

SÉRIE TECNOLOGIA DA INFORMAÇÃO - *HARDWARE*

SERVIDORES DE REDES





*Iniciativa da CNI - Confederação
Nacional da Indústria*

SÉRIE TECNOLOGIA DA INFORMAÇÃO - HARDWARE

SERVIDORES DE REDES



CONFEDERAÇÃO NACIONAL DA INDÚSTRIA – CNI

Robson Braga de Andrade
Presidente

DIRETORIA DE EDUCAÇÃO E TECNOLOGIA

Rafael Esmeraldo Lucchesi Ramacciotti
Diretor de Educação e Tecnologia

SERVIÇO NACIONAL DE APRENDIZAGEM INDUSTRIAL – SENAI

Conselho Nacional

Robson Braga de Andrade
Presidente

SENAI – Departamento Nacional

Rafael Esmeraldo Lucchesi Ramacciotti
Diretor-Geral

Gustavo Leal Sales Filho
Diretor de Operações



*Iniciativa da CNI - Confederação
Nacional da Indústria*

SÉRIE TECNOLOGIA DA INFORMAÇÃO - HARDWARE

SERVIDORES DE REDES



© 2012. SENAI – Departamento Nacional

© 2012. SENAI – Departamento Regional de Santa Catarina

A reprodução total ou parcial desta publicação por quaisquer meios, seja eletrônico, mecânico, fotocópia, de gravação ou outros, somente será permitida com prévia autorização, por escrito, do SENAI.

Esta publicação foi elaborada pela equipe do Núcleo de Educação a Distância do SENAI de Santa Catarina, com a coordenação do SENAI Departamento Nacional, para ser utilizada por todos os Departamentos Regionais do SENAI nos cursos presenciais e a distância.

SENAI Departamento Nacional

Unidade de Educação Profissional e Tecnológica – UNIEP

SENAI Departamento Regional de Santa Catarina

Núcleo de Educação – NED

FICHA CATALÓGRAFICA

S491g

Serviço Nacional de Aprendizagem Industrial. Departamento Nacional.

Gestão de pessoas / Serviço Nacional de Aprendizagem Industrial. Departamento Nacional, Serviço Nacional de Aprendizagem Industrial. Departamento Regional de Santa Catarina . Brasília : SENAI/DN, 2012.

142 p. II. (Série Segurança do Trabalho).

ISBN 978-85-7510-484-3

1. Gestão de Pessoas 2. Trabalho em Equipe I. Serviço Nacional de Aprendizagem Industrial. Departamento Regional de Santa Catarina II. Título III. Série

CDU:005.95

SENAI

Sede

Serviço Nacional de
Aprendizagem Industrial
Departamento Nacional

Setor Bancário Norte • Quadra 1 • Bloco C • Edifício Roberto
Simonsen • 70040-903 • Brasília – DF • Tel.: (0xx61) 3317-
9001 Fax: (0xx61) 3317-9190 • <http://www.senai.br>

Lista de ilustrações

Figura 1 - Processador com 4 Núcleos.....	21
Figura 2 - Arquitetura Interna CPU AMD Opteron	22
Figura 3 - Exemplo do sistema Cluster	26
Figura 4 - Diagrama de Multiprocessadores	27
Figura 5 - Arquitetura em Blocos de um Computador	46
Figura 6 - Placa-mãe para 2 Processadores.....	47
Figura 7 - <i>Hardware</i> de Servidor	47
Figura 8 - Tipos de servidores	51
Figura 9 - Servidor Low-End	51
Figura 10 - Servidor Low-End Sun	52
Figura 11 - Chassi de Servidores Blade	53
Figura 12 - Cartão Blade Server da HP	54
Figura 13 - Rack com Servidores e Cabos.....	54
Figura 14 - Servidor de Rack da Dell	55
Figura 15 - Super Servidor IBM System P5	56
Figura 16 - Microprocessador IBM Power 7	60
Figura 17 - Pastilha do Microprocessador IBM Power 7	60
Figura 18 - CPU INTEL Core I7	61
Figura 19 - Modelo de Aterramento.....	67
Figura 20 - Novo modelo de tomadas	69
Figura 21 - Novo modelo de plugues	69
Figura 22 - Pulseira Antiestática.....	70
Figura 23 - Estabilizador de Baixa Potência	72
Figura 24 - Modelo de No-Breaks.....	76
Figura 25 - Grupo Gerador	79
Figura 26 - Modelo de Hierarquia de Memórias	84
Figura 27 - Alocação Contínua de Memória	89
Figura 28 - Modelo de um Processo	90
Figura 29 - Modelo de um PCB – Bloco de Controle de Processos	91
Figura 30 - O mapeamento de endereços de memória lógica x física, realizado pela MMU – Unida- de de Gerenciamento de Memória.....	92
Figura 31 - Formas de Alocação de Memória.	92
Figura 32 - Partições de Memória com Tamanhos Diferentes	93
Figura 33 - Alocação de Processos na Memória. Partições de Tamanhos Diferentes	94
Figura 34 - Modelo de Swap de Memória	97
Figura 35 - Tela do Programa htop no GNU/Linux.	99
Figura 36 - Tipos de Organização Interna de Arquivos	102
Figura 37 - Exemplos de Alocação de Blocos em Disco	103
Figura 38 - Exemplo de Alocação Contígua de Blocos	104
Figura 39 - Exemplo de Fragmentação em Disco.....	105

Figura 40 - Alocação Encadeada de Blocos em Disco.....	105
Figura 41 - Exemplo de Alocação Indexada de Blocos em Disco	106
Figura 42 - Exemplo de Alocação de Blocos por um <i>I-node</i>	107
Figura 43 - Propriedades da Lista de Controle de Acesso – ACL no Windows – NTFS	111
Figura 44 - Estrutura de Diretórios Típica. Sistemas Unix/Linux.....	115
Figura 45 - Modelo de Permissões no Unix/Linux.....	117
Figura 46 - Tela do Gnome System Monitor	119
Figura 47 - Modelo de Camadas de <i>Software</i> num Sistema Linux	122
Figura 48 - Modelo de camadas de <i>software</i> para acesso ao <i>hardware</i>	123
Figura 49 - Modelo de camadas com <i>driver</i> de dispositivos.....	125
Figura 50 - Modelo de comunicação para acessar um arquivo.....	125
Figura 51 - Arquitetura do Windows	127
Figura 52 - Leitor Biométrico para Controle de Acesso	134
Figura 53 - Data Center	138
Figura 54 - Arquivo <i>passwd</i>	162
Figura 55 - Detalhes do arquivo <i>passwd</i>	163
Figura 56 - Senhas criptografadas	164
Figura 57 - Alterando senha.....	164
Figura 58 - Criação usuário senha	165
Figura 59 - Criação usuário redigitando a senha	165
Figura 60 - Criação usuário, nome completo do usuário.....	166
Figura 61 - Criação usuário, número da sala	166
Figura 62 - Criação de usuário, número de telefone	166
Figura 63 - Criação usuário, telefone residencial	166
Figura 64 - Criação usuário, outras informações.....	167
Figura 65 - Criação usuário, finalização	167
Figura 66 - Comando su.....	169
Figura 67 - Arquivo <i>group</i>	171
Figura 68 - Detalhes do arquivo <i>group</i>	171
Figura 69 - Permissões	175
Figura 70 - Permissões e permissões especiais	176
Figura 71 - Binários	177
Figura 72 - Tela da BIOS.....	195
Figura 73 - Tela BIOS <i>Setup</i> aba <i>Boot</i>	195
Figura 74 - Tela BIOS <i>Setup</i> aba <i>Boot</i>	196
Figura 75 - Salvando configuração <i>Setup</i>	196
Figura 76 - Menu <i>BOOT</i>	197
Figura 77 - Escolha do Idioma	198
Figura 78 - Localização Geográfica I.....	199
Figura 79 - Localização Geográfica II.....	199
Figura 80 - Localização Geográfica III.....	200
Figura 81 - Configurações Locais IV.....	200

Figura 82 - Layout do Teclado.....	201
Figura 83 - Tela de Verificação de Dispositivo.....	201
Figura 84 - Configuração Rede DHCP	202
Figura 85 - Erro na Configuração da Rede.....	202
Figura 86 - Configuração de Rede Manual.....	202
Figura 87 - IP Address	203
Figura 88 - Máscara de Rede	203
Figura 89 - Gateway da Rede	204
Figura 90 - Endereço DNS	204
Figura 91 - Nome do Equipamento	204
Figura 92 - Nome do Domínio.....	205
Figura 93 - Senha do <i>root</i>	206
Figura 94 - Repetindo a senha do <i>root</i>	206
Figura 95 - Criando novo Usuário	207
Figura 96 - Apelido do usuário	207
Figura 97 - Senha usuário comum	207
Figura 98 - Repetindo a senha do usuário comum.....	208
Figura 99 - Fuso Horário.....	208
Figura 100 - Método de Particionamento.....	210
Figura 101 - Selecionando o Disco	210
Figura 102 - Criar Tabela de Partição.....	211
Figura 103 - Área Livre do Disco (<i>free space</i>)	211
Figura 104 - Nova partição	211
Figura 105 - Tamanho da nova partição	212
Figura 106 - Tipo da partição	212
Figura 107 - Localização da Partição.....	213
Figura 108 - Editando a partição	213
Figura 109 - Ponto de montagem.....	214
Figura 110 - <i>Flag</i> de inicialização.....	214
Figura 111 - Finalizando a primeira partição	215
Figura 112 - Finalização das partições.....	215
Figura 113 - Gravando as alterações no disco	216
Figura 114 - Formatando as partições.....	216
Figura 115 - Instalando sistema básico	216
Figura 116 - Gerenciador de Pacotes I	217
Figura 117 - Gerenciador de Pacotes II.....	217
Figura 118 - Erro do gerenciador de pacotes.....	218
Figura 119 - Seleção de <i>software</i>	218
Figura 120 - Pesquisa de Participação	219
Figura 121 - Seleção de <i>software</i>	219
Figura 122 - Instalando <i>software</i>	220
Figura 123 - Instalação do Grub.....	220

Figura 124 - Instalando o Grub	220
Figura 125 - Finalizando a instalação.....	221
Figura 126 - Completando a instalação.....	221
Figura 127 - Grub	221
Figura 128 - Tela de <i>login</i> do Linux	222
Figura 129 - Início da Instalação	223
Figura 130 - Configuração de idioma	224
Figura 131 - Iniciando a instalação	224
Figura 132 - Tela de aguarde.....	224
Figura 133 - Escolha do sistema.....	225
Figura 134 - Licença	225
Figura 135 - Tipo da instalação.....	225
Figura 136 - Local para instalação.....	226
Figura 137 - Local de instalação 1	226
Figura 138 - Tamanho partição	227
Figura 139 - Partição dividida	227
Figura 140 - Disco particionado.....	227
Figura 141 - Instalando o Windows	228
Figura 142 - Andamento da Instalação	228
Figura 143 - Tela de <i>reset</i>	228
Figura 144 - Tela de retorno do Windows.....	228
Figura 145 - Completando a instalação	229
Figura 146 - Andamento da instalação	229
Figura 147 - Mensagem de senha	229
Figura 148 - Criando a senha do administrator.....	230
Figura 149 - Confirmação de alteração de senha.....	230
Figura 150 - Preparando o desktop	230
Figura 151 - Server manager.....	231
Figura 152 - <i>Administrative Tools</i>	231
Figura 153 - Máquinas Virtuais Tipo 1	238
Figura 154 - Máquinas Virtuais do Tipo 2	239
Figura 155 - Virtualização Total	240
Figura 156 - Paravirtualização	241
Figura 157 - Grupo de Volumes	247
 Quadro 1 - Matriz curricular.....	16
Quadro 2 - Tipos de <i>Raid</i>	40
Quadro 3 - Dispositivos de hardware.....	50
Quadro 4 - Três tipos básicos de oermissão.....	116
Quadro 5 - Opções do fdisk	148
Quadro 6 - Tipos de fdisk.....	150
Quadro 7 - Opções do mkfs	150

Quadro 8 - Opções do DF	153
Quadro 9 - Opções do DU	153
Quadro 10 - Opções do fsck	153
Quadro 11 - Opções do fstab	155
Quadro 12 - Opções <i>dump</i>	155
Quadro 13 - Opções <i>pass</i>	156
Quadro 14 - Opções do <i>mount</i>	156
Quadro 15 - Opções do <i>umount</i>	158
Quadro 16 - Detalhamento do arquivo <i>passwd</i>	163
Quadro 17 - Detalhamento do arquivo <i>group</i>	172
Quadro 18 - Variações das permissões	176
Quadro 19 - Chmod	178
Quadro 20 - Tabela de atributos.....	182
Quadro 21 - Níveis de <i>RAID</i>	243
 Tabela 1 - Serviços de Rede x Hardware Mínimo	37
Tabela 2 - Estrutura de um <i>i-node</i>	109
Tabela 3 - Exemplo arquivo /etc/fstab	155
Tabela 4 - Tabela de permissões.....	177
Tabela 5 - Partições	209

Sumário

1 Introdução	15
2 Conceitos de Multiprocessamento.....	19
2.1 Multiprocessamento	20
2.2 Microprocessadores para multiprocessamento.....	21
2.3 Sistemas com múltiplos processadores	23
3 Multusuário e Multitarefa	31
3.1 Sistemas multitarefa.....	32
3.2 Sistemas multusuário	33
3.3 Servidores de rede multusuário e multitarefa	34
3.4 Sistemas operacionais com suporte a multusuários e multitarefas	41
4 Arquitetura de <i>Hardware</i> de Servidores.....	45
4.1 <i>Hardware</i> de servidores de rede.....	46
4.2 Dispositivos de <i>hardware</i> redundantes.....	48
4.2.1 Servidores de rede com baixa, média e alta especialização <i>hardware</i>	51
4.2.2 Microprocessadores CISC e RISC	56
5 Riscos Elétricos.....	65
5.1 Alimentação elétrica	66
5.2 Estabilizadores elétricos.....	71
5.2.1 No-break.....	73
5.2.2 Grupo Gerador	76
6 Gerenciamento de Memória.....	83
6.1 Gerenciamento de memória no computador.....	84
6.2 Gerenciamento de memória pelo <i>hardware</i>	86
6.3 Gerenciamento de memória pelo sistema operacional.....	88
7 Gerenciamento de Dados.....	101
7.1 Gerenciamento de arquivos	102
7.2 O <i>i-node</i>	108
7.3 Gerenciamento de arquivos no Windows	111
7.4 Gerenciamento de arquivos no UNIX/LINUX	113
8 Gerenciamento de Acesso ao <i>Hardware</i>	121
8.1 Acesso ao <i>hardware</i>	122
9 Mecanismos de Segurança	131
9.1 Segurança física e lógica	132
9.2 Mecanismos de segurança.....	133
9.3 Mecanismos de segurança lógica	135

10 Trabalhando com Discos e Sistemas de Arquivos	141
10.1 Sistemas de arquivos	142
10.1.1 Tipos de sistemas de arquivos	142
10.2 Agrupamento dos arquivos	143
10.3 Particionamento.....	145
10.3.1 Tipos de partições	146
10.3.2 Criando partições	148
10.3.3 Formatação.....	150
10.3.4 Endereçamento dos arquivos	151
10.3.5 Gerenciando o sistema de arquivo	153
10.3.6 Montando dispositivos.....	154
11 Administrando Sistemas.....	161
11.1 Administração sistema operacional para rede.....	162
11.1.1 Contas de usuários.....	162
11.1.2 Criando contas de usuários	164
11.2 Gerenciando grupos	171
11.3 Permissões do sistema.....	175
11.3.1 Chmod.....	178
11.3.2 Chown	179
11.3.3 Chgrp	180
11.3.4 Isattr.....	182
11.4 Quotas de disco.....	183
11.4.1 Implementando as cotas de disco	183
11.4.2 Limitando espaço	185
12 Sistemas Operacionais	191
12.1 Sistemas operacionais de rede	192
12.1.1 Linux.....	192
12.2 Instalação sistema operacional de arquitetura aberta.....	193
12.2.1 Procedimentos iniciais	194
12.2.2 Configuração do <i>boot</i>	194
12.2.3 Iniciando a instalação do sistema Linux.....	197
12.2.4 <i>Layout</i> do teclado.....	200
12.3 Instalação de sistema operacional de arquitetura fechada.....	222
12.3.1 Procedimentos iniciais.....	223
13 Trabalhando com Sistemas de Redundância, Virtuais e Lógicos	235
13.1 Virtualização de sistemas operacionais	236
13.1.1 A origem da virtualização.....	236
13.1.2 O funcionamento da virtualização.....	237
13.1.3 Máquina virtual	237
13.1.4 Tipos de virtualização	240
13.2 RAID – Redundant Array of Independent Disks.....	241
13.2.1 Níveis de <i>RAID</i>	242

13.2.2 Criação de <i>array</i> de discos.....	243
13.3 LVM – <i>Logical Volume Manager</i>	246
13.3.1 <i>Logical Volumes (LV)</i>	246
13.3.2 Gerenciando os volumes lógicos.....	247
Referências.....	257
Minicurrículo dos Autores.....	259
Índice	261

Introdução

1



Desde a década de 60, quando os computadores eram utilizados apenas por pesquisadores, cientistas e de uso militar, que os sistemas operacionais são freqüentemente atualizados. Uma das primeiras modificações foi fazer com que os sistemas operacionais realizassem mais de uma tarefa simultâneo. Mas não foram apenas os sistemas operacionais que evoluíram, outros serviços e aplicações também obtiveram melhorias cuja finalidade era favorecer ao usuário final. Como exemplo, é possível citar a virtualização, que era utilizada apenas para estudos, e hoje está presente em diversos ramos da informática.

Neste livro didático serão abordados, além dos sistemas operacionais de arquitetura aberta e fechada e virtualização, outros diversos assuntos, como riscos elétricos, gerencia de memória, a importância de redundância dos discos físicos, os sistemas de arquivos Linux e Windows, instalarem sistemas operacionais de arquitetura aberta e fechada e administrar um sistema operacional, tarefa esta muito árdua de responsabilidade dos administradores de sistemas.

Abaixo segue a matriz curricular com a unidade curricular que veremos neste curso.

Técnico em Redes de Computadores

MÓDULOS	DENOMINAÇÃO	UNIDADES CURRICULARES	CARGA HORÁRIA	CARGA HORÁRIA DO MÓDULO
Básico	Básico	<ul style="list-style-type: none">• Eletroeletrônica Aplicada• Montagem e Manutenção de Computadores• Ferramentas para Documentação Técnica	60h 160h 120h	340h
Específico I	Ativos de Rede	<ul style="list-style-type: none">• Cabeamento Estruturado• Arquitetura de Redes• Comutação de Rede Local• Interconexão de Redes PR• Gerenciamento e Monitamento de Rede	108h 80h 120h 96h 60h	464h

Específico II	Servidores de Rede	• Servidores de Redes	120h	396h
		• Serviços de Rede	120h	
		• Serviços de Convergência	60h	
		• Segurança de Redes	96h	

Quadro 1 - Matriz curricular

Fonte: SENAI DN

Agora você é convidado a trilhar os caminhos do conhecimento. Faça deste processo um momento de construção de novos saberes, onde teoria e prática devem estar alinhadas para o seu desenvolvimento profissional. Bons estudos!

Anotações:

Conceitos de Multiprocessamento

2



Neste capítulo que inicia serão abordados os principais conceitos sobre multiprocessamento. Nesta primeira parte do conteúdo você conhecerá os conceitos relacionados aos sistemas operacionais, bem como os recursos de *hardware* necessários para que o multiprocessamento possa acontecer.

O assunto que abre este capítulo trata sobre microprocessadores para multiprocessamento, e, em seguida, sistemas com múltiplos processadores. E ao final desse capítulo, você terá subsídios para:

- a) compreender o multiprocessamento;
- b) entender o que é escalonamento;
- c) conhecer os microprocessadores para multiprocessamento;
- d) compreender o que são sistemas com multiprocessadores.

Deste modo, você terá visto os conceitos principais sobre o multiprocessamento.

