiarem os fontes juntos com os objetos simultaneamente.

1. Não é permitida a cópia, modificação, sub-licenciamento ou distribuição do Programa, exceto sob as condições expressas nesta Licença. Qualquer tentativa de cópia, modificação, sublicenciamento ou distribuição do Programa é proibida, e os direitos descritos nesta Licença cessarão imediatamente. Terceiros que tenham recebido cópias ou direitos na forma desta Licença não terão seus direitos cessados desde que permaneçam dentro das cláusulas desta Licença.

2. Não é necessária aceitação formal desta Licença, apesar de que não haverá documento ou contrato que garanta permissão de modificação ou distribuição do Programa ou seus trabalhos derivados. Essas ações são proibidas por lei, caso não se aceitem as condições desta Licença. A modificação ou distribuição do Programa ou qualquer trabalho baseado neste implica na aceitação desta Licença e de todos os termos desta para cópia, distribuição ou modificação do Programa ou trabalhos baseados neste.

3. Cada vez que o Programa seja distribuído (ou qualquer trabalho baseado neste), o recipiente automaticamente recebe uma licença do detentor original dos direitos de cópia, distribuição ou modificação do Programa objeto destes termos e condições. Não podem ser impostas outras restrições nos recipientes.

4. No caso de decisões judiciais ou alegações de uso indevido de patentes ou direitos autorais, restrições sejam impostas que contradigam esta Licença, estes não isentam da sua aplicação. Caso não seja possível distribuir o Programa de forma a garantir simultaneamente as obrigações desta Licença e outras que sejam necessárias, então o Programa não poderá ser distribuído.

   Caso esta Seção seja considerada inválida por qualquer motivo particular ou geral, o seu resultado implicará na invalidação geral desta licença na cópia, modificação, sublicenciamento ou distribuição do Programa ou trabalhos baseados neste.

   O propósito desta seção não é, de forma alguma, incitar quem quer que seja a infringir direitos reclamados em questões válidas e procedentes, e sim proteger as premissas do sistema de livre distribuição de software. Muitas pessoas têm feito contribuições generosas ao sistema, na forma de programas, e é ne-

cessário garantir a consistência e credibilidade do sistema, cabendo a estes e não a terceiros decidirem a forma de distribuição dos softwares.

Esta seção pretende tornar claro os motivos que geraram as demais cláusulas desta Licença.

5. Caso a distribuição do Programa dentro dos termos desta Licença tenha restrições em algum País, quer por patentes ou direitos autorais, o detentor original dos direitos autorais do Programa sob esta Licença pode adicionar explicitamente limitações geográficas de distribuição, excluindo aqueles Países, fazendo com que a distribuição somente seja possível nos Países não excluídos.

6. A Fundação de Software de Livre Distribuição (FSF - Free Software Foundation) pode publicar versões revisadas ou novas versões desta Licença Pública Geral de tempos em tempos. Estas novas versões manterão os mesmos objetivos e o espírito da presente versão, podendo variar em detalhes referentes a novas situações encontradas.

   A cada versão é dado um número distinto. Caso o Programa especifique um número de versão específico desta Licença a qual tenha em seu conteúdo a expressão “ou versão mais atualizada”, é possível optar pelas condições daquela versão ou de qualquer versão mais atualizada publicada pela FSF.

7. Caso se deseje incorporar parte do Programa em outros programas de livre distribuição de softwares é necessária autorização formal do autor. Para softwares que a FSF detenha os direitos autorais, podem ser abertas exceções desde que mantido o espírito e objetivos originais desta Licença.