¹ SMARTPHONE

Telefone celular com capacidades de processamento semelhantes à um microcomputador, tipicamente executando um sistema operacional próprio, com recursos de acesso à Internet e conexões de rede sem fio (Wireless) e/ou conexões GSM-3G.

² TABLETS

Microcomputadores formados somente por uma tela de cristal líquido sensível ao toque (*touch screen*), com tamanhos entre 7 e 11 polegadas, com conexões de rede sem fio (Wireless) ou através de GSM-3G, alguns modelos também funcionam como *Smartphone*.

2.1 MULTIPROCESSAMENTO

Você sabe o que um processamento de dados pode representar?

O processamento de dados representa a execução de programa residente em memória principal (RAM – *Random Access Memory* – Memória de Acesso Aleatório), em que as instruções do programa são executadas de forma sequencial pelo processador. O controle da execução do programa está a cargo do sistema operacional, o qual, dentre outras responsabilidades, objetiva a otimização do uso do microprocessador (CPU – *Central Processor Unit* – Unidade Central de Processamento).

Como é possível perceber, dependemos do sistema operacional e do microprocessador para a execução de um programa sequencial, em que diversos programas funcionam ao mesmo tempo. Nesse caso, tanto o sistema operacional quanto a CPU devem suportar esta característica.



Stockbyte (20-?)

Atualmente, quase todos os microprocessadores que são comercializados possuem características de multiprocessamento. Quanto aos sistemas operacionais, esta característica também está presente, inclusive em sistemas de *smartphones*¹ e *tablets*², por exemplo.

O multiprocessamento é a execução de vários programas de computador de forma simultânea (ou quase) permitindo que várias tarefas sejam realizadas ao mesmo tempo, ou então, no mínimo, de uma forma sequencial, porém muito rápida. Neste caso, o sistema operacional deverá realizar uma dura tarefa denominada 'escalonamento'.

Mas o que vem a ser escalonamento?

O escalonamento é uma característica dos sistemas operacionais que permite o compartilhamento do tempo do microprocessador com todos os programas

residentes em memória, concedendo um tempo justo para cada programa, de forma que todos possam executar suas instruções, dando a impressão de uma execução paralela de vários programas.



FIQUE ALERTA

Muitos processadores modernos possuem mais de um núcleo interno, ou seja, estes microprocessadores possuem duas ou mais CPUs internas (dois ou mais núcleos).

Deste modo, microprocessadores modernos com estas características permitem que vários programas sejam executados de forma paralela, pois muitos programas são executados um em cada CPU ou, até mesmo, em várias. Assim, um programa poderá ser executado em mais de uma CPU, pois o sistema operacional otimizará a utilização, concedendo tempo para um programa em todas as CPUs, caso estas estejam disponíveis.

2.2 MICROPROCESSADORES PARA MULTIPROCESSAMENTO

Como visto anteriormente, a capacidade para execução de vários programas ao mesmo tempo, ou seja, o multiprocessamento é dependente do microprocessador e do sistema operacional. Dentre as marcas mais conhecidas estão: Intel, AMD, IBM e HP, e estas possuem capacidades para multiprocessamento. O microprocessador E6510, da família Xeon 6000 da Intel, possui quatro núcleos internos. Trabalha com um clock de 1.73Ghz e possui 12 megabytes de cache nível 3 (L3). Veja como é a estrutura em blocos deste microprocessador, na figura a seguir.

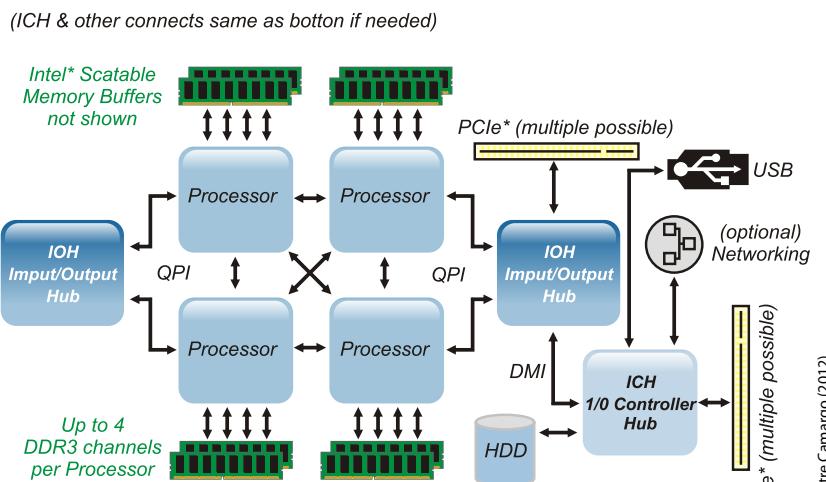


Figura 1 - Processador com 4 Núcleos

³ BARRAMENTOS PCI

O Barramento PCI (*Peripheral Component Interconnect - Interconector de Componentes Periféricos*) é um elemento para conectar periféricos em computadores baseados na arquitetura IBM PC. Foi criado pela Intel, em junho de 1992, na mesma época em que desenvolvia o processador Pentium. Tem capacidade de trabalhar a 32 bits ou 64 bits e as frequências de 33MHz ou 66MHz, oferecendo altas taxas de transferência de dados. Um barramento PCI de 32 bits pode transferir até 132MBits por segundo, trabalhando a 33MHz, enquanto um slot PCI de 64 bits tem sua taxa máxima dobrada, alcançando 264MiBits por segundo à frequência de 33MHz, ou até 528MiBits por segundo, operando a 66MHz. Dicionário Babylon e Wikipédia (2011)

⁴ CLOCK

Sob o ponto de vista de processadores, representa a frequência de operação de um processador. Atualmente, o *clock* dos microprocessadores é medido em Gigahertz – Ghz, significando a execução de bilhões de instruções por segundo. Não pode ser entendido como uma medida de velocidade, mas de execução de instruções. Entretanto, há instruções mais complexas dentro de um microprocessador que, para serem executadas, precisam de mais de um ciclo de *clock*, bem como, há microprocessadores que podem executar mais de uma instrução no mesmo ciclo de *clock*.

Na figura que você visualizou, foi possível verificar os componentes internos da CPU e seus quatro núcleos *processor* interligados com os demais componentes do computador, como a memória RAM (DDR3) e os barramentos PCI³.

Este tipo de microprocessador é geralmente utilizado em servidores de rede. Em muitos modelos comercialmente disponíveis, há servidores de rede contendo 4 ou 8 CPUs, como a da figura. Neste caso, tem-se um servidor de rede com 8 CPUs físicas, tendo cada uma delas 4 núcleos, totalizando 32 processadores internos disponíveis para processamento.

A família de processadores 6100 da AMD chega a ter CPUs com até 12 núcleos internos. O modelo 6176 SE possui 12 núcleos internos, trabalha com um *clock* de 2.3Ghz, 512MB de *cache* L2 por núcleo e, ainda, 12MB de *cache* L3 para uso comum por todos os núcleos do microprocessador.

Sem dúvida é um dos microprocessadores mais avançados atualmente, permitindo sua utilização em servidores de rede de média e alta capacidade e, até mesmo, em supercomputadores.

A figura seguinte irá mostrar um diagrama em blocos da estrutura interna de uma CPU AMD Opteron, com 6 núcleos internos. Este modelo de CPU também é adequado para servidores de rede, pois possibilitam maior *performance* e a capacidade de trabalho com outras CPUs idênticas dentro de uma mesma placa-mãe.

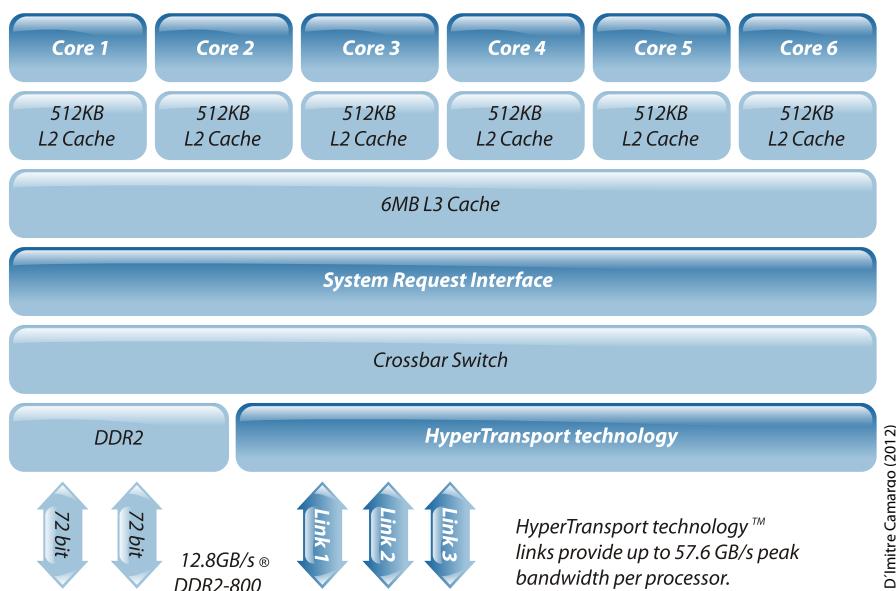


Figura 2 - Arquitetura Interna CPU AMD Opteron

A IBM possui a linha de microprocessadores POWER7, na qual cada microprocessador pode possuir até 8 núcleos internos, trabalhando com *clock*⁴ de 3,3Ghz de frequência e podendo executar até 4 *Threads* por núcleo. Muitos sistemas de servidores IBM para uso como servidores de rede já podem vir com este tipo de

microprocessador, permitindo composições de servidores com até 256 microprocessadores por máquina e endereçando incríveis 8TB (terabytes) de memória.

Atualmente o mercado mundial de microprocessadores possui diversas opções de CPUs, as quais podem oferecer uma ampla gama de aplicações, desde simples *tablets*, microcomputadores tipo *desktop* e servidores de rede básicos, até grandes servidores contendo mais de 200 núcleos de microprocessadores, permitindo assim, uma ampla gama de aplicações e utilizações.

Em geral, é possível perceber que a capacidade para multiprocessamento está plenamente atendida atualmente pelos diversos fabricantes de microprocessadores, em que, o que é importante saber é que existem outras características relevantes para a definição de um bom servidor de rede, as quais você conhecerá ao longo deste livro didático.



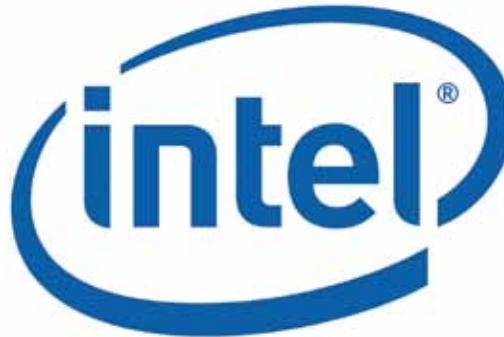
**SAIBA
MAIS**

Para aprofundar conhecimentos sobre barramentos de dados, antigos e atuais, acesse o seguinte endereço: <<http://www.clubedohardware.com.br/artigos/Barramento-PCI-Express/1060/1>>.

2.3 SISTEMAS COM MÚLTIPLOS PROCESSADORES

Sistemas com múltiplos processadores são computadores que possuem internamente CPUs com dois ou mais núcleos, ou então várias CPUs contendo um ou mais núcleos internos.

A rigor, conforme já foi apresentado, quase todos os fabricantes e modelos de microprocessadores possuem características de muitos núcleos. Desde os mais simples, como o Atom da Intel, eles já possuem em seu interior a capacidade de execução de múltiplas *Threads*, permitindo a implementação do multiprocessamento.



Cubicom [20-7])

Desse modo, as arquiteturas atuais de servidores de rede comercializados já possuem como base microprocessadores com dois ou mais núcleos, o que então nos permite dizer que temos à nossa disposição uma ampla variedade de escolhas entre CPUs com múltiplos núcleos e servidores com duas ou mais CPUs.

Do ponto de vista do controle de execução de processos, os processadores de uma máquina com múltiplos núcleos precisam implementar alguma forma de gerência, pois caso contrário, uma CPU poderia entrar em conflito com outra na execução de um processo, ou então, acessar a mesma área de memória. A solução encontrada foi a tecnologia do **Multiprocessamento Simétrico** ou **SMP**.



Consultando os sites a seguir você poderá obter mais informações sobre os microprocessadores com capacidade para multitarefa e multiprocessamento.

<<http://www.intel.com.br>>
<<http://www.amd.com.br>>
<<http://www.ibm.com.br>>

No modelo de multiprocessamento simétrico existe uma única cópia do sistema operacional na memória, mas qualquer CPU poderá executá-la. No momento em que chegar alguma chamada de sistema, a CPU local responsável é acionada e chaveia a execução para o modo núcleo e então processa a chamada. Esse modelo está implementado atualmente em todas as CPUs comercializadas no mercado e é uma característica importante na escolha de um servidor de rede.

Já que o assunto tratado descreve sistemas com múltiplos processadores, é importante que você conheça os conceitos de **Sistemas Fortemente Acoplados** e **Sistemas Fracamente Acoplados**. O conceito desses dois sistemas se aplica aos Sistemas Operacionais, mas de certa forma, fornece uma visão mais ampla das arquiteturas de computadores, já que é possível perceber que servidores de rede com uma ou mais CPUs internas perfazem um sistema fortemente acoplado.

E qual é o conceito de um sistema fortemente acoplado?

Sistemas fortemente acoplados são os modelos de arquitetura de *hardware* de servidores que descrevemos até então, nos quais é possível ter computadores com uma ou várias CPUs. Nesse caso, estas CPUs estão interligadas internamente por meio dos circuitos e controladores internos da placa-mãe, ou seja, estão fortemente acopladas, definindo uma arquitetura de *hardware* única, consistente e completamente funcional.



VOCÊ SABIA?

Que em um sistema com vários processadores, no momento da carga do sistema operacional somente um dos processadores é utilizado? Após essa etapa é que os demais processadores poderão ser utilizados para trabalho.

Sistemas fracamente acoplados são sistemas operacionais de rede que trabalham de forma única, utilizando vários computadores, dando a impressão de ser um único sistema, quando na verdade, é composto por vários computadores.

No contexto da arquitetura de *hardware* de servidores de rede, não é possível afirmar que existem arquiteturas fracamente acopladas. No entanto, num contexto mais amplo, que abrange não só a arquitetura de *hardware* mas também dos sistemas operacionais envolvidos, é possível dizer que um sistema fracamente acoplado é aquele baseado em um *hardware* interligado através de algum tipo de conexão física de rede.

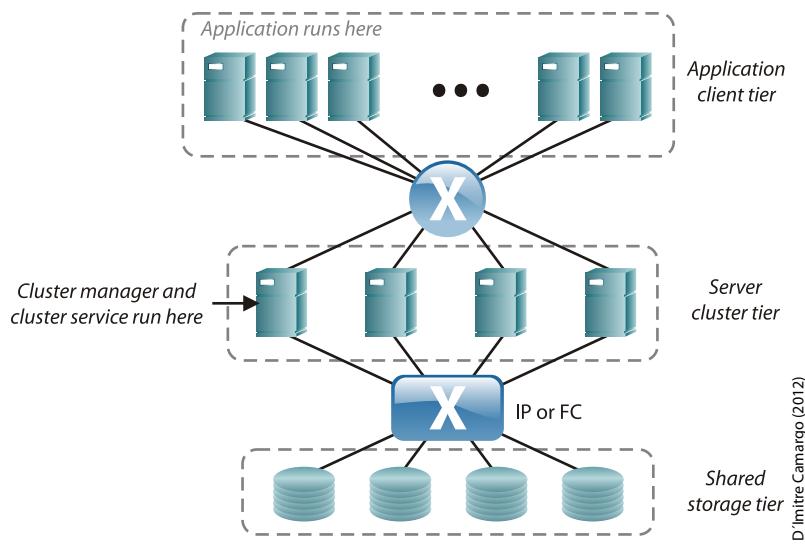


VOCÊ SABIA?

Que o tipo de sistema fracamente acoplado mais conhecido é o *Cluster*?

Mas o que é *Cluster*?

Cluster é um sistema composto de vários computadores trabalhando em conjunto, sob o mesmo sistema operacional, executando tarefas em todos os computadores simultaneamente, dando a impressão de que todos os computadores são uma única máquina, quando na verdade são várias, podendo chegar a centenas de computadores interligados, dependendo do projeto.



D'Inizio Camargo (2012)

Figura 3 - Exemplo do sistema Cluster



FIQUE ALERTA

Servidores com múltiplos processadores tendem a aquecer e o controle da temperatura deve ser levado a sério. Mesmo que os gabinetes destas máquinas sejam adequados, o ambiente para estes computadores também deve ser ajustado para garantir a refrigeração do equipamento, provendo um fluxo de ar renovado constantemente.

Uma característica importante de um *Cluster* é a de que todos os computadores membros estão fisicamente próximos, ou seja, na mesma sala, andar ou prédio, interligados por meio de conexões de alta velocidade e de interfaces de fibra ótica, ou mesmo, conexões *Gigabit Ethernet* baseadas em pares metálicos.

Quando os projetos se tornam mais complexos e a necessidade de computação é muito elevada, seja pela quantidade de dados a serem analisados e processados ou pela complexidade de cálculos a serem realizados, surge a necessidade de aumentar ainda mais a capacidade computacional dos *Clusters*.

A seguir, acompanhe uma situação que ocorreu no Projeto SETI - *Search for Extra-Terrestrial Intelligence*.



CASOS E RELATOS

O Projeto SETI

Um *Cluster* com milhares de computadores ao redor do mundo foi utilizado para processar sinais captados dos radiotelescópios, na tentativa de identificação de sinais oriundos de vida extraterrestre. O projeto SETI – Pesquisa por Inteligência Extraterrestre - ajudou muito na melhora dos algoritmos usados para processamento distribuído, entretanto, nenhum sinal inteligente ainda foi captado. O filme *Contato*, baseado no livro de Carl Seagan, mostrou um pouco dos objetivos deste projeto.

A interligação de *Clusters* forma um novo conceito, denominado *Grid*. Uma *Grid*, ou Grade Computacional, é formada por um conjunto de computadores locais ou remotos, executando uma tarefa comum, geralmente distribuída por algum nó (computador) principal dentro da grade. Na figura seguinte, você poderá verificar uma classificação geral dos sistemas com múltiplos processadores.

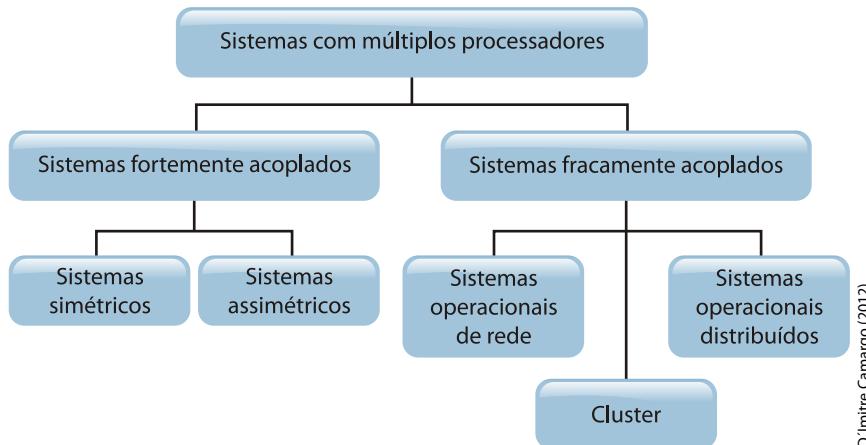


Figura 4 - Diagrama de Multiprocessadores
Fonte: Adaptado de Machado e Maia (1997)



RECAPITULANDO

Viu quanta informação importante você acabou de conhecer? Nesta primeira parte do livro didático, você viu conceitos sobre multiprocessamento e multitarefa, além de saber que os microprocessadores podem implementar, na prática, estes conceitos. Também conheceu exemplos de sistemas aplicados aos conceitos estudados, como o *Cluster* computacional.

Os estudos apresentados neste capítulo são importantes para você entender e determinar um tipo de processador que pode atender os requisitos para um servidor de rede com multiprocessamento. Portanto, sempre que julgar necessário volte ao estudo do capítulo. Um bom exercício para sua aprendizagem também poderá ser o diálogo entre colegas e seu professor. Quanto mais você conversar sobre o que aprende maior será o domínio sobre o assunto.

Anotações:

Multiusuário e Multitarefa

3



Depois de estudar multiprocessamento, chegou o momento de conhecer o multiusuário e a multitarefa. Neste capítulo, você conhecerá os conceitos sobre um sistema computacional com recursos para suporte a usuários e tarefas, em que serão apresentados os conceitos sobre os sistemas que envolvem ambos. Você verá também conteúdos sobre os servidores de rede com capacidade para multiusuário e multitarefas, e os sistemas operacionais com suporte para ambos.

E ao final deste aprendizado, você terá subsídios para:

- a) compreender o que é um sistema multitarefa;
- b) compreender o que é um sistema multiusuário;
- c) compreender e entender sobre os servidores de rede multiusuário e multitarefa;
- d) entender os conceitos necessários de um sistema operacional multiusuário e multitarefas.

Preparado para mais uma jornada de novos saberes? Atente para os detalhes destacados neste conteúdo e procure fazer a conexão com os conceitos vistos no capítulo anterior, porque cada informação se relaciona com a outra. Em frente!

3.1 SISTEMAS MULTITAREFA

Agora que você já conhece as características dos microprocessadores, perceberá que do ponto de vista da arquitetura de computadores e, logicamente, dos servidores de rede, há plena capacidade para execução simultânea de várias tarefas. Entretanto, para que um sistema seja multiusuário não basta apenas o *hardware*, mas também o *software*. Neste caso, trata-se do ‘sistema operacional’.

Você sabe o que faz um sistema operacional multitarefa?

Um sistema operacional multitarefa é todo sistema que permite a execução de várias tarefas simultaneamente, ou seja, é o sistema operacional que possibilita que você possa executar um processador de textos, um navegador web e também escutar música, tudo ao mesmo tempo.



Independentemente de se ter um *hardware* com várias CPUs ou, simplesmente, um único processador, a capacidade de multitarefa é uma responsabilidade do sistema operacional. Vale lembrar que até pouco tempo atrás não havia CPUs com diversos núcleos, mas ainda assim, era possível a execução de várias tarefas no computador. Sistemas como o Windows 98, Windows XP, Windows NT Workstation, GNU/Linux, Unix, MacOS, dentre outros, já suportavam a execução de multitarefas.



Ingram Publishing ([20-7])

Com o advento das CPUs de vários núcleos, a multitarefa ficou ainda melhor, pois podemos ter o benefício extra do processamento paralelo, onde cada tarefa (por exemplo, um processador de textos e um navegador web), pode ser executada paralelamente, um em cada 16PU.

Todos os sistemas operacionais modernos, como o Windows Seven, Windows Server 2008, além de todos os GNU/Linux, Unix, MacOS, dentre outros, suportam a execução de múltiplas tarefas simultaneamente. Mais recentemente, temos até

sistemas para *smartphones*, como o Symbian, por exemplo, que também permitem a execução multitarefa.

3.2 SISTEMAS MULTIUusuÁRIO

Um sistema operacional multiusuário é todo sistema que permite o uso compartilhado do computador por dois ou mais usuários. Este tipo de sistema deve controlar o compartilhamento de recursos entre os usuários, não permitindo que um usuário interfira nas atividades dos demais e controlando, principalmente, o uso da memória, gerenciamento de arquivos em disco e dos processos individuais de cada usuário.

Logicamente, se o computador possui uma ou mais CPUs e estas possuem dois ou mais núcleos, o processamento de todas as tarefas geradas pelos usuários simultâneos no sistema fica mais facilitado e, certamente, um sistema com esta característica deverá possuir melhor *performance* que um sistema com uma única CPU.

É necessário você saber que há uma distinção entre um sistema multiusuário e um sistema multitarefa de um único usuário. Um sistema multiusuário é também um sistema multitarefa, porém há sistemas que são multitarefas, mas não suportam vários usuários simultâneos, como os sistemas executados em computadores do tipo *Desktop*, como o Windows XP, Vista e Seven e os sistemas para *smartphones*.

A característica de uso simultâneo de um computador por vários usuários é uma função quase que obrigatória para os sistemas operacionais de rede. Os sistemas operacionais de rede implementam e possibilitam a característica de acesso multiusuário, em que os acessos ao servidor, por exemplo, podem ser realizados diretamente via um terminal/*console*, ou também remotamente, através de sessões de terminal remota.

É importante citar os softwares emuladores de terminais remotos, como o x3270, que simula um terminal IBM 3270; o ssh em ambiente GNU/Linux, que permite abertura de sessões remotas em servidores GNU/Linux e Unix; e também o software *Remote Desktop Client*, o qual permite a abertura de sessões remotas de terminal em servidores Windows.

É possível também abrir sessões remotas de terminal gráfico Xwindow em servidores GNU/Linux, diretamente de uma estação de trabalho executando GNU/Linux, ou então, por meio de uma estação Windows, utilizando-se, por exemplo, o Software VNC.

Em todos os casos, é importante que o sistema que se deseja conectar em acesso remoto seja gráfico ou em modo caractere, possua suporte para acesso

simultâneo de vários usuários, ou seja, que este tenha características de um suporte operacional multusuário.

**FIQUE
ALERTA**

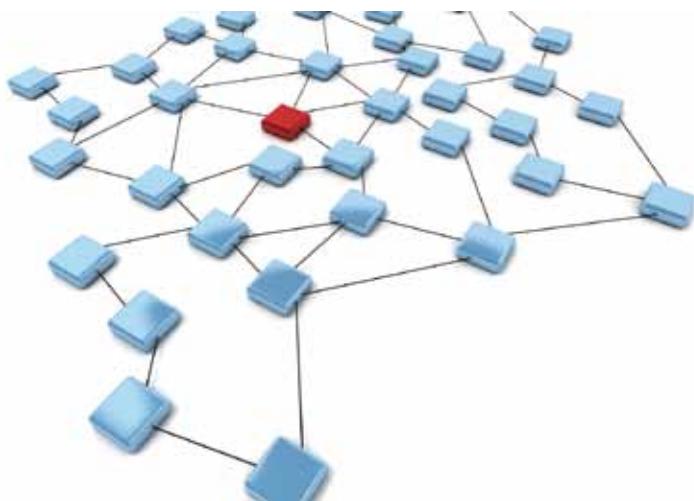
Ao especificar um servidor de rede para trabalhos com multitarefa e multusuário, tenha em mente que estas duas características juntas exigem muito processamento.

Para a situação que você acabou de conhecer, se o servidor de rede precisar ser acessado simultaneamente por vários usuários com sessão interativa (tipo terminal remoto ou cliente gráfico remoto como o VNC ou Rdesktop), este servidor precisará de *hardware* adequado, tipicamente com maior quantidade de memória do que o habitual para um servidor comum. Nesse caso, as especificações corretas devem ser levantadas de acordo com a estimativa de usuários que irão utilizar o servidor de forma interativa e também quais programas serão executados.

3.3 SERVIDORES DE REDE MULTIUusuÁRIO E MULTITAREFA

Servidores de Rede são sistemas computacionais que disponibilizam serviços a usuários ou sistemas, por meio de uma rede de computadores. Este tipo de equipamento exige uma especialização no seu *hardware*, pois em virtude dos serviços que fornece, precisa garantir um mínimo de estabilidade, *performance*, segurança e disponibilidade.

Sem um *hardware* adequado, não há como garantir serviços numa rede de computadores, pois por melhor que seja o sistema operacional de um servidor de rede, o sistema não conseguirá manter níveis de confiabilidade, *performance* e disponibilidade, sem que o *hardware* tenha características para atendimento destes requisitos.



iStockphoto (20-71)

A rigor, para servidores de rede é importante que o *hardware* (para este tipo de equipamento) tenha, no mínimo, as seguintes características:

- a) fonte de alimentação redundante;
- b) controladora de disco rígido com suporte mínimo ao RAID 1;
- c) duas interfaces de rede;
- d) dois discos rígidos;
- e) processadores com dois ou mais núcleos ou, no mínimo, duas CPUs físicas e de acordo com a carga de serviços a que se destina o equipamento;
- f) memória RAM adequada ao sistema operacional de rede e aos softwares que estarão instalados no servidor;
- g) garantia de peças ou de suporte do fabricante.

As características que você acabou de conhecer representam os recursos mínimos de *hardware* que um servidor de rede precisa possuir. É muito comum encontrar servidores de rede instalados em *hardwares* do tipo *Desktop* sem nenhuma redundância de *hardware* ou, até mesmo, instalados em ambientes totalmente irregulares e sem o mínimo de controle de acesso e de condições físicas e ambientais.

Existem diversos tipos de *hardware* para servidores de rede, desde simples servidores com redundância mínima, até superservidores de rede, com características de *mainframe* ou supercomputador. Entretanto, a grande dificuldade está na definição de qual servidor de rede é o mais adequado aos propósitos que você definiu previamente, os quais ele deverá atender.

É comum encontrar servidores de rede superdimensionados para as atividades que estão executando, ou então, servidores recentemente instalados e que já se encontram sobrecarregados, pois o dimensionamento da carga de serviços foi

¹ FASTETHERNET

Protocolo de rede local que possibilita sinalização de até 100 Megabits por segundo em modo Full-Duplex, ou seja, transmissão e recepção ao mesmo tempo. É implementado em hardware, na interface de rede.

incorretamente executado e agora o servidor não consegue atender os usuários e sistemas de forma satisfatória.

**VOCÊ SABIA?**

Nos ambientes de rede empresariais, os servidores de rede são utilizados para quase todo tipo de tarefa, como: servidor de arquivos, servidor de impressão, servidor web, servidor de aplicação e servidor de banco de dados.

² GIGABITETHERNET

Protocolo de rede local que possibilita sinalização de 1 à 10 Gigabits por segundo em modo Full-Duplex. É implementado em hardware, na interface de rede.

Em algumas empresas, dependendo do porte delas, é possível encontrar servidores realizando atividades diversas, para as quais ele não possui um *hardware* corretamente dimensionado. Deste modo, fica claro que nestes servidores é comum ocorrer algum tipo de problema em alguns dos serviços prestados.

Acompanhe um fato histórico no caso a seguir.

**CASOS E RELATOS**

Computadores de 80

No final da década de 80, existiam no Brasil computadores denominados de supermicros. Eles realizavam processamento como se fossem um computador multiusuário e multitarefa. Na verdade eles conseguiam isso porque, para cada usuário conectado havia uma placa interna na máquina com CPU e memória dedicados, atendendo até 4 conexões de terminais. Nestes sistemas, o disco rígido era compartilhado por todas as CPUs internas e em cada uma delas um sistema operacional, do tipo DOS multiusuário era executado. Tinha-se a impressão de um único computador processando, mas na verdade eram vários.



iStockphoto (20-71)

No contexto dos principais serviços realizados por servidores de rede, é possível apresentar alguns requisitos e características mínimas de *hardware* e *software* que estes equipamentos devem possuir. Deste modo, ao analisar os requisitos para um determinado serviço, será possível verificar o tipo de *hardware* mais adequado para o servidor que irá atender determinado serviço, ou serviços.

Atualmente, como as arquiteturas de computadores para servidores de rede estão muito avançadas, equipamentos hoje disponíveis e classificados como **servidores de baixa especialização de hardware** (*low end*), conseguem atender diversos serviços de rede ao mesmo tempo.

Tabela 1 - Serviços de Rede x Hardware Mínimo

SERVIÇO DE REDE	HARDWARE/SOFTWARE MÍNIMOS
Compartilhamento de arquivos	<ul style="list-style-type: none"> • 2 Interfaces de rede FastEthernet¹ ou GigaBitEthernet²; • 2 Unidades de disco rígido; • controladora de disco com <i>Raid 1</i>, ou 5 ou 6; • processador com 2 ou mais núcleos; • memória RAM mínima de 4 Gigabytes; • 1 Unidade Gravadora de DVD ou unidade de Fita DAT, AIT, DLT para <i>backup</i> de dados; • sistema Operacional de Rede.
Servidor de Impressão	<ul style="list-style-type: none"> • 2 Interfaces de rede FastEthernet ou GigaBitEthernet; • 2 Unidades de disco rígido; • controladora de disco com <i>Raid 1</i>, 5 ou 6; • processador com 2 ou mais núcleos; • memória RAM mínima de 4 Gigabytes; • Sistema Operacional de Rede.

³ SCSI

Small Computer System Interface, ou Interface de Sistema para Computadores Pequenos, é uma interface de comunicação paralela que permite a conexão de vários dispositivos como discos rígidos, CD-ROM e scanner com o computador. Devido ao seu preço, esta interface não era comum em computadores pessoais. Somente em servidores de rede é que estas interfaces foram muito utilizadas. Atualmente, esta tecnologia está em fase de transição para um novo modelo denominado SAS.

⁴ SAS

Serial Attached SCSI ou SCSI anexado Serial é uma interface e protocolo de gerenciamento e armazenamento de dados. Representa uma melhora na tecnologia SATA, onde foi baseado. O SAS é um barramento serial mais versátil, rápido e confiável que o antigo SCSI, no qual, inicialmente, possuía taxas de transferência de até 300MB/s e, atualmente, as taxas atingem 1200MB/s. Esta interface possibilita ligar os HDs com extensores a uma única porta SAS.

⁵ SATA

Serial ATA. É uma interface serial de comunicação para transferência de dados de dispositivos de armazenamento, como discos rígidos e discos ópticos. Atualmente é quase um padrão de interface para discos rígidos em computadores pessoais. Existem três padrões para esta interface: o SATA 150, que possui capacidade para transmissão de 1.5 Gigabit por segundo; o SATA 300, com capacidade para transmissão de 3.0 Gigabit por segundo; e uma versão SATA 600, ainda em desenvolvimento, a qual poderá transmitir dados até 6.0 Gigabit por segundo.

Servidor WEB (sem aplicação Java ou Aspx)	<ul style="list-style-type: none"> • fonte redundante; • 2 Interfaces de rede FastEthernet ou GigaBitEthernet; • 2 Unidades de disco rígido; • controladora de disco com <i>Raid</i> 1, 5 ou 6; • processador com 2 ou mais núcleos, ou 2 ou mais processadores (CPU); • memória RAM mínima de 4 Gigabytes ou maior, dependendo do número de sites/portais e de acessos simultâneos; • 1 Unidade Gravadora de DVD ou unidade de Fita DAT, AIT, DLT para <i>backup</i> de dados; • Sistema Operacional de Rede.
Servidor de Aplicação (Java - dependendo do porte - ou Aspx)	<ul style="list-style-type: none"> • fonte redundante; • 2 Interfaces de rede FastEthernet ou GigaBitEthernet; • 2 ou 3 Unidades de disco rígido; • controladora de disco com <i>Raid</i> 1, ou 5 ou 6, recomendável <i>Raid</i> 5 ou 6; • processador com 2 ou mais núcleos ou 2 ou mais processadores (CPU); • memória RAM mínima de 8 Gigabytes ou maior, dependendo do número de sistemas instalados ou do número de acessos simultâneos; • 1 Unidade Gravadora de DVD ou unidade de Fita DAT, AIT, DLT para <i>backup</i> de dados; • Sistema Operacional de Rede.
Servidor de Banco de Dados	<ul style="list-style-type: none"> • fonte redundante; • 2 Interfaces de rede FastEthernet ou GigaBitEthernet; • 2 ou 3 Unidades de disco rígido; • controladora de disco com <i>Raid</i> 1, ou 5 ou 6, recomendável <i>Raid</i> 5 ou 6; • processador com 2 ou mais núcleos, ou 2 ou mais processadores (CPU); • memória RAM mínima de 8 Gigabytes ou maior, dependendo do número de acessos simultâneos; • 1 Unidade Gravadora de DVD ou unidade de Fita DAT, AIT, DLT para <i>backup</i> de dados; • Sistema Operacional de Rede.

Com relação à tabela que você acabou de conferir, é necessário apontar algumas considerações, principalmente com relação aos critérios de seleção de um tipo de *hardware* para outro e também com relação ao serviço de rede.

Alguns serviços de rede não são tão importantes, como por exemplo, os serviços de impressão e compartilhamento de arquivos, pois estes serviços podem ser restaurados/ recuperados em minutos ou, talvez, em algumas horas. Em todos os casos, o impacto para os usuários é contornável.

**SAIBA
MAIS**

Confira os sites dos principais fabricantes de servidores de rede, e veja os sistemas atuais com capacidades multiusuário e multitarefa. Para isso acesse:

<<http://www.ibm.com.br>>

<<http://www.hp.com.br>>

<<http://www.dell.com.br>>

Os servidores de Rede que executam serviços web, aplicações de rede ou de banco de dados necessitam fortemente de redundância no *hardware*. A redundância no *hardware* está atendida com a especificação da fonte redundante, a qual, em caso de queima de uma unidade, a outra automaticamente assume o seu papel. No caso da ligação de cada fonte de alimentação em uma fonte de energia diferente, por exemplo, uma fonte conectada num estabilizador e outra conectada num sistema de *No-break* ou *Short Break*, o servidor continuará funcionando mesmo que a energia da concessionária seja interrompida.

As interfaces de rede também atendem aos quesitos de redundância, pois deve haver, no mínimo, duas interfaces de rede por servidor. Neste caso, especificamente, há sistemas operacionais de rede que permitem a otimização destas interfaces, permitindo que as duas funcionem simultaneamente, balanceando a carga de conexões e acessos entre elas. Em uma situação em que uma destas interfaces deve ficar inativa, o tráfego automaticamente é redirecionado para a interface restante.

**FIQUE
ALERTA**

No caso de interfaces configuradas para uso simultâneo e balanceado, as conexões externas preferencialmente devem ser realizadas em *switchs* de rede distintos, pois as duas interfaces de rede são conectadas em um único *switch*. Caso o *switch* queime ou apresente problemas, a redundância destas interfaces de rede não adiantaria em nada.

O tipo de abordagem apresentado no Alerta que você acabou de verificar é conhecido como **Ether-Channel** e está disponível nos sistemas GNU/Linux.

Nos requisitos de redundância de discos rígidos, optou-se por definir um mínimo de segurança para um servidor de rede, o que, no caso, está atendido pelo espelhamento de discos realizado pela controlada *Raid* (*Redundant Array of Inexpensive Disk*) com *Raid 1, 5 ou 6*.

Você já sabia o que é *Raid*? Já conhecia o *Raid 1,5 e 6*? A seguir, veja quais são as características de cada um.

Raid 1	É a implementação no <i>hardware</i> do espelhamento de disco (<i>mirror</i>) em que tudo que é gravado num disco, a controladora <i>Raid</i> grava no outro. Deste modo, em caso de perda de um dos discos, o outro poderá ser utilizado.
Raid 5	É uma situação ideal para muitos serviços de rede, pois a perda por agregação de discos físicos é menor que no <i>Raid 1</i> . Porém, para implementar um <i>Raid 5</i> é preciso, no mínimo, 3 discos rígidos, em que um deles será utilizado para armazenar a paridade dos dados. No caso de perda de um dos discos, a controladora reconstrói a informação a partir do disco de paridade e o sistema continua funcionando corretamente, como se nada tivesse ocorrido.
Raid 6	É um nível de redundância de discos mais especializado e mais atual. O problema desta implementação física de redundância é que as controladoras <i>Raid</i> disponíveis no mercado não possuem um custo razoável. Outro fator contra a sua adoção em servidores de rede menos especializados é que as controladoras disponíveis para o <i>Raid 6</i> somente implementam o recurso em discos tipo SCSI ³ ou SAS ⁴ , muitas vezes não possibilitando de utilizar discos SATA ⁵ II ou SATA III, os quais possuem <i>performance</i> semelhante aos discos SCSI ou SAS, porém possuindo um custo mais baixo.

Quadro 2 - Tipos de *Raid*

Os requisitos de processadores e memória levam em conta que serviços de rede que possuem interação em nível de sessão de usuário (como uma aplicação Java ou ASPx, ou ainda, num servidor web) necessitam maior capacidade de processamento, nestas situações disponibilizando mais processadores para implementar mais *performance* das aplicações.



VOCÊ SABIA?