8. UMA VEZ QUE O PROGRAMA É LICENCIADO SEM ÔNUS, NÃO HÁ QUAL-

QUER GARANTIA PARA O PROGRAMA. EXCETO QUANDO TERCEIROS EXPRESSEM-SE FORMALMENTE, O PROGRAMA É DISPONIBILIZADO EM SEU FORMATO ORIGINAL, SEM GARANTIAS DE QUALQUER NATUREZA, EXPRESSAS OU IMPLÍCITAS, INCLUINDO MAS NÃO LIMITADAS, ÀS GARANTIAS COMERCIAIS E DO ATENDIMENTO DE DETERMINADO FIM. A QUALIDADE E A PERFORMANCE SÃO DE RISCO EXCLUSIVO DOS USUÁRIOS, CORRENDO POR SUA CONTA OS CUSTOS NECESSÁRIOS A EVENTUAIS ALTERAÇÕES, CORREÇÕES E REPAROS JULGADOS NECESSÁRIOS.

9. EM NENHUMA OCASIÃO, A MENOS QUE REQUERIDO POR DECISÃO JUDICIAL OU POR LIVRE VONTADE, O AUTOR OU TERCEIROS QUE TENHAM MODIFICADO O PROGRAMA, SERÃO RESPONSÁVEIS POR DANOS OU PREJUÍZOS PROVENIENTES DO USO OU DA FALTA DE HABILIDADE NA SUA UTILIZAÇÃO (INCLUINDO MAS NÃO LIMITADA A PERDA DE DADOS OU DADOS ERRÔNEOS), MESMO QUE NÃO TENHA SIDO EMITIDO AVISO DE POSSÍVEIS ERROS OU DANOS.

FIM DA LICENÇA

Como Aplicar Estes Termos a Novos Programas?

Caso você tenha desenvolvido um novo programa e deseja a sua ampla distribuição para o público, a melhor forma de conseguí-lo é torná-lo um software de livre distribuição, onde qualquer um possa distribuí-lo nas condições desta Licença.

Para tanto basta anexar este aviso ao programa. É aconselhável indicar ainda no início de cada arquivo fonte a ausência de garantias e um apontamento para um arquivo contendo o texto geral desta Licença, como por exemplo:

```
(uma linha para dar o nome do programa e uma breve idéia do que
ele faz.)
 Copyright ® 19yy nome do autor

    Este programa é um software de livre distribuição,
    que pode ser copiado e distribuído sob os termos da Licença
    Pública Geral GNU, conforme publicada pela Free Software
    Foundation, versão 2 da licença ou (a critério do autor)
    qualquer versão posterior.

    Este programa é distribuído na expectativa de ser útil aos
    seus usuários, porém NÃO TEM NENHUMA GARANTIA, EXPLÍCITAS
    OU IMPLÍCITAS, COMERCIAIS OU DE ATENDIMENTO A UMA
    DETERMINADA FINALIDADE. Consulte a Licença Pública Geral GNU
```

```
para mais detalhes.

Deve haver uma cópia da Licença Pública Geral
GNU junto com este software em inglês ou português. Caso
não haja escreva para Free Software Foundation, Inc.,
675 Mass Ave, Cambridge, MA 02139, USA.
```

Inclua também informações de como contatar você através de correio eletrônico ou endereço comercial/residencial.

Caso o programa seja interativo, apresente no início do programa um breve aviso. Por exemplo:

```
Gnomovision versão 69, Copyright  nome do autor Gnomovision
NÃO POSSUI NENHUMA GARANTIA; para detalhes digite “mostre
garantia”. Este é um software de livre distribuição e você
está autorizado a distribuí-lo dentro de certas condições.
Digite “mostre condição” para mais detalhes.
```

Os comandos hipotéticos “mostre garantia” e “mostre condição” apresentarão as partes apropriadas da Licença Pública Geral GNU. Evidentemente os comandos podem variar ou serem acionados por outras interfaces como clique de mouse, etc..

Esta Licença Pública Geral não permite a incorporação de seu programa em programas proprietários. Se o seu programa é uma subrotina de biblioteca, você pode

achar mais interessante permitir a “ligação” de aplicações proprietárias com sua biblioteca. Se é isso que você deseja fazer, use a Licença Pública Geral GNU para Bibliotecas no lugar desta Licença.

Índice Remissivo

Símbolos

A

B

C

D

E

F

G

H

I

L

M

N

P

Q

R

S

T

U

V

W