Que há uma relação direta entre mais capacidade de processamento e o total de memória RAM disponível, principalmente em servidores que atendem centenas ou milhares de usuários simultâneos?

Quanto mais aplicações poderão ser executadas em paralelo, fruto da adição de mais núcleos ou, até mesmo, de mais CPUs com vários núcleos, mais memória principal será necessária. Logo, devemos sempre pensar que estas duas variáveis devem caminhar juntas, para cima ou para baixo.

A especificação de unidades de fita para realização de *backups* é um requisito básico, pois servidores de rede precisam implementar alguma rotina, cópia de seus dados e, se possível, retirando-os do mesmo ambiente, como fator de proteção em caso de sinistros físicos, tal como um incêndio, inundação ou mesmo roubo de equipamentos. Entretanto, o uso de uma unidade de DVD ou, até mesmo *Blu-Ray*, na execução de *backup* de dados é perfeitamente viável e até mais

barata. No modelo de *backup* em mídia ótica, haverá sempre o inconveniente de ter que controlar uma quantidade maior de mídias de *backup*, pois as unidades de fita conseguem armazenar muito mais dados do que as unidades óticas.

As especificações que você viu até o momento para servidores de redes foram baseadas nos serviços de rede comumente disponíveis nestes tipos de servidores. Logicamente é possível perceber que estes serviços são, em sua essência, serviços para muitos usuários simultâneos, o que nos remete para sistemas operacionais que possuem a capacidade multiusuário e multitarefa, o que veremos a seguir.



VOCÊ SABIA?

Que atualmente todos os microprocessadores comercializados permitem a execução de multitarefa? Os processadores de *smartphones* e, até mesmo, os embutidos em carros, permitem esta façanha.

3.4 SISTEMAS OPERACIONAIS COM SUPORTE A MULTIUusuÁRIOS E MULTITAREFAS

As características de suporte à execução de múltiplas tarefas, bem como de muitos usuários simultâneos, são de responsabilidade do sistema operacional. Logicamente, como já descrito anteriormente, a execução de múltiplas tarefas num servidor de rede deve ser suportada pela CPU do servidor. Como os microprocessadores atuais, em sua maioria, suportam a execução de múltiplas tarefas (processos ou *threads*), os sistemas operacionais já possuem então a arquitetura ideal para prover as capacidades de múltiplos usuários simultâneos e também de múltiplas tarefas.

O suporte multiusuário e multitarefa está disponível em praticamente todos os sistemas operacionais de rede, executados ou não em servidores de rede.

Os principais sistemas operacionais de rede com suporte multiusuário e multitarefa são os seguintes:

- a) GNU/Linux (qualquer distribuição);
- b) Unix da família System V;
- c) Unix da família BSD;
- d) OpenBSD;
- e) FreeBSD;
- f) MaC OS X (multitarefa, mas único usuário simultâneo);

- g) Windows Seven (multitarefa, mas único usuário simultâneo);
- h) Windows 2xxx Server;
- i) Oracle-Sun Solaris;
- j) Oracle-Sun SunOS;
- k) HPUX;
- l) HPOpenVMS;
- m) IBM AIX.



RECAPITULANDO

No capítulo que você acabou de estudar, conheceu os conceitos que envolvem os sistemas multiusuário e multitarefa. Aprendeu que é fundamental possuir um sistema operacional que suporte múltiplos usuários simultâneos e múltiplas tarefas, bem como ter um *hardware* que possua CPUs com capacidades para isso.

Apesar das arquiteturas de computadores atuais suportarem e implementarem estes conceitos, o correto dimensionamento do *hardware* e do sistema operacional é um fator preponderante para que os sistemas, como um todo, atendam aos usuários. Estes conceitos lhe ajudarão na especificação correta de um sistema computacional com características para multiusuário e multitarefa.

Mas você ainda não estudou sobre arquitetura de *hardware* de servidores, não é mesmo? Prepare-se, pois este será o assunto do próximo capítulo. Acompanhe!

Arquitetura de *Hardware* de Servidores

4



O capítulo que inicia apresentará à você os conceitos sobre o *hardware* de servidores de rede. Nesta parte do livro didático você verá que existem diferenças importantes entre o *hardware* de um servidor de rede e de um computador pessoal de uso geral.

No capítulo 4 serão abordados os conceitos sobre os dispositivos de *hardware* redundantes que os servidores de rede devem possuir. Você conhecerá também as definições sobre os tipos de servidores de rede, classificados sob o conceito de especialização no *hardware*, em que os servidores podem ser classificados como: baixa, média ou alta especialização no *hardware*. Ainda, estudará os conceitos sobre os microprocessadores CISC e RISC, bem como suas diferenças básicas e onde geralmente são empregados.

E ao encerrar este capítulo, você terá subsídios para entender melhor os conceitos sobre a arquitetura de *hardware* de servidores, estando capacitado para:

- a) entender os conceitos básicos sobre o *hardware* de servidores de rede;
- b) compreender o que são os dispositivos de *hardware* redundante;
- c) compreender e entender como os servidores de rede são classificados;
- d) compreender os conceitos sobre os microprocessadores CISC e RISC, entendendo suas diferenças e onde são utilizados.

4.1 HARDWARE DE SERVIDORES DE REDE

Você sabia que um computador que desempenha as funções de um servidor de rede possui a mesma arquitetura funcional que um computador qualquer, como a de um *Desktop*?

Entretanto, o que muda nesta arquitetura são as especializações implementadas em cada componente da arquitetura.

Quer um exemplo?

As controladoras de disco possuem capacidade para *Raid* nos níveis 0, 1, 5, 6 e 10. A quantidade de interfaces de rede é maior, geralmente chegando a 4, 6 ou, até mesmo, 8 interfaces. O número de CPUs disponíveis em servidores de rede, geralmente está na ordem de 4 até 8 em servidores iniciais (*low end*), chegando até 128 ou 256 CPUs em servidores de alta especialização, denominados como servidores *High End*.

Como estes equipamentos possuem, em geral, a mesma arquitetura básica, acompanhe na figura seguinte uma representação da arquitetura de *hardware* de um computador.

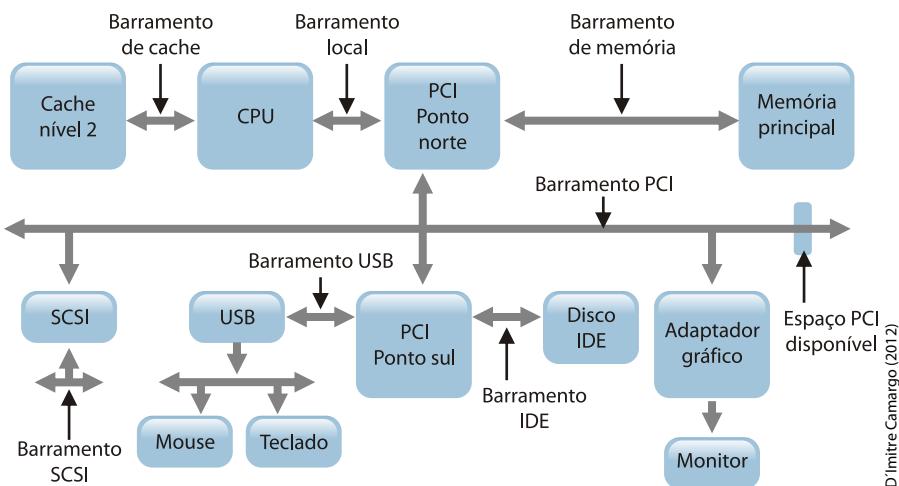


Figura 5 - Arquitetura em Blocos de um Computador
Fonte: Adaptado de Paula (2011)

Dimitri Camargo (2012)

Decorrente da especialização de *hardware* necessária para servidores de rede, a arquitetura anteriormente apresentada é amplamente melhorada, contendo muitos outros componentes e circuitos, pois as redundâncias necessárias no *hardware* devem também estar implementadas no nível do projeto.

Na figura a seguir, veja uma placa-mãe para um servidor de rede, a qual possui a capacidade para duas CPUs físicas.



Figura 6 - Placa-mãe para 2 Processadores

A figura que você verá a seguir mostra outro exemplo de *hardware* para servidor de rede, na qual é possível visualizar vários componentes importantes, dentre eles, a fonte redundante, que fica disposta no lado direito da figura.



Figura 7 - Hardware de Servidor

Você deve ter observado, na última figura, que há redundâncias de ventiladores internos, vários *slots* para pentes de memória e dissipadores de calor, os quais são tipicamente utilizados sobre *chipsets* de controle de barramentos, como o PCI, por exemplo.

4.2 DISPOSITIVOS DE *HARDWARE* REDUNDANTES

Em virtude da importância dos serviços instalados em servidores de rede, este tipo de computador precisa ter características especiais, além dos itens como CPU, memória e quantidade de espaço em disco.



**FIQUE
ALERTA**

Servidores de rede necessitam de dispositivos redundantes, ou seja, dispositivos que trabalham em paralelo, onde em caso de uma parada em um deles, o outro continua trabalhando normalmente. Quando isso acontece, o usuário do servidor de rede muitas vezes nem percebe que um problema ocorreu no servidor.

A quantidade de dispositivos redundantes num servidor de rede, de certa forma, está relacionada com o valor do equipamento. A implementação de dispositivos de *hardware* redundante exige projetos específicos, componentes mais especializados e uma engenharia de projeto bem definida. Essas características especiais tornam o produto final mais caro, porém muito melhor.

Apesar dos preços mais elevados, é possível obter servidores de rede com alguns componentes redundantes e que não tornam o servidor de rede muito mais caro. Certos componentes como discos rígidos, interfaces de rede, controladoras de discos, por exemplo, podem ser adquiridos separadamente, compondo assim um servidor com algum nível de redundância.

No quadro a seguir, você conhecerá os dispositivos de *hardware* que podem ser encontrados em servidores de rede, contendo redundância. Esses dispositivos nem sempre estão presentes em todos os servidores. Entretanto, quanto mais dispositivos de *hardware* redundantes num servidor de rede, mais seguro é o equipamento e também, mais caro.

DISPOSITIVO REDUNDANTE	CARACTERÍSTICAS
Discos Rígidos	<p>Unidades de discos rígidos são os principais dispositivos de servidores de rede que necessitam ser redundantes, ou seja, para um servidor de rede é imperativo que o mesmo tenha, no mínimo, duas unidades de disco.</p> <p>Conforme descrito no item anterior, há diversos tipos de controladoras de disco, sendo uma para cada tipo de disco. Deste modo, precisamos de discos rígidos fabricados de acordo com a controladora de discos do servidor. Se o servidor contiver controladoras de disco SATA, teremos que usar discos SATA; se contiver controladoras de disco SAS, poderemos usar discos SAS ou então SATA; e assim por diante.</p> <p>Entretanto, a redundância nos discos rígidos não depende somente de possuir mais discos, mas também da controladora de discos e do sistema operacional do servidor.</p> <p>A redundância de discos deve ser implementada, sempre que possível, via <i>hardware</i>, através da controladora de discos, a qual deve implementar algum nível de <i>RAID</i> (0, 1, 5, 6 ou 10).</p> <p>Deste modo, para implementar uma redundância mínima de discos, com dois discos, podemos obter o nível <i>RAID</i> 1 – ‘Espelhamento’, onde os dados são duplicados do disco principal para o espelho (mirror). Neste modelo, o sistema operacional irá enxergar somente um único disco. A outra unidade fica com acesso somente da controladora de discos, mas poderá ser utilizado em caso de pane da primeira unidade.</p> <p>Se estiverem disponíveis três discos rígidos ou mais, poderá ser implementado o <i>RAID</i> 5, sendo que, neste modelo, um dos discos do <i>Array</i> (grupo de discos) irá armazenar informações de paridade. No caso de perda de um dos discos, o disco de paridade é utilizado para a reconstrução da informação, sem perda de dados. Um modelo mais seguro de redundância de discos é o <i>RAID</i> 6. Neste modelo é preciso cinco discos, no qual dois discos serão utilizados para armazenamento de paridade.</p> <p>As unidades de discos podem possuir uma característica muito importante que é a capacidade de troca à quente, ou seja, estes discos podem ser removidos do servidor com este ainda ligado. O nome desta característica de troca à quente é denominado de <i>Hot Swap</i>. Unidades de discos com esta capacidade são, em geral, bem mais caras que discos convencionais, comparando-se discos de mesma tecnologia e capacidade de armazenamento.</p>
Interfaces de rede	<p>As interfaces de rede, ou comumente chamadas de placas de rede, são dispositivos indispensáveis em servidores de rede. Em quase todos os servidores de rede comercializados atualmente existem, no mínimo, duas interfaces instaladas. Em servidores de médio porte e grande porte, há modelos de equipamentos com 8 ou 10 interfaces de rede.</p>

CPU (microprocessador)	Servidores de rede mais especializados podem possuir a redundância de CPU. No caso de parada de uma CPU, as demais continuam funcionando, entretanto, os sistemas operacionais terão que tratar os problemas gerados pelos processos que estavam sendo executados em uma CPU que parou de funcionar, pois a tarefas em execução terão que ser encaminhadas para execução em outra CPU, o que pode causar problemas para os sistemas em execução. Sendo assim, este tipo de redundância é muito importante, porque o servidor poderá ser reiniciado rapidamente, retirando-se ou mesmo inabilitando a CPU com problemas.
------------------------	---

Quadro 3 - Dispositivos de hardware

Como você pôde conferir, os servidores de rede podem possuir diversas opções de *hardware* redundante. E isto, logicamente, ocasiona que para uma quantidade de *hardware* redundante mais elevada, o valor do equipamento também será mais alto. Nesse sentido, é comum, no mercado, as empresas classificarem seus servidores em níveis de *performance* e de redundância.

Você quer um exemplo? então acompanhe a situação descrita em Casos e Relatos.



CASOS E RELATOS

Perda de dois discos num sistema RAID 5

A confiança franca em *hardware* de servidores pode nos levar a problemas sérios. Apesar da confiabilidade dos sistemas de discos redundantes com a implementação de um *RAID* nível 5, apresento o relato do problema em um servidor que tinha um sistema com 4 (quatro) discos rígidos em *RAID* 5. Este sistema suporta a perda de até um disco, sem problemas. Aconteceu então que, num certo dia, dois discos rígidos pararam de funcionar. Deste modo, não há sistema de redundância de discos de aguente. Como resultado, foram mais de dois meses tentando restaurar mais de 50 Gigabytes de dados perdidos dos usuários, dos quais não se tinha um *backup* completo. Então, devemos sempre utilizar, em sistemas críticos, a melhor redundância possível.

4.2.1 SERVIDORES DE REDE COM BAIXA, MÉDIA E ALTA ESPECIALIZAÇÃO HARDWARE

Tipicamente, há três tipos de servidores de rede: os de baixa especialização no *hardware*, denominados *Low End*; os de média especialização, denominados de *Middle End*; e servidores com alta especialização no *hardware*, denominados *High End*.

Baixa = *Low End*

Média = *Middle End*

Alta = *High End*

Figura 8 - Tipos de servidores

D'Imitre Camargo (2012)

Saiba com mais detalhes as características de cada um.

Servidores Low End, com baixa especialização no *hardware*, possuem geralmente duas interfaces de rede, dois discos SATA, uma CPU e memória RAM entre 4 e 8 Gigabytes. Estes servidores possuem custo normalmente um pouco acima de um microcomputador comum, tipo *Desktop*, porém o seu *hardware* possibilita um incremento de dispositivos que objetivam a melhoria das características do equipamento, concedendo ao mesmo, maior especialização.

Em servidores desta natureza, muitas vezes, é possível adicionar mais discos rígidos, interfaces de rede e memória RAM. Dependendo do fabricante, também é possível adicionar mais uma CPU para processamento ou então permitir a troca da CPU por um modelo mais rápido.



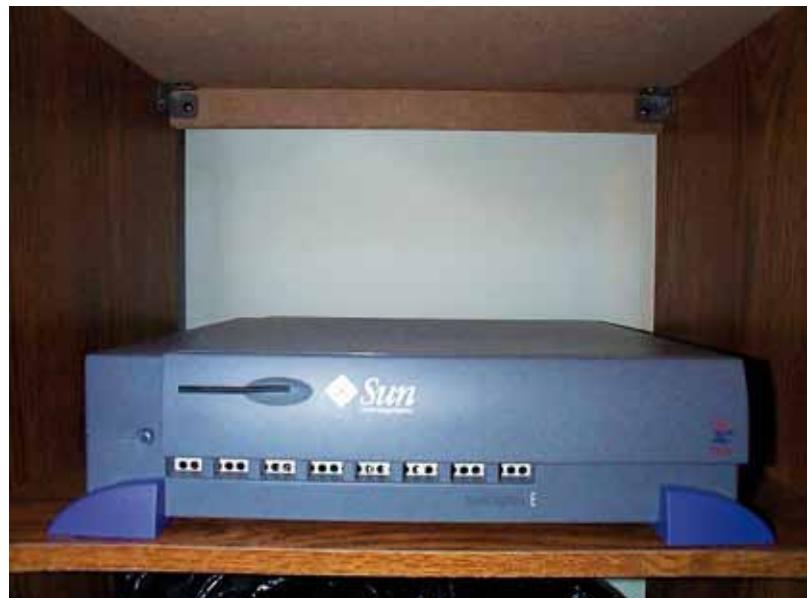
Figura 9 - Servidor Low-End

Anandtech (20-?)

Servidores Middle End, com média especialização no *hardware*, são muitas vezes chamados de *Middle End ou Midrange Servers*. Estes equipamentos possuem, em geral, muitos dispositivos redundantes de *hardware*. Dentre estes dispositivos estão:

- a) fontes redundantes de alimentação;
- b) duas ou mais interfaces de rede;
- c) discos rígidos com tecnologia SAS ou SCSI e com tecnologia Hot Swap (discos que podem ser substituídos com o servidor ligado).

Além destas características de redundância, estes servidores geralmente possuem de dois (2) a oito (8) processadores e de 8 a 32 Gigabytes de memória RAM.



Robert S. Dubinski ([20-?])

Figura 10 - Servidor Low-End Sun

Muitos modelos de servidores de rede com média especialização no *hardware* possuem também gabinetes que possibilitam a inserção de mais CPUs e unidades de discos rígidos. Outra característica importante destes servidores é que atualmente no mercado existem modelos destes servidores que são fabricados para montagem em *rack*, ou também construídos para uso da tecnologia *Blade*.

Mas que tecnologia é essa?

A tecnologia *Blade* é uma arquitetura de construção de servidores de rede, a qual possibilita uma alta densidade de servidores num único gabinete ou chassis, compartilhando os recursos comuns como Conectividade de Redes e Conexões para interfaces de Fibra (*Fiber Channel*), utilizadas por discos SAS ou SCSI, alimentação elétrica, ventilação e gerência centralizada.

**VOÇÊ SABIA?**

Que a tecnologia *Blade* foi desenvolvida e implementada comercialmente em 2001, por Christopher Hipp e Kirkeby David e, posteriormente, em 2005, foi adquirida pela Hewlett Packard (HP)? Atualmente, diversas empresas possuem linhas de servidores *Blade* comercializadas, dentre elas: IBM, HP, Dell e Cisco.

A figura que você verá a seguir apresenta um chassis contendo servidores *Blade*, em que é possível perceber a alta densidade de servidores instalados. Neste modelo você observará uma lâmina de servidor desconectada do barramento. Há também neste chassis, unidades de discos rígidos e outros conectores de rede e de gerência.



Senetic (20-?)

Figura 11 - Chassi de Servidores Blade

Já na figura seguinte, você poderá visualizar um cartão de servidor *Blade* da HP, em que é possível ver a alta densidade dos componentes internos de um servidor de rede. Este modelo é ainda menor do que o apresentado na figura anterior.



V3 {[20-?])

Figura 12 - Cartão Blade Server da HP

De outra forma e para que o leitor possa comparar as vantagens da tecnologia *Blade*, na figura 11 podemos ver um *rack* contendo alguns servidores de rede, onde é visível a quantidade de cabos e conectores necessários para manter este ambiente.



RV Cabeamento Estruturado {[20-?])

Figura 13 - Rack com Servidores e Cabos

Por ser uma tecnologia com custo mais elevado, a tecnologia *Blade* é mais utilizada em *Datacenters*, onde a quantidade de servidores de rede é um requisito fundamental e o espaço nesses ambientes é um artigo que vale ouro. Logo, o emprego dessa tecnologia torna-se um requisito indispensável.

**SAIBA
MAIS**

Para saber outras informações e detalhes sobre a tecnologia *Blade*, acesse os seguintes endereços:

<http://www.ibm.com/br/systems/bladecenter/blade_servers/index.phtml>;

<http://it.wikipedia.org/wiki/Blade_server>.

Servidores High End, com alta especialização no *hardware*, denominados de *High End Servers*, podem possuir literalmente quase todos os seus componentes redundantes. Geralmente estes servidores, além das características de redundância, possuem um elevado poder computacional, em muitos casos, chegando aos patamares do poder computacional de computadores de grande porte (*mainframes*).

Nesta linha de servidores, com alta especialização de *hardware*, estão disponíveis duas ramificações de processadores, nas quais é possível encontrar equipamentos com grande capacidade computacional.

Como modelo desses processadores temos os da família x86, comercializados principalmente pela Intel e AMD. Outro modelo de processador que pode ser citado é aquele com tecnologia RISC – *Reduced Instruction Set Computer* (Computador com Conjunto Reduzido de Instruções).

Na figura seguinte, você verá um servidor DELL que possui capacidade para até 4 processadores Intel com 8 núcleos internos, perfazendo um total de 32 CPUs num único servidor de *rack*. Este servidor também suporta até 1 Terabyte de memória RAM e possui outros dispositivos avançados, como discos SSD (*Solid State Disk* ou Disco de Estado Sólido), fontes redundantes, interfaces de rede *on-board* com quatro (4) saídas, dentre outras características.



Used Servers (10-?)

Figura 14 - Servidor de Rack da Dell

Expandindo ainda mais as características de um servidor de alta especialização no *hardware* e alta performance computacional, na figura a seguir, você conhecerá um servidor *IBM System p5 595*, o qual possibilita o uso de 64 CPUS *IBM Power*, que são processadores produzidos pela própria IBM e utilizam a tecnologia RISC.



Figura 15 - Super Servidor IBM System P5

Como já apresentado, este tipo de servidor possui *performance* compatível com computadores de grande porte, sendo utilizados para aplicações de missão crítica, de alta disponibilidade e/ou com grande risco financeiro, em que, neste caso, os valores justificam os investimentos em equipamento desta magnitude.

Neste modelo específico pode-se chegar a até 2 Terabytes de memória RAM e executar sistemas operacionais como o *Red Hat Enterprise Linux* ou o sistema *Unix* da IBM, denominado AIX.

4.2.2 MICROPROCESSADORES CISC E RISC



VOCÊ
SABIA?

Que os microprocessadores trabalham executando instruções programadas pelos programas em execução?

Sim. Um programa de computador é uma sequência lógica de comandos que instrui o microprocessador (CPU) a fazer alguma coisa. A linguagem que os microprocessadores conhecem é a linguagem da máquina, também conhecida como linguagem de montagem ou *Assembly*.

Deste modo, todos os programas são, de uma forma ou de outra, traduzidos para uma linguagem de máquina para que os microprocessadores possam entender os comandos e executá-los. O processo de conversão de uma linguagem de programação de alto nível (como Java ou C) para uma linguagem de máquina é denominado ‘compilação’.

Durante o processo de compilação, os comandos são traduzidos pelo compilador para a linguagem de máquina adequada ao microprocessador em que o programa será executado. Como você pode perceber, há uma vinculação no processo de compilação com o microprocessador que será usado para executar o programa.

Desta forma, não é possível compilar um programa para que seja executado em qualquer microprocessador, pois as linguagens de máquina dos microprocessadores são diferentes. De uma maneira geral, os microprocessadores falam línguas diferentes internamente, e para que possamos fazê-los trabalhar corretamente, é preciso falar sua língua nativa, ou seja, é necessário compilar os programas utilizando compiladores específicos para cada microprocessador (CPU).



FIQUE ALERTA

Conforme apresentado, os sistemas operacionais, aplicativos e programas que são compilados para os microprocessadores RISC não funcionariam em computadores que utilizam microprocessadores com tecnologia CISC. Para isso ocorrer, é preciso que os sistemas sejam recompilados na outra plataforma, ou seja, você deve saber adequar os softwares para cada tipo de arquitetura de computador que vai utilizar. Assim, se você possui ou administra um servidor com microprocessador RISC, deverá somente utilizar um software compilado para esta arquitetura.

Neste sentido, é possível apresentar à você os conceitos que envolvem as famílias de microprocessadores CISC e RISC. Acompanhe uma breve história no Casos e Relatos a seguir.



CASOS E RELATOS

A descoberta de Cocke

Em meados dos anos 70, o cientista John Cocke, da IBM, descobriu, por meio de estudos e pesquisas, que a maior parte dos programas utilizava

um conjunto muito pequeno de instruções dos microprocessadores, ou seja, os programas subutilizavam os recursos disponíveis nos microprocessadores. Naquela época, já existiam CPUs com um grande número de instruções, desta maneira, foi proposta a criação de CPUs com um conjunto reduzido de instruções internas. Assim, Cocke originou o termo RISC – *Reduced Instruction Set Computer*, ou computador com um conjunto de instruções reduzidas.

O primeiro projeto prático de uma CPU RISC foi o IBM 801, em 1975. Este microprocessador foi utilizado para tarefas simples dentro de outros computadores IBM e serviu como base para o primeiro processador RISC para um computador pessoal, chamado na época de IBM PC-RT, lançado pela IBM em 1986.

Então, na década de 80 e 90 muitos outros projetos de microprocessadores RISC surgiram, e com isso, vários tipos de microprocessadores RISC estavam disponíveis, tais como: os chips MPS R2000; Sparc, da Sun Microsystems; PowerPC, da IBM, que foram utilizados nos computadores pessoais da Apple, os *Macintosh*.

Por outro lado, os microprocessadores que possuem uma grande quantidade de instruções internas são denominados de microprocessadores CISC – *Complex Instruction Set Computer* ou Computador com Conjunto de Instruções Complexas. Ao possuir um conjunto de instruções complexas, internamente na CPU, os compiladores, ou seja, os programas que fazem a tradução dos comandos das linguagens de programação para linguagem de máquina são mais simples, de forma que estes não têm muito trabalho nesta tradução, pois o microprocessador possui instruções complexas. Esta facilidade dos compiladores resulta em programas menores, ou seja, o total de código gerado na linguagem de máquina (*assembly*) é menor, se formos comparar com o mesmo programa compilado para um microprocessador RISC.

Para possuir instruções complexas dentro do microprocessador, este necessita armazenar estas instruções no que podemos denominar de **microcódigo**, o qual é possível afirmar que é quase que um microprograma dentro da CPU. Microprocessadores RISC não possuem microcódigo e pelo fato de possuírem poucas instruções, também possuem uma complexidade de construção menor, com menos transístores e lógica auxiliar. Com isso, possuem um custo menor.

**SAIBA
MAIS**

Praticamente a maioria dos microcomputadores tipo *Desktop* e dos servidores de rede de baixa especialização de hardware possuem microprocessadores CISC, pois, em geral, utilizam a família de processadores INTEL Pentium ou AMD, já que ambos são CPUs com conjunto de instruções complexas ou CISC.

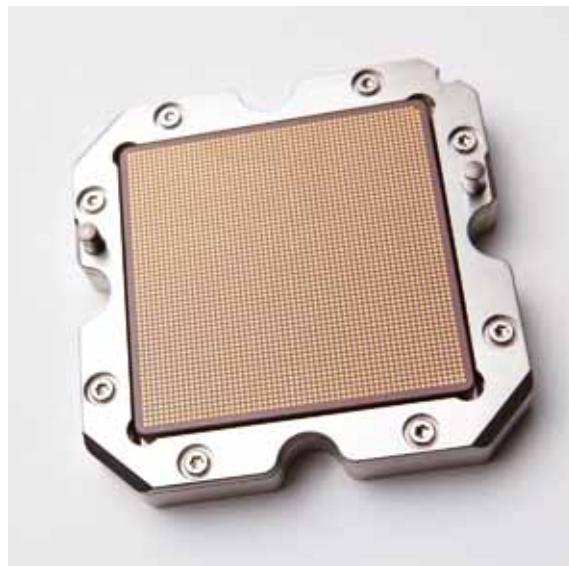
Atualmente, os microprocessadores RISC dominam o mercado de servidores de média e alta capacidade de processamento, em que existem equipamentos com mais de 128 CPUs internas, ou até mais. Muitos processadores RISC estão embutidos em consoles de jogos como o *Playstation*, em smartphones e embarcados em veículos. Os processadores CISC, por sua vez, estão presentes na maioria dos computadores pessoais e em servidores de rede.

**VOCÊ
SABIA?**

Sempre houve muita discussão entre microprocessadores com tecnologia RISC e CISC. Hoje em dia, os conceitos quase que não valem mais, pois ambas utilizam conceitos trocados uma da outra, ou seja, microprocessadores RISC com um número muito grande de instruções, e microprocessadores CISC com instruções mais simples.

Mas há um ponto em que existe alguma convergência. Os processadores RISC possuem ligeira vantagem sobre o processamento de cálculos em ponto flutuante e por isso são muito utilizados em consoles de jogos eletrônicos, como o *Playstation 3*, por exemplo. Aliás, o microprocessador do *Playstation 3* é tão potente que a UFRJ montou um Cluster com 21 consoles do mesmo, executando um sistema Linux e com objetivo de pesquisas na área da dinâmica molecular.

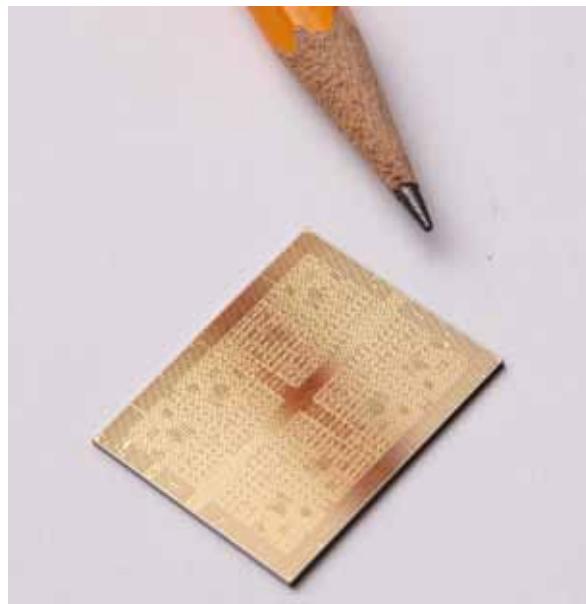
Na figura seguinte, temos a imagem de um microprocessador IBM Power 7, que é uma das CPUs RISC mais avançadas e atualmente equipa os computadores da Linha Power da IBM. Esta CPU é fabricada com tecnologia de 45 nanômetros, possui 1,2 bilhão de transístores e pode rodar com *clock* de até 4,2 Gigahertz. Este simples microprocessador possui 8 núcleos internos (cores).



Oh My Geek ([20-?])

Figura 16 - Microprocessador IBM Power 7

Em termos comparativos, na figura a seguir é possível ter a idéia do tamanho da pastilha interna do microprocessador, comparando-a com um lápis.



Oh My Geek ([20-?])

Figura 17 - Pastilha do Microprocessador IBM Power 7

Os microprocessadores com tecnologia CISC, devido ao grande número de instruções internas, exigem que o tamanho dos mesmos não seja o mesmo dos processadores RISC. Mesmo sendo fabricados com tecnologia em escala nanométrica, seu tamanho não consegue diminuir, por restrições no processo de fabricação e problemas técnicos que envolvem os materiais, dissipação do calor e condução elétrica.

Na próxima figura você verá a imagem de um microprocessador Intel Core i7. Este é um dos mais avançados produzidos com a tecnologia CISC. Por isso, a CPU é construída com processo de fabricação de 32 nanômetros, possui 4 núcleos internos e cada núcleo implementa o conceito de *HyperThread*, permitindo a simulação de mais de uma CPU por núcleo. Deste modo, o sistema operacional irá encontrar 8 CPUs internas, contidas dentro de uma única pastilha física. Além dessas características, diversos avanços no barramento de memória e maior *cache* interno concedem a este microprocessador uma alta capacidade de processamento e de I/O em memória.



Develop3D ([20-7])

Figura 18 - CPU INTEL Core i7

Pesquise nos sites seguintes outros detalhes sobre microprocessadores RISC e CISC:



- <<http://paginas.fe.up.pt/~jcf/ArqCompLEEC/recursos/Risc-Cisc.pdf>>;
- <<http://www.noticiastecnologia.com.br/ibm-anuncia-chip-power-7-e-produzira-o-servidor-por-aqui>>;
- <<http://www.intel.com.br/content/www/br/pt/processors/core/core-i7ee-processor.html>>

Não é possível fazer uma comparação direta entre os microprocessadores RISC e CISC, pois no atual estágio da tecnologia de construção, os fabricantes atuais embutem características de um, dentro do outro. As características dos sistemas que serão utilizados em computadores com microprocessadores RISC ou CISC determinam qual arquitetura deverá ser utilizada. Num cenário científico, por exem-

plo, é quase unânime a utilização de computadores com tecnologia RISC, pela sua melhor capacidade para execução em cálculos e também pela grande densidade de CPUs obtidas e alcançadas comercialmente em equipamentos de fabricantes como IBM, HP e Oracle-Sun.

Por outro lado, aplicações comerciais e de uso geral são quase que totalmente usuárias de processadores com tecnologia CISC da Intel ou AMD.

É importante saber que para cada tipo de arquitetura de microprocessador é necessário ter um sistema operacional compatível. Esse fato direciona para que as aplicações também sejam compiladas para essa arquitetura, o que de certa forma impede o uso geral de servidores mais especializados que utilizam a tecnologia RISC. Um caso particular, como exemplo, é o sistema operacional GNU/Linux, que possui versões para várias arquiteturas RISC.



RECAPITULANDO

Neste capítulo, você pôde estudar os principais conceitos que envolvem a arquitetura de *hardware* de servidores. Conheceu as principais tecnologias de microprocessadores do tipo RISC e CISC, bem como a tecnologia *Blade*, que é bastante útil para *Datacenters*, onde a concentração de servidores é muito alta. Você aprendeu também que tal tecnologia ajuda no compartilhamento de recursos comuns e ajuda, inclusive, na redução do consumo.

Você pôde ainda ver os principais dispositivos que podem ter características redundantes, pois servem para aumentar a confiabilidade e a disponibilidade de servidores de rede (principalmente os servidores utilizados para missões críticas), além de poder conhecer exemplos de tipos e tamanhos de servidores de rede.

Os conceitos estudados, e os demais vistos nos capítulos anteriores, são fundamentais para você compreender o funcionamento de um servidor de rede, independente de tamanho e capacidade, permitindo uma visão crítica e fundamentada no momento da especificação de sistemas, de forma a atender determinadas demandas de serviços ou usuários.

Anotações:

Riscos Elétricos

5



Nesta parte do livro didático, você estudará os conceitos relacionados à alimentação elétrica dos servidores de rede, bem como, os riscos elétricos que podemos estar sujeitos ao manusear equipamentos, como servidores de rede, *switch*, roteadores, dentre outros.

Você também conhecerá os conceitos de Aterramento Elétrico, Estabilizadores de tensão, *No-Break* e Grupo Gerador de energia.

E ao finalizar o estudo deste capítulo, você terá subsídios para:

- a) entender e compreender os conceitos básicos sobre alimentação elétrica de servidores;
- b) entender o funcionamento básico de um sistema de Aterramento Elétrico e por que ele é importante;
- c) entender e compreender os riscos elétricos, bem como conhecer as precauções necessárias no manuseio de equipamentos eletrônicos, como servidores de rede;
- d) entender o funcionamento dos Estabilizadores de Tensão;
- e) entender o funcionamento básico de um *No-Break*;
- f) entender qual a função de um Grupo Gerador Elétrico e onde é utilizado.

Curioso para saber quais são os riscos apresentados nas próximas páginas? Os conceitos sobre elétrica são fundamentais para seu aprendizado. Por isso, fique atento para as informações seguintes, pois lhe serão bastante úteis.

5.1 ALIMENTAÇÃO ELÉTRICA

Ambientes que comportam computadores, em especial por servidores de rede, *switchs*, roteadores, modems, entre outros, devem ser preparados para o acondicionamento destes equipamentos e seus periféricos. Neste contexto, as questões ambientais relacionadas à temperatura, umidade, nível de ruído, impurezas e controle de acesso são importantes. Entretanto, este capítulo irá enfatizar somente as questões que envolvem o ambiente elétrico de servidores de rede, bem como as características, necessidades e os riscos expostos aos trabalhadores destes ambientes.

O estado atual da tecnologia de computadores exige um controle muito rígido nas características de alimentação elétrica de computadores e servidores de rede. Estes equipamentos exigem o fornecimento de energia, no mínimo estabilizada, com baixa ou nenhuma variação de voltagem, com aterramento e, sempre que possível, com sistema de fornecimento ininterrupto de energia, seja por meio de *No-break* ou de grupo gerador.

É importante salientar que, projetos elétricos específicos devem ser realizados e implementados quando se trata de equipamentos especializados de rede, como é o caso de servidores de rede, seus periféricos e também - e não menos importante - dos equipamentos de rede como roteadores, *switchs* e *modems*.

Há dois fatores fundamentais para a alimentação elétrica de servidores de rede: o primeiro é o correto fornecimento de energia elétrica na tensão adequada e sem variação nos valores absolutos de tensão; já o segundo, envolve o aterramento elétrico da instalação. É muito comum encontrar servidores de rede instalados em um ambiente controlado, com relação à temperatura, umidade, controle de acesso, porém sem o correto aterramento elétrico ou aterramento inexiste.

Muitas pessoas acreditam que o aterramento elétrico é desnecessário e que o custo para sua implantação não se justifica. Entretanto, no caso específico de servidores de rede, o aterramento é imprescindível, sendo um fator de alto risco para o equipamento.

E você sabe o que é aterramento elétrico? Aterramento elétrico é a conexão permanente de hastes metálicas diretamente na terra, com a finalidade de criar um caminho seguro de escoamento, ou de condução de eletricidade, diretamente para a terra, objetivando garantir a continuidade elétrica, conduzindo qualquer tipo de corrente elétrica para as hastes metálicas e, por sua vez, para a terra.

De um modo geral, o aterramento elétrico possui três objetivos básicos:

- a) proteger o usuário de equipamentos elétricos/eletroônicos das descargas atmosféricas (raios) conduzindo estas descargas diretamente para a terra;

- b) transferir (descarregar) cargas elétricas estáticas acumuladas em gabinetes de servidores, microcomputadores, armários e racks de comunicação, diretamente para a terra;
- c) ajudar no funcionamento de dispositivos de proteção, como fusíveis e disjuntores, através do desvio da corrente para a terra.

A Associação Brasileira de Normas Técnicas – ABNT – possui uma norma que define as instalações elétricas em baixa tensão. Essa norma é a **NBR 5410**. As subseções desta norma, 6.3.3.1.1, 6.3.3.1.2 e 6.3.3.1.3 apresentam os possíveis sistemas de aterramento que podem ser implementados.

As normas sobre aterramento

NBR 7117:81;

NBR 5410/1997 (Instalações elétricas de Baixa Tensão);

NBR 5419/2001 (Sistemas de Proteção de Descargas Atmosféricas); e

NBR 14136 – Novo padrão de tomadas brasileiras, você poderá consultar nos seguintes arquivos:

<<http://www.electricware.com/sup/terra.pdf>> e

<<http://py2mok.tripod.com/arquivos-pdf-py2mok-leo/aterramento1.pdf>>



Dentre os sistemas de aterramento da norma NR 5410, o modelo mais adequado é o sistema **Sistema TT**. A figura a seguir apresenta um exemplo deste sistema, em que é possível perceber que o fio neutro é aterrado logo na entrada, e segue na instalação, como neutro, até o equipamento.

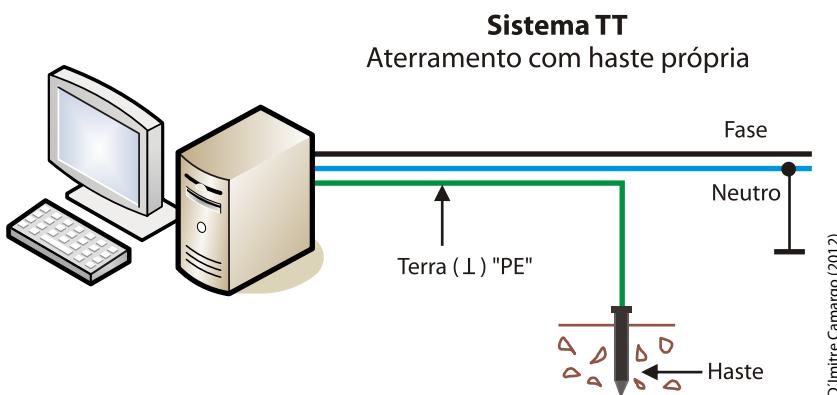


Figura 19 - Modelo de Aterramento
Fonte: Adaptado de Paula (2011)

No caso da figura que você viu, o gabinete é aterrado por meio de um fio-terra com uma haste própria. As fontes de alimentação de servidores de rede ou microcomputadores já fazem a conexão das partes metálicas do gabinete com o conector terra da tomada elétrica, que por sua vez, deverá ser conectado com o aterramento da instalação.

Mas você já sabe a diferença entre o fio neutro e o fio-terra? O **fio neutro** é fornecido pelas concessionárias de energia elétrica e geralmente já é aterrado. Por isso, é muito comum encontrar instalações elétricas em que conectam o fio-terra ao fio neutro. Entretanto, esta não é a maneira mais eficiente ou, melhor dizendo, não é a maneira mais correta.

Outra característica importante do fio neutro é que ele serve como retorno de corrente elétrica, ou seja, é possível haver fluxo de corrente retornando pelo fio neutro. Esta é uma das razões para não conectar um aterramento neste fio.

O **fio-terra**, por sua vez, não deve possuir corrente. Este fio, conforme apresentado, é um escoadouro de corrente elétrica, principalmente para eletricidade estática, pois este tipo de corrente é fatal para equipamentos eletrônicos, especialmente para memórias RAM de servidores ou microcomputadores.



FIQUE ALERTA

A falta de aterramento ou aterramento mal feito pode ser considerado um risco elétrico, pois servidores de rede e microcomputadores são construídos sob especificações que necessitam desta conexão, sob risco de queima de componentes internos e a consequente perda de garantia. Portanto, o aterramento deve ser considerado um item imprescindível na instalação elétrica de servidores de rede, microcomputadores, switches e roteadores.

Desde Julho de 2006 as instalações elétricas possuem aterramento elétrico, conforme a Lei nº 11.337. Portanto, é esperado que instalações elétricas de servidores de rede e microcomputadores possuam o correto aterramento.

A partir da aprovação da norma **NBR 14136**, em 2001, as tomadas e plugues de conexão elétrica no Brasil tiveram uma nova padronização. Neste novo modelo, os conectores e as tomadas elétricas correspondentes obedecem a um padrão único. Estas regras valem para todo tipo de conexão elétrica entre dispositivos eletroeletrônicos e as fontes de energia, sejam elas diretamente das concessionárias de energia ou de equipamentos como estabilizadores de tensão elétrica ou *no-breaks*. O novo modelo de conectorização elétrica pode ser visto nas figuras a seguir.

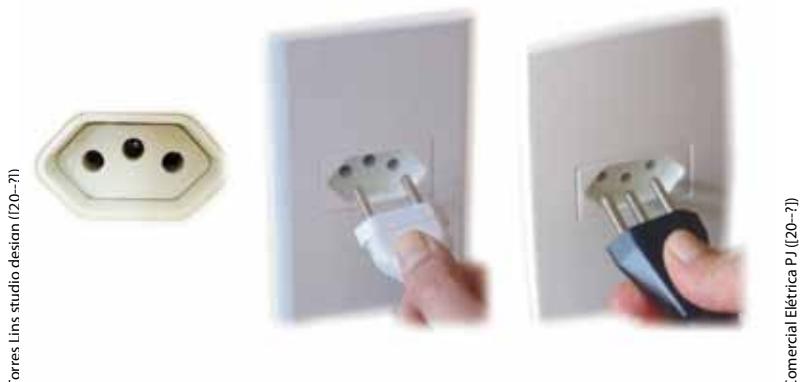
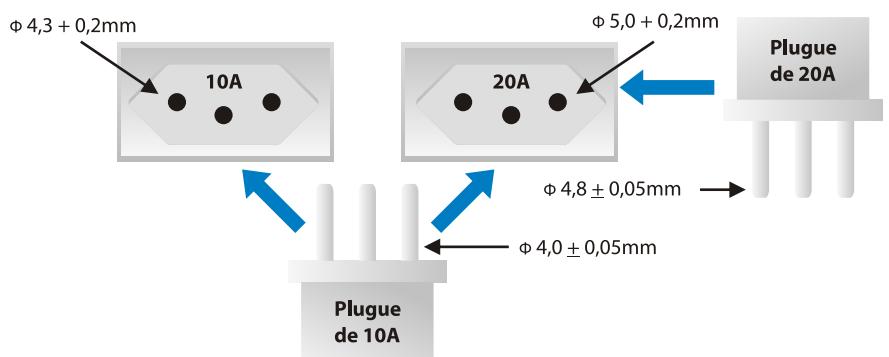


Figura 20 - Novo modelo de tomadas

A partir deste novo modelo, os riscos elétricos no manuseio de tomadas e conectores ficou bastante reduzido, evitando-se várias possibilidades de conexões erradas. Além deste, existe também um padrão de tomadas e conectores para cargas elétricas de 10 Ampères e 20 Ampères, onde não será mais possível conectar plugues elétricos com cargas de 20 Amperes em tomadas de 10 Ampères. Veja na figura seguinte o novo modelo de plugues e tomadas.

Figura 21 - Novo modelo de plugues
Fonte: Adaptado de Paula (2011)

Ao manipular dispositivos eletrônicos, é preciso ter cuidados especiais, principalmente com a eletricidade estática. Para resolver ou, ao menos atenuar, possíveis problemas com eletricidade estática na manutenção de computadores, existe o recurso da pulseira antiestática. Esta pulseira deve ser utilizada sempre que for necessário manusear equipamentos eletrônicos, principalmente computadores.



Sob hipótese alguma abra um quadro de distribuição elétrica para ver as conexões internas ou para trocar algum disjuntor elétrico. Estas atividades devem ser realizadas por pessoas capacitadas, como técnicos ou engenheiros eletricistas.

Tendo-se como premissa que o computador ou servidor de rede, que será tanto manuseado para manutenção como para adicionar ou substituir pentes de memória, discos rígidos ou placas internas está conectado eletricamente numa rede que tenha um aterramento corretamente construído. Nesse caso, a pulseira deve ser colocada em seu pulso, de forma que fique sem folgas, apertada o suficiente para manter fixo e em contato permanente com a pele, a parte metálica da pulseira.

Esta parte metálica da pulseira possui internamente um resistor elétrico, o qual objetiva consumir possíveis correntes estáticas que você possui, e/ou originadas do gabinete onde foi conectada. A parte da pulseira que possui um conector, do tipo garra jacaré, deverá ser conectada no gabinete do equipamento em manutenção.

Na figura seguinte, é possível conhecer a pulseira antiestática, utilizada na manutenção de computadores.

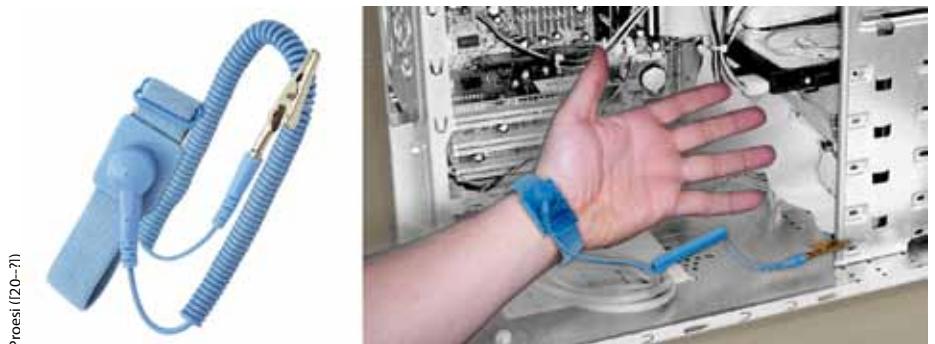


Figura 22 - Pulseira Antiestática

Conforme apresentado, outro fator de igual importância para servidores de rede e microcomputadores é a correta alimentação elétrica fornecida para estes equipamentos. Quanto mais especializados forem os servidores de rede, mais cuidados no fornecimento de energia elétrica deverão ser dispensados, para que tais equipamentos possam trabalhar sob condições normais.

A alta especialização no *hardware*, em geral, apresenta maior consumo de energia elétrica, pois os servidores de rede podem possuir internamente diversos discos rígidos, CPUs e interfaces internas. Além disso, e no mesmo ambiente

físico, devem ficar os demais ativos de rede, como roteadores e *switchs*, os quais também necessitam do correto fornecimento de eletricidade.

Para resolver problemas com alimentação elétrica em ambientes críticos, existem soluções que podem ser adotadas, objetivando a estabilidade dos equipamentos, e para que se possa trabalhar de forma ininterrupta por vários anos.

5.2 ESTABILIZADORES ELÉTRICOS

A forma mais simples de implementar a estabilidade no fornecimento de energia é por meio de um 'estabilizador de tensão'. Este equipamento estabiliza a tensão de saída, caso a tensão de entrada apresente uma variação. Por exemplo: se a tensão de entrada variar de 220 Volts para 223 Volts, o estabilizador irá tentar manter a tensão de saída em 220 Volts, ou seja, o equipamento conectado na saída do estabilizador não irá perceber a variação. Entretanto, estabilizadores de tensão, quando mal dimensionados ou então construídos com componentes fora de especificação, apresentam mais problemas e riscos elétricos para os equipamentos do que se estivessem conectados diretamente na rede elétrica.

Os estabilizadores precisam obedecer à norma **NBR 14373**, da ABNT, que define as principais características técnicas que um estabilizador de tensão deve possuir. Dentre as características que um estabilizador deve possuir, estão as seguintes:

- a) um filtro de linha, para reduzir ruídos originados na rede elétrica;
- b) um protetor contra surtos da rede elétrica, sendo uma proteção contra descargas elétricas;
- c) desligamento automático, que desliga a saída do estabilizador quanto a rede elétrica estiver fora das condições de utilização;
- d) um protetor térmico – proteção adicional contra sobrecarga;
- e) aumento da faixa de tensão de entrada para 45% em redes 110V, 115V, 120V e 127V e 40% em redes 220V;
- f) um True-RMS – que permite o funcionamento correto do estabilizador em redes elétricas com distorções;
- g) sensor de potência – recurso que desliga o estabilizador quando o usuário utilizar equipamentos que excedam a potência do estabilizador.

Com estas exigências, os estabilizadores ficam mais seguros para uso com servidores de rede ou microcomputadores.



Outras informações sobre instalações elétricas e os equipamentos descritos p <http://www.coinfo.cefetpb.edu.br/professor/ilton/hardware/novo/inst_eletricas/Instala_Eletricas/instala.html#inicio>;
<<http://www.abinee.org.br/informac/revista/44h.pdf> -sobre as novas normas para estabilizadores>;
<<http://www.csolutions.com.br/mundoinf/estab.htm>>;
<<http://www.hardware.com.br/dicas/va-watt-pfc.html>>;
<http://www.joseclaudio.eng.br/grupos_geradores_5.html>;
<<http://www.siemens.com.br/templates/coluna1.aspx?channel=7425>>.

A seguir, será possível visualizar um estabilizador de tensão de uso doméstico. Este modelo é muito utilizado para uso residencial na alimentação elétrica para microcomputadores e impressoras do tipo jato de tinta.



Americanas ([20-7])

Figura 23 - Estabilizador de Baixa Potência

De acordo com o que foi apresentado, é possível perceber que os estabilizadores somente tentam manter o nível de tensão elétrica dentro de certos padrões, porém não conseguem gerar eletricidade própria quando da queda de energia. Deste modo, estabilizadores de eletricidade não representam uma solução adequada para servidores de rede. Mesmo para os servidores de rede com baixa especialização no *hardware*, estes equipamentos não são recomendados, porque muitos dos modelos encontrados no mercado não conseguem fornecer a potência elétrica suficiente exigida para os servidores de rede.

Conheça a seguir os dois principais dispositivos de fornecimento de energia de forma ininterrupta.

5.2.1 NO-BREAK

A solução mais recomendada para servidores de rede, no caso de alimentação elétrica são os dispositivos de fornecimento de energia de forma ininterrupta, ou *No-break*, como são conhecidos no mercado (também chamados de UPS – *Uninterruptible Power Supply* ou Fonte de Alimentação Ininterrupta). Os *No-breaks* podem gerar eletricidade e alimentar servidores de rede, quando ocorrer uma queda no fornecimento de energia elétrica. Estes equipamentos conseguem gerar energia a partir de baterias, muitas vezes bem semelhantes às baterias utilizadas em veículos.

Como estas baterias possuem certa quantidade de carga armazenada, então os *No-breaks* somente conseguem manter os equipamentos energizados enquanto houver carga nas baterias. Apesar de geralmente os sistemas de *No-break* não conseguirem manter por muito tempo os equipamentos ligados, pelo menos podem conceder aos administradores do ambiente um tempo extra para poderem avisar os usuários dos servidores e, então, procederem o desligamento dos equipamentos de forma planejada e segura.

A quantidade de tempo que um *No-break* consegue manter equipamentos ligados depende basicamente de dois fatores. O primeiro é o banco de baterias, ou seja, quanto mais baterias o sistema contiver, mais carga poderá armazenar e por mais tempo poderá manter dispositivos ligados. O segundo fator que influencia no tempo de fornecimento de energia elétrica é justamente a quantidade de equipamentos conectados no *No-break*. Quanto mais equipamentos conectados em um *No-break*, menor será o tempo de fornecimento de energia, pois todos os consumos de energia dos equipamentos são somados, constituindo no que se denomina Carga. A carga significa o total do consumo de energia elétrica que um *No-break* deverá fornecer.

E você sabe qual é a unidade de medida elétrica utilizada para medir a potência elétrica neste tipo de equipamento? É o **VA** (Volt x Ampère). Entretanto, a unidade VA não deve ser entendida como unidade de potência em Watt, pois a diferença entre elas baseia-se no conceito de Fator de Potência.

O **Fator de Potência** é uma parte da corrente elétrica que fornece a energia para a carga, e o seu valor é um número entre 0 e 1. Nos dispositivos que possuem filamentos incandescentes, como aquecedores elétricos e lâmpadas, o valor do fator de potência é igual a 1 (um). Nos demais equipamentos, o valor total da corrente não consegue ser utilizada, então, uma parte desta corrente é retornada ou perdida. A corrente que não é utilizada e que retorna, muitas vezes é formada por corrente reativa que é causada pela própria natureza das cargas eletrônicas (que são os elétrons livres dos fios condutores). Em outras vezes, esta corrente de retorno é uma corrente distorcida, gerada, por exemplo, por interferências geradas por motores ou indutores.

No caso de servidores de rede ou microcomputadores, o Fator de Potência fica com valores entre 0,6 e 0,7. Deste modo, a potência medida em Watts para estes equipamentos é um valor entre 60% e 70% do valor em VA. Um valor aceitável tecnicamente para uso em cálculos de potência para microcomputadores e servidores de rede é o valor de 0,65 para o Fator de Potência.

Veja um exemplo a seguir.

Um *No-break* com capacidade para fornecer 5000VA de potência, irá fornecer até 5000 Watts para alimentação de lâmpadas elétricas incandescentes, ou seja, 100% da sua capacidade. Isto porque nestes equipamentos a corrente elétrica é toda consumida no filamento da(s) lâmpada(s). Porém, este mesmo *No-break* somente conseguirá alimentar computadores ou servidores de rede com consumo total de até 3250 Watts. A diferença nas potências é justamente causada pelo Fator de Potência.

É muito comum o valor da potência de um *No-break* ser especificado em VA ou em Watts. Para fazer a conversão de Watts para VA, basta dividir o valor em Watts por 0,65, para o caso dos equipamentos conectados ao *No-break* serem somente computadores, *switchs* ou roteadores. Veja:

$$\mathbf{VA = Watts / 0,65.}$$

Então, *No-break* de 5000 Watts de potência poderá produzir: **VA = 5000 / 0,65 > VA = 7692 VA**

Deste modo, para fazer a conversão inversa de uma potência em VA (Volt/Ampère) para Watts, faça:

$$\mathbf{Watts = VA \times 0,65}$$

Para um *No-break* com 1000 VA de potência poderá produzir: **Watts = 1000 x 0,65 > Watts = 650**

Os cálculos que você acabou de ver ajudam a dimensionar a potência elétrica de um *No-break* e neste cálculo, é necessário saber de antemão o consumo de todos os equipamentos que serão conectados ao *No-break*. Deve-se também considerar uma margem de segurança para expansão, no caso de serem conectados mais equipamentos no futuro. Uma boa margem de segurança seria adotar um percentual de 40% a mais, quando calculando as potências dos equipamentos que irão ser conectados ao *No-break*.

Por exemplo:

Após um levantamento dos equipamentos que serão conectados e protegidos por um *No-break*, sendo estes equipamentos somente servidores de rede, microcomputadores, *switchs* e roteadores, você obteve uma potência de 3000 VA (Volt/Ampère). Nestes valores deve-se adicionar a margem de segurança de 40%, ou seja, mais 1200 VA. Deste modo, o *No-break* para suportar seus equipamentos deverá possuir uma potência de 4200 VA (Volt/Ampère), de outra forma, possuir uma potência em Watts de:

$$\text{Watts} = \text{VA} \times 0,65 > \text{Watts} = 4200 \times 0,65 = 2730 \text{ Watts}$$

Existem diversos tipos de *No-breaks*, com várias tecnologias de controle e monitoramento, principalmente em sistemas com grande capacidade de potência, em que muitos equipamentos deste tipo são denominados *No-breaks* inteligentes, pois possuem monitoração integrada e conectada com um microcomputador ou servidor.

Por meio destas conexões, os *softwares* de gerência conseguem saber quanto tempo ainda resta da carga de baterias, quando ocorrer uma queda de energia e, então, conseguem desligar os equipamentos automaticamente, de forma segura, garantindo a integridade dos dados, o que não ocorreria caso a carga das baterias não pudesse manter os equipamentos ligados.

Os *softwares* de monitoração de *No-breaks* inteligentes, além da possibilidade de desligamento dos equipamentos, também conseguem informar mais detalhes do *No-break*, como a situação das cargas das baterias, os percentuais de consumo dos equipamentos conectados, as sobrecargas de tensão, a subtensão, dentre outros.

Na figura a seguir, é possível conhecer dois tipos de equipamentos *No-break*. No lado esquerdo, sistemas de baixa potência e no lado direito, um sistema de grande potência, geralmente utilizado em *Datacenters* e outras instalações que

necessitam de fornecimento ininterrupto de energia, como centros cirúrgicos de hospitais.



PC Leve ([20-?])

Figura 24 - Modelo de No-Breaks

5.2.2 GRUPO GERADOR

Você deve ter percebido, ao longo do seu estudo, que o fornecimento de energia para servidores de rede e microcomputadores possui muitas características e equipamentos envolvidos. Viu também que a complexidade das soluções de fornecimento de energia aumenta quando as potências envolvidas no fornecimento de energia também aumentam, e nesta linha de pensamento ainda é necessário apresentar uma solução de fornecimento de energia para grandes quantidades de equipamentos (como *Datacenters*, por exemplo) que não apresente restrições de tempo para manter os equipamentos energizados.

A solução para o fornecimento de energia de forma ininterrupta, e sem restrições de tempo, é o Grupo Gerador. Grupo Gerador é um sistema combinado de um motor Diesel e um gerador de corrente alternada (alternador) montados com componentes adicionais para controle, supervisão e monitoramento, objetivando o fornecimento de energia elétrica de forma ininterrupta, a qual é produzida por meio do consumo de Diesel.

Estes equipamentos são empregados comumente em centros cirúrgicos de hospitais, pois é um dos locais de maior situação crítica quando há falta de energia elétrica. Também é utilizado em *shows* e em locais que exijam equipamentos em funcionamento contínuo, como os centros de monitoramento de tráfego aéreo. Estes centros de monitoramento não podem parar, uma vez que inúmeros acidentes poderiam ocorrer, colocando em risco a vida de milhares de pessoas.

A seguir, acompanhe uma situação que ocorreu com a empresa Petrobras.



CASOS E RELATOS

Obra na Amazônia

A Petrobras precisou iniciar uma obra no Amazonas, na construção do oleoduto Brasil-Bolívia. No local não havia nenhuma infraestrutura elétrica disponível. Nestes locais, a única solução aplicável de fornecimento de energia elétrica é o emprego de um Grupo Gerador.

Acondicionado em um contêiner, o equipamento forneceu energia elétrica para todo o canteiro de obras, incluindo iluminação, computadores, telefones, antenas de comunicação via satélite e demais equipamentos de engenharia utilizados nas obras.

Sem o emprego de um Grupo Gerador, as condições de trabalho em canteiros de obras em locais de difícil acesso ou inóspitos é muito difícil, o que nos faz lembrar sempre da importância da eletricidade para o nosso dia a dia e para o nosso trabalho.

A construção dos Grupos Geradores de energia elétrica geralmente é realizada em virtude das características de consumo elétrico onde serão utilizados. As empresas fornecedoras deste tipo de equipamento tendem a manter seus produtos de forma padronizada, ou seja, são equipamentos de uso geral. Entretanto, devido às características peculiares de cada consumidor, os equipamentos, muitas vezes, não conseguem atender ou então são superdimensionados.

Grupos Geradores para uso naval, industrial ou de telecomunicações possuem requisitos diferenciados de fornecimento elétrico, exigindo, deste modo, que o equipamento seja quase que construído sob demanda.

Muitos outros fatores técnicos, além da carga atendida (gerada) pelos Grupos Geradores, devem ser atendidos, pois são solicitados pelos consumidores, como por exemplo: tempo de partida, controle remoto, nível de ruído, capacidade de operar em conjunto com a rede elétrica ou então com outro Grupo Gerador, possuir partida e parada automática.

O dimensionamento de um Grupo Gerador deve ser realizado por equipes especializadas, formadas por engenheiros eletricistas, onde todos os fatores que foram mencionados, além de outros, deverão ser levados em consideração. Em

geral, e como base para o dimensionamento de um Grupo Gerador, alguns critérios devem ser esclarecidos/elucidados, dentre eles:

- a) o local da instalação: em locais com ambiente controlado, ou insalubres ou então no mar (caso de geradores navais);
- b) o tipo da carga: para quais equipamentos o Grupo Gerador terá que fornecer energia, como por exemplo: computadores, equipamentos de telecomunicações, iluminação, motores de indução, retificadores de corrente, fornos, etc.);
- c) regime de operação: quantas horas o sistema irá funcionar por dia, se é um sistema reserva ou não, se será a única fonte de energia;
- d) os riscos envolvidos no caso da necessidade de parada do Grupo Gerador para manutenção e quanto tempo os consumidores podem ficar sem eletricidade.

Estas e outras questões são fundamentais para a definição deste tipo de equipamento. Por isso, e na maioria das vezes, uma equipe inteira é que trata deste assunto e geralmente são empresas especializadas que somente comercializam este tipo de equipamento.



VOCÊ SABIA?

Que os centros cirúrgicos dos hospitais devem possuir um grupo gerador específico para atendimento das cirurgias?

Com relação ao emprego destes equipamentos na área de Tecnologia da Informação, seu uso é muito comum em centros de dados (*Datacenters*) que atendem centralizadamente clientes ao redor do mundo, como bancos, empresas financeiras de cartão de crédito e empresas que fornecem serviços de busca e de computação em nuvem, na Internet.

A seguinte figura mostra um grupo gerador em que é possível observar: o motor no centro; o seu sistema de resfriamento com um radiador, no lado esquerdo; e o alternador, no lado direito.



Cummins ([20-?])

Figura 25 - Grupo Gerador

A maioria dos grupos geradores industriais são produzidos e embalados dentro de um contêiner. Estes são muito parecidos com os contêineres utilizados no transporte de cargas por navio. Este acondicionamento em contêiner possibilita o transporte e montagem do grupo gerador em locais diversos, como num chão de fábrica, canteiros de obras em florestas ou em *shows* em locais abertos e distantes.



RECAPITULANDO

Neste capítulo foi possível conhecer diversos conceitos importantes para seu aprendizado, não é mesmo? Um deles foi o de Riscos Elétricos, pois envolvem servidores de rede e microcomputadores. O conceito de Aterramento Elétrico também tem sua importância atribuída aos servidores de rede e demais equipamentos eletrônicos, já que tais equipamentos eletrônicos - como servidores de rede e microcomputadores - requerem um correto manuseio, por meio do uso de uma pulseira antiestática.

Foi possível conhecer outros conceitos interessantes, como os Estabilizadores de Tensão elétrica e suas funções de dimensionamento e o seu uso para estabilização elétrica. Além disso, você pôde aprender sobre o *No-break* e o Grupo Gerador, ambos com suas específicas funções, conforme recém estudado.

Estes conceitos o ajudarão nas atividades de manutenção de servidores de rede ou microcomputadores, pois você poderá identificar os tipos de equipamentos de energia que envolvem ambientes computacionais, suas conexões, objetivos, forma de trabalho e riscos envolvidos no caso de instalações mal projetadas.

Anotações:

Gerenciamento de Memória

6



Este capítulo destina-se ao aprendizado direcionado à memória nos computadores. Nesta parte do seu estudo, você irá conhecer como funciona o gerenciamento de memória em servidores de rede. Para tanto, duas abordagens serão apresentadas: a primeira enfoca o gerenciamento de memória diretamente pelo *hardware*, ou seja, como o *hardware* gerencia a memória no computador. A segunda aborda como o sistema operacional gerencia a memória.

Com os conceitos adquiridos você estará capacitado, ao final deste capítulo, a responder sobre os seguintes assuntos:

- a) saber gerenciar os comandos de funcionamento de uma memória;
- b) gerenciar uma memória orientada pelo *hardware* do computador;
- c) realizar o gerenciamento de memória executado pelo sistema operacional.

Como você pode perceber, este capítulo reserva um aprendizado bem interessante.

6.1 GERENCIAMENTO DE MEMÓRIA NO COMPUTADOR

O gerenciamento de memória em um computador é uma das principais funções do equipamento, pois na memória é que estão todos os dados em processamento. Tudo que é possível pensar em termos computacionais, de uma maneira ou de outra, passa pela memória do computador. Ao acessar à Internet, baixar um arquivo, escutar uma música, executar um programa, salvar dados num *pen-drive*, enfim, não há processamento sem memória. Deste modo, o Gerenciamento de Memória assume um papel importante no contexto do processamento da informação.

No estágio atual da tecnologia de construção de computadores, há diferentes tipos de memórias, pois também há diferentes características de acesso e tamanho para cada uma delas. Imagine um modelo de hierarquia de memórias, em que esta hierarquia é dividida por dois fatores fundamentais das memórias, que são o seu tempo de acesso e a capacidade de armazenamento.

Tanenbaum (2010) apresenta a seguinte hierarquia de memórias, conforme a figura:

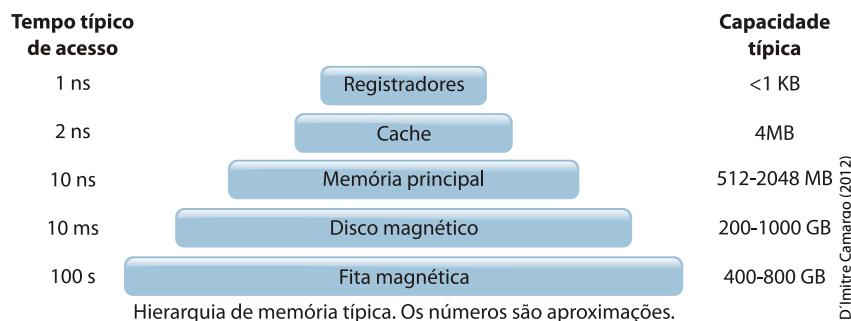


Figura 26 - Modelo de Hierarquia de Memórias
Fonte: Adaptado de Tanenbaum (2010, p. 14)

No modelo que você acabou de conferir, é possível verificar, de uma maneira mais geral, os tipos de memórias, as capacidades típicas e os tempos de acesso. Você viu também que os Registradores também são considerados como um tipo de memória. Todos os microprocessadores possuem basicamente dois tipos de registradores: os **Registradores de Endereços**, que possuem endereços físicos de memória, e os **Registradores de Dados**, que possuem dados propriamente ditos. Deste modo, os dois tipos de registradores possuem informações, ou seja, armazenam dados.

Como os registradores estão dentro da CPU, o acesso a eles é instantâneo, pois dentro da CPU é que o processamento é realizado. E para que isso seja possível, as instruções internas da CPU (comandos do microprocessador) precisam manipular

dados dos registradores. Quando uma informação não está disponível nos registradores da CPU, a mesma precisa então acessar uma memória auxiliar, chamada de *cache*.

Atualmente existem três tipos de memórias *cache*. Estas memórias são classificadas por níveis: **memória cache L1, cache L2 e cache L3**.

Conforme a hierarquia, seus tempos de acesso e tamanho de armazenamento também são diferentes e dependem da arquitetura de construção do microprocessador. Nos primeiros modelos de microprocessadores, as memórias *cache* L1 ficavam em *chips* fora da CPU. Hoje em dia, com o processo de miniaturização, todos os níveis de memória *cache* ficam dentro da própria pastilha da CPU.



VOCÊ SABIA?

Que as diferenças no tempo de acesso entre a memória principal e o disco rígido são da ordem de **10⁶**? Isso pode parecer pouco, mas veja um comparativo pensando no tempo: se o disco rígido demora 1 segundo para encontrar um bloco de dados de uma página de memória virtual, na memória principal este tempo valeria 11,58 dias! É muito tempo pra ficar parado esperando. Por isso o sistema de memória virtual não é uma solução interessante.

O microprocessador Intel XEON E3-12000 possui internamente 64 Kbytes de *Cache* L1, 256 Kbytes de *cache* L2 e 8 Mbytes de *cache* L3. Como esta CPU possui 4 núcleos, ou seja, 4 microprocessadores internamente, os *caches* L1 e L2 são individuais por núcleo, ou seja, cada núcleo consegue acessar seus próprios *caches* L1 e L2. O *cache* L3 é compartilhado por todos os núcleos. Apesar deste arranjo de memórias *cache* ser complicado, os microprocessadores conseguem funcionar perfeitamente. E por meio das quantidades individuais de memória *cache*, os microprocessadores possuem *performance* diferentes, porém, aqueles com mais quantidade deste tipo de memória geralmente possuem melhor capacidade de processamento ou, de outra forma, processam instruções mais rapidamente, pois não precisam gastar tempo buscando dados na memória RAM (*Random Access Memory* – Memória de Acesso Aleatório).

A memória principal de um computador, denominada de memória RAM, é a mais importante, uma vez que é nesta memória que todos os programas de usuários em execução e o próprio sistema operacional residem. Atualmente, é comum encontrar computadores com memórias RAM com 2, 4 ou 8 Gigabytes de capacidade. Para servidores de rede, conforme apresentado, valores de 8, 16 ou 32 Gigabytes são mais comuns, pois servidores de rede geralmente possuem softwares que prestam serviços para inúmeros usuários simultaneamente, e quanto

mais memória disponível, mais acessos e com mais rapidez ele consegue atender às solicitações.

Existe ainda uma pequena quantidade de memória nos computadores, denominada de memória ROM (*Read Only Memory* – Memória somente de leitura). É nesta memória que comumente fica armazenado o programa de carga do computador, muitas vezes chamado de BIOS, ou *Basic Input Output System* – Sistema Básico de Entrada e Saída. O BIOS é utilizado para inicializar o computador, realizando testes básicos de memórias, configurando dispositivos como discos rígidos e demais interfaces e carregando o sistema operacional. Esta memória não pode ser apagada ou regravada, ela somente pode ser lida e o programa nela residente (*o bootstrap loader*) vem gravado de fábrica.

Hoje em dia muitos computadores utilizam uma tecnologia de memória denominada *Flash*, a qual pode ser gravada e regravada, mantendo seus dados quando o computador for desligado. Deste modo, é comum encontrarmos o BIOS gravado em memória *Flash*, o que também permite a muitos fabricantes atualizarem o BIOS, para corrigir algum problema ou mesmo liberar atualizações.

Na sequência da hierarquia de memórias estão os discos magnéticos. Estes discos, mais comumente conhecidos como HD (*hard drive*) ou discos rígidos, possuem uma grande quantidade de armazenamento. Atualmente, discos com 500 Gigabytes ou 1 Terabyte podem ser encontrados facilmente. Apesar da grande capacidade de armazenamento, se você comparar o tempo de acesso de uma informação no disco rígido (HD) com o tempo de acesso na memória principal (RAM), verá que a diferença está na ordem de **10⁶**, ou seja, mais ou menos um milhão de vezes mais lento. Por isso, quanto mais informação residente na memória principal, mais rápido será o processamento.

Outros tipos de armazenamento com fitas magnéticas e discos óticos, como CD-ROM, DVD-ROM ou *Blu-Ray* possuem tempo de acesso ainda maiores que os discos rígidos. Devido a este fato, são utilizados como memória de armazenamento de transporte, para levar dados de um computador para outro ou como meio de armazenamento de *backup* de dados.

6.2 GERENCIAMENTO DE MEMÓRIA PELO *HARDWARE*

De acordo com Tanenbaum (2010), o gerenciamento das instâncias superiores de memória, ou seja, dos registradores e também das memórias *cache*, são realizadas diretamente pelo *hardware*. A própria CPU se encarrega de controlar os acessos a estas memórias, deixando a memória principal (RAM) sob o controle do sistema operacional.

Entretanto, esta tarefa está longe de ser simples, pois tanto os registradores quanto as memórias *cache* possuem um tempo de acesso muito baixo, da ordem 1 ou 2 nanossegundos (1 nanossegundo = 1×10^9 segundos, ou 0,000000001 segundos), o que engrandece a responsabilidade, pois sabe-se que o tamanho destas memórias é muito pequeno, então o controle deve ser preciso e eficiente.

Para gerenciar a memória *cache*, a CPU emprega vários tipos de algoritmos, dependendo do microprocessador. No caso das CPUs INTEL, os conteúdos do *cache* L1 devem também estar no *cache* L2. Este mecanismo é denominado de **cache inclusivo**. De outro modo, nos processadores da AMD, os conteúdos dos *caches* L1 e L2 devem ser diferentes. Desta forma, o nome do mecanismo de *cache* da AMD é denominado de **cache exclusivo**. Os mecanismos citados, que manipulam os dados das memórias *cache*, também se aplicam ao *cache* L3.

A forma de gravação dos dados na memória *cache* também possui algumas diferenças de implementação. As formas de gravação mais conhecidas são as seguintes.

- a) **Write-Back**: a CPU grava os dados diretamente na memória *cache* e o sistema se encarrega de gravar a informação, posteriormente, na memória principal.
- b) **Write-Through**: quando o sistema gravar uma informação na memória *cache* também irá gravar na memória principal ao mesmo tempo. Esta técnica possui pior desempenho, mas é mais fácil de implementar e está sempre sincronizando o *cache* com a memória principal.

Alguns projetos de servidores e microcomputadores permitem que a forma de gravação nas memórias *cache* seja configurada no BIOS do equipamento, permitindo mudar as configurações, onde dependendo da escolha, o sistema poderá ter alterações de *performance*.

O funcionamento da memória *cache*, juntamente com a memória principal, implementa um processo de gerenciamento de memória pelo *hardware* (no caso, pela CPU).

A memória RAM é dividida em linhas de *cache*, denominadas de **cache lines**, possuindo tamanhos típicos de 64 bytes. A linha 0 (zero) possui os endereços de 0 a 63, a linha 1 (um) possui os endereços 64 a 127, e assim por diante. Deste modo, as linhas mais usadas serão mantidas nas memórias *cache*. Assim, quando um programa precisa de uma informação, a CPU verifica se a mesma já não está contida na memória *cache* L1. Se não estiver, procura na *cache* L2, e então na *cache* L3. Se a informação estiver na *cache* L1, L2 ou L3, o processo é chamado de **cache hit**, e não será necessário buscar a informação na memória principal. Caso não encontre o dado requisitado nos três níveis de memória *cache*, o processo é

denominado de ***cache miss***, sendo gerada uma requisição para busca do dado na memória principal.

Com a utilização dos três níveis de memória *cache*, os projetos de servidores de microcomputadores ficaram mais arrojados, pois em outros tempos o acesso às memórias *cache* era muito menor do que na memória principal, o que torna o sistema mais eficiente.

Sendo assim, é possível perceber que o processo de gerenciamento dos registradores e das memórias *caches* são de responsabilidade da própria CPU. Este modelo possibilita que o sistema operacional se encarregue do gerenciamento da memória principal, pois esta também é uma grande responsabilidade. Como o próprio nome diz, memória principal, é necessário lembrar que todos os programas em execução estarão contidos nela.

A memória RAM possui um alto custo, por isso, não é recomendada a inserção de memória a qualquer momento, pois existe um limite físico de endereçamento de memórias, e também no projeto de servidores de rede e microcomputadores em geral.

No conteúdo a seguir, você verá como o sistema operacional consegue gerenciar a memória principal, facilitando a nossa vida ao fazer com que todos os programas sejam atendidos e consigam trabalhar, e fazer aquilo para o qual foram desenvolvidos.



**SAIBA
MAIS**

Obtenha mais informações sobre os tipos de memória *cache* no seguinte site: <<http://www.hardware.com.br/dicas/entendendo-cache.html>>.

6.3 GERENCIAMENTO DE MEMÓRIA PELO SISTEMA OPERACIONAL

Neste item, você verá como o sistema operacional gerencia e controla a memória principal de um computador. Como você estudou, existem vários tipos de sistemas operacionais, uns mais e outros menos eficientes na gestão do uso da memória principal, o que logicamente indica que pode haver vários algoritmos de controle de acesso para gravação e remoção de dados na memória principal.

Tanto o sistema operacional quanto os programas de usuários ocupam espaços na memória principal. Como regra, o sistema operacional ocupa os primeiros endereços da memória, até porque, como visto anteriormente, ele é carregado

primeiro no processo de inicialização. Após sua carga, os demais programas/aplicativos é que poderão ser carregados para a memória principal.

A figura a seguir demonstra um exemplo de alocação contínua da memória principal pelo sistema operacional.

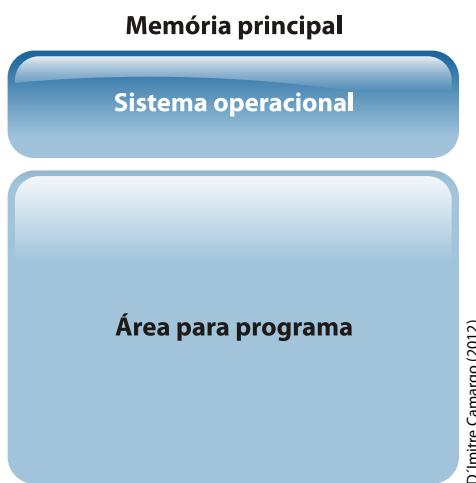


Figura 27 - Alocação Contínua de Memória
Fonte: Adaptado de Machado e Maia (1997)

Apesar da figura tratar de uma simples representação de ocupação de espaço na memória principal, na verdade não é tão simples assim.

É preciso apresentar o conceito de processo, pois ele será utilizado muito neste capítulo, já que os processos, de fato, que ocupam espaço da memória principal. Um processo é um programa em execução.

Você sabe qual é a diferença entre processo e programa?

O programa é uma entidade estática, ou seja, é somente um arquivo contendo instruções de máquina para alguma finalidade. O processo são estas instruções em execução. Deste modo, um programa representa uma entidade estática, já o processo é uma entidade dinâmica.

Assim, quando se fala que o sistema operacional está residente em memória, na verdade se quer referenciar todos os processos que compõem o sistema operacional. E são muitos!

Um processo em memória possui certas características importantes, as quais são denominadas de Contexto. Ele possui um contexto de *software*, um contexto de *hardware* e o espaço de endereçamento.

No contexto de *software* existem algumas informações, como o número do processo PID, o nome do processo, a prioridade de execução, o tempo do processador, dentre outras.

No contexto de *hardware*, tem-se as informações dos registradores gerais, como o registrador de *status* do processo.

É no espaço de endereçamento que estão definidos os endereços de memória alocados pelo processo. A figura que você verá em seguida mostra uma representação das informações pertinentes a um processo.



Tanto os processos do sistema operacional, quanto dos aplicativos de usuários obedecem a mesma estrutura que você acabou de acompanhar. Como o assunto em questão envolve um modelo onde há vários processos em execução, logicamente lembra-se do conceito de multiprogramação, em que há vários programas (processos) em execução num computador.

Para que isso seja possível, ou seja, para haver diversos processos em execução e ocupando a memória principal, o sistema operacional precisa implementar um controle sobre esta memória. Este controle é realizado pelo módulo de Gerenciamento de Memória do sistema operacional, o qual também não deixa de ser um processo em execução, porém com altíssima prioridade no uso da CPU.

Para controlar processos, o sistema operacional possui uma estrutura de dados em memória, denominada de **PCB – Process Control Block**, ou Bloco de Controle de Processos. Num bloco de controle de processos há várias informações sobre o processo como: estado do processo, nome do processo, prioridade, limites de memória, lista de arquivos abertos, dentre outras informações. Na seguinte figura é possível ver o exemplo de um bloco de controle de processos.



Figura 29 - Modelo de um PCB – Bloco de Controle de Processos
Fonte: Adaptado de Machado e Maia (1997)

Deste modo, vimos que todos os programas em execução ou processos, ocupam espaço na memória principal do computador, seja com informações deles mesmos, como instruções e variáveis, quanto com informações das estruturas de dados utilizadas para gerenciar os processos, ou seja, os PCBs.

Dessa forma, então é possível afirmar que o sistema operacional precisa gerenciar a memória, da forma mais eficiente possível, pois existem vários processos competindo pelo uso da CPU e também por espaços de memória?

Sim! O sistema operacional sozinho não conseguiria gerenciar a memória de forma eficiente, ele precisa da ajuda de componentes do *hardware* para fazer esta tarefa. Para uma melhor compreensão, é preciso que você entenda o conceito de memória lógica e memória física. Estes dois conceitos são fundamentais na gerência de memória.

Assim, os espaços lógicos ocupados por um processo são diferentes do espaço físico. Estes espaços, na verdade, são espaços virtuais. Mas na execução de um processo, os espaços virtuais são traduzidos para os espaços (endereços) físicos, por meio de um componente de *hardware* chamado de **MMU – Memory Management Unit** – Unidade de Gerenciamento de Memória, que é o responsável pelo mapeamento dos endereços virtuais para endereços físicos.

A figura seguinte apresenta esta tarefa.

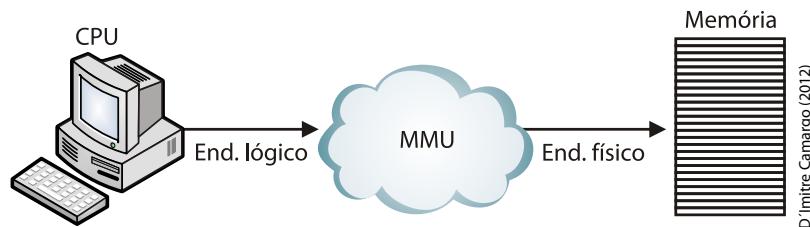


Figura 30 - O mapeamento de endereços de memória lógica x física, realizado pela MMU – Unidade de Gerenciamento de Memória.

Fonte: Adaptado de Oliveira, Carissimi e Toscani (2001)

Mas qual é a situação ideal de programa?

É aquela em que o programa não precisa saber, de fato, qual o endereço onde ele será executado, diferentemente de programas que alocam endereços físicos de memória, chamados de endereços absolutos. Desta maneira, é possível perceber que um programa que aloca memória de forma absoluta irá gerar algum transtorno para o sistema operacional, pois poderá ocorrer que o endereço que o programa quer acessar esteja ocupado por outro programa.



Os programas que não alocam espaços físicos diretos são denominados de **Programas de Código Relocável**, os quais deixam a cargo do sistema operacional o mapeamento da área de memória que o programa irá utilizar.

Resumidamente, um dos principais objetivos do gerenciamento de memória é a atividade de alocação de memória para processos que desejam ser executados, e todas as tarefas adicionais que aparecem e/ou são derivadas da alocação de memória. A figura seguinte apresenta as principais formas de alocação de memória.

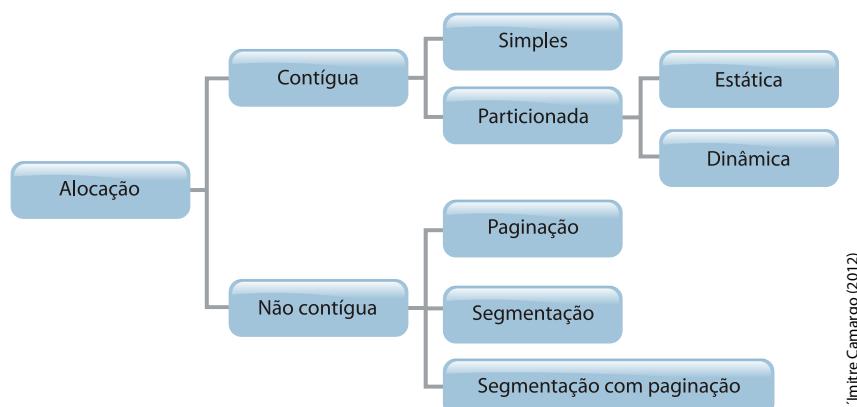


Figura 31 - Formas de Alocação de Memória.
Fonte: Adaptado de Oliveira, Carissimi e Toscani (2001).

D'Imitre Camargo (2012)

A seguir, conheça detalhadamente cada uma das alocações representadas na figura que você acabou de conferir.

Alocação contínua simples

Neste modelo de alocação, a memória é dividida em duas partes: uma para o sistema operacional (ocupando as partes iniciais da memória) e outra para o processo do usuário. Neste modelo, o processo dos usuários poderia acessar qualquer região de memória, inclusive do sistema operacional. Um exemplo deste caso era o sistema DOS e seus aplicativos.

Uma evolução deste modelo de gerenciamento foi a inclusão de controles por meio de registradores de início e fim de memória, que indicam os limites de uso para os programas e também o uso da MMU.

Alocação contínua particionada estática

Aqui o sistema operacional cria múltiplas partições na memória, todas com o mesmo tamanho. Cada partição recebe um processo. Então, logicamente, o número de programas em execução (multiprogramação) dependerá da quantidade de partições. Porém, neste modelo ocorre um problema, quando, por exemplo, um programa é menor que o tamanho da partição. Neste caso irá sobrar memória e esta não poderá ser utilizada, pois está alocada na partição e em um processo. Este problema é denominado de **Fragmentação Interna**.

Alocação contínua particionada dinâmica

Neste modelo de alocação, o sistema operacional cria partições de memória de tamanho e quantidades diferentes, conforme a demanda dos processos. O sistema operacional então controla o total das partições alocadas, partições livres e o tamanho das partições.

A figura seguinte apresenta uma ilustração simples de como podem ser alocadas partições de memória de tamanhos variados pelo sistema operacional.

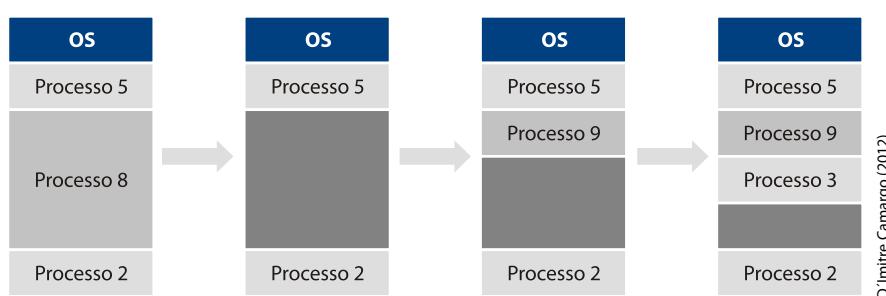


Figura 32 - Partições de Memória com Tamanhos Diferentes
Fonte: Adaptado de Oliveira, Carissimi e Toscani (2001)

D'Imitre Camargo (2012)

Um dos objetivos da alocação de partições dinamicamente é a redução do problema de fragmentação interna, pois os processos alocam partições e tamanhos conforme a necessidade, e as partições acabam ficando em tamanho e números diferentes, o que exige um controle maior do gerenciamento de memória.



FIQUE ALERTA

A alocação dinâmica de partições de memória resolve o problema da fragmentação interna, mas cria outro: o da fragmentação externa.

Perceba que, na dinâmica de criação de partições variadas, ao finalizar um processo, poderá ocorrer de o espaço todo da partição acabar ficando liberado para uso. Porém, o tamanho deixado talvez não seja o suficiente para a criação e alocação de outra partição, criando um novo problema, denominado **Particionamento Externo**.

Acompanhe, na figura a seguir, um exemplo de como isso poderá ocorrer, ao tentar alocar uma partição para um processo com tamanho de 120Kbytes.

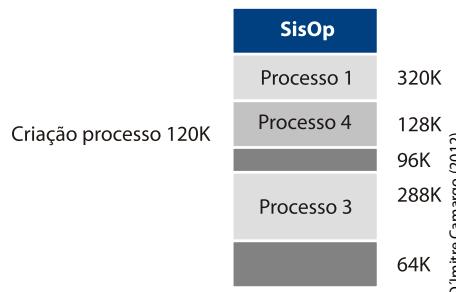


Figura 33 - Alocação de Processos na Memória. Partições de Tamanhos Diferentes
Fonte: Adaptado de Oliveira, Carissimi e Toscani (2001)

Como visto na figura, os espaços vazios de memória que poderiam ser alocados não são formados por uma área contígua de memória, logo, tem-se a fragmentação externa.

As soluções possíveis para resolver os problemas da fragmentação externa irão exigir mais consumo de CPU pelo gerenciador de memória e, em muitos casos, talvez um acesso a disco.

Mas o que fazer neste tipo de situação?

A solução para este caso seria realocar as partições, criando uma área de memória contígua, eliminando-se os espaços (fragmentos) de memória sem uso. Conforme visto, este modelo utiliza mais CPU e acesso a disco, pois poderá ser

necessário realocar partições transferindo-as para uma área em disco (*swapping*) temporária, para então trazer para a memória principal novamente.

O gerenciamento de memória com alocação contígua particionado dinamicamente exige que o sistema operacional responda pelos seguintes critérios:

- a) determine qual área de memória livre será utilizada pelo novo processo;
- b) mantenha uma lista de espaços livres (lacunas) na memória principal;
- c) deverá percorrer a lista de espaços livres para encontrar uma lacuna que seja possível alocar para o novo processo.

A forma de percorrer a lista de espaços livres (lacunas) poderá ser realizada por meio de alguns algoritmos. Veja alguns deles.

- a) **First fit** (primeiro encaixe): este algoritmo procura uma lacuna de memória que seja grande para o processo e a quebra em dois. A primeira aloca ao processo e a outra restante torna-se um segmento livre de memória, porém menor. Isso somente não ocorre caso o algoritmo encontre uma lacuna que seja exatamente do tamanho do processo. É um algoritmo bem rápido, pois sua procura por lacunas tende a ser a menor possível;
- b) **Next fit** (próximo encaixe): funciona igual ao algoritmo *first fit*, porém ele memoriza a posição do segmento de memória disponível de tamanho suficiente. Quando for executado novamente, iniciará a busca a partir do ponto memorizado, não necessitando percorrer a lista de espaços livres novamente. Com isso, este algoritmo é um pouco inferior ao *first fit*;
- c) **Best fit** (melhor encaixe): neste algoritmo é percorrida a lista inteira de espaços livres de memória (lacunas), e o gerenciador de memória escolhe o menor segmento de memória livre que seja adequado ao processo sendo criado. Ele procura sempre o segmento de memória que esteja próximo do tamanho do processo sendo criado, tendo assim uma melhor correspondência entre a solicitação de segmentos livres e dos segmentos disponíveis. Este algoritmo é mais lento que o *first fit* e também gera mais desperdício de memória, pois há uma tendência de deixar segmentos muito pequenos de memória livre, os quais são, em geral, inúteis na alocação de processos;
- d) **Worst fit** (pior encaixe): este algoritmo procura o maior segmento de memória livre que atenda ao processo, após a sua alocação. O segmento restante ainda seria grande o suficiente para alocação a outros processos.

Em todos os casos, sempre haverá segmentos de memória livres, que de uma forma ou de outra, não serão utilizados por serem muito pequenos para alocação em novos processos, causando, desta forma, um pequeno desperdício de memória.

Mas também existe outra alternativa no gerenciamento de memória, a qual alguns sistemas operacionais recorrem frequentemente. Apesar de não ser uma solução ideal, permite que o total ocupado de memória principal do sistema (alocada para processos) seja maior do que a memória real do computador. Ou seja, passa a ser possível a execução de mais processos do que a memória principal suporta. Este conceito é denominado de **Memória Virtual**.

Cada programa possui o espaço de endereçamento que utiliza e que é dividido em páginas. Cada uma destas páginas é uma série contínua de endereços. Então, estas páginas são mapeadas para a memória física (real) do computador. Entretanto, nem todas as páginas, necessariamente, precisam estar na memória principal ou memória real.

Deste modo, quando o programa faz uma referência a um endereço que já está mapeado para a memória física, o *hardware* faz o mapeamento dinamicamente. Quando então o programa precisa acessar um endereço de memória que não está mapeado para a memória física, mas está na memória virtual, o sistema operacional é informado e terá que buscar as instruções da memória virtual.

O dispositivo comumente utilizado para armazenamento das páginas de memória virtual é o disco rígido. Entretanto, sistemas operacionais possuem abordagens diferentes para a implementação da memória virtual. Nos sistemas Windows, o sistema operacional cria um arquivo comum em disco denominado ***pagefile.sys***. Este arquivo fica escondido dentro do diretório raiz do disco de inicialização do sistema operacional, geralmente o disco C:.

Nos sistemas Unix ou Linux, a memória virtual também possui espaço reservado em disco, porém, nestes sistemas é necessária a criação de uma partição inteira para esta finalidade. Esta partição não precisa ser formatada, sendo ela mesma um tipo de *filesystem* do sistema.

As duas abordagens possuem restrições. No caso do Windows, ao utilizar-se um arquivo comum como área de memória virtual, fica-se sujeito aos problemas do *filesystem* em utilização, no caso, o disco C; porém, no caso de expansão da utilização da memória virtual, muito comum nos sistemas Windows, o arquivo ***pagefile.sys*** é aumentado automaticamente.

Por outro lado, no caso dos sistemas Unix e Linux, uma partição própria e com acesso restrito do sistema operacional é utilizada e possui a vantagem de que nenhum usuário irá acessá-la e também pelo fato de que o acesso ao dispositivo é direto, ou seja, ele não passa por estruturas de dados de formatações de *filesystem*.

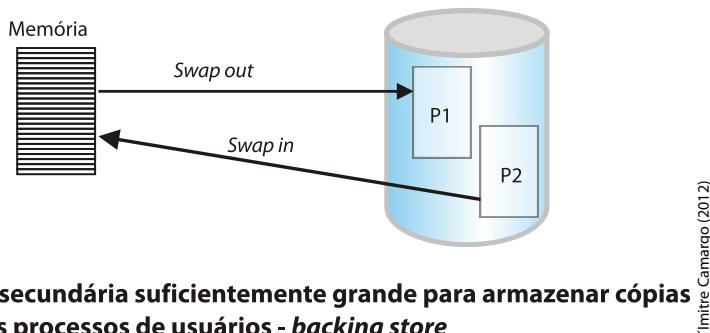
Mas nesta situação existe o inconveniente de que, caso seja necessário aumentar o tamanho da memória virtual, cria-se o problema da falta de espaço físico disponível nos discos rígidos, e neste caso, será necessário diminuir uma das

partições adjacentes à partição da memória virtual, também chamada de **partição de Swap**, para poder aumentar a área da memória virtual.

Para o processo de busca de páginas na memória virtual e de carga na memória principal, existe um recurso denominado **Swap in**. O processo inverso é denominado **Swap out**, e na figura seguinte você poderá compreender o funcionamento de um modelo Swap.

■ Processo necessita estar na memória para ser executado

Se não há mais espaço em memória é necessário fazer um rodízio de processos em memória



■ Memória secundária suficientemente grande para armazenar cópias de todos os processos de usuários - *backing store*

Figura 34 - Modelo de Swap de Memória
Fonte: Adaptado de Oliveira, Carissimi e Toscani (2001)

Acompanhe a situação a seguir para compreender melhor um dos principais problemas no gerenciamento de memória.



CASOS E RELATOS

Servidor de rede com falta de memória

A principal tarefa de um sistema operacional é, sem dúvida, o gerenciamento de memória.

Certa vez em uma *lan house*, Valdir, técnico em redes, ao analisar um servidor de rede, verificou que o mesmo estava muito lento, que as CPUs não estavam em plena carga e também que os usuários reclamavam da lentidão do sistema.

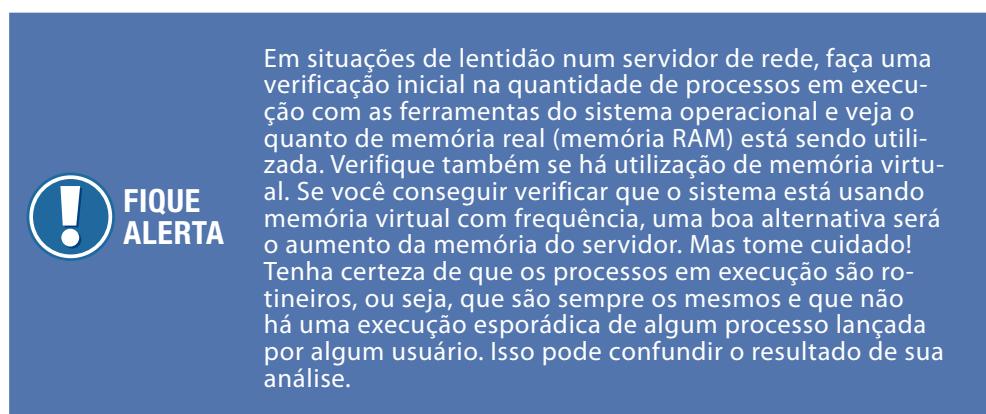
Ao observar o uso da memória, Valdir notou uma atividade excessiva de paginação, ou seja, o sistema estava utilizando a memória virtual a pleno vapor. Como é um técnico em redes, Valdir lembrou que quando o siste-

ma começa a utilizar memória virtual é porque não possui memória real disponível. Então só havia duas formas de resolver o problema e acalmar os ânimos dos usuários: retirar os sistemas do servidor, colocando em outro (que não estava disponível naquela época) ou então adicionar mais memória.

Após alguns minutos, Valdir definiu que a melhor solução era dobrar o número de memória do servidor. Dessa forma, não foi preciso comprar outro servidor.

Na vida diária da administração de servidores de rede, quando o equipamento começa a ficar muito lento, demorando mais do que o normal para atender requisições de usuários, a primeira tarefa a ser realizada é justamente verificar como está o nível de utilização da memória principal do servidor.

Em geral, quando um sistema começa a utilizar muita memória virtual, ou seja, quando realiza rotineiramente a paginação virtual (*swap in/swap out*), é um forte indicativo de que este equipamento precisa de mais memória real (RAM).



Perceba que o uso da memória virtual é apenas um recurso momentâneo, que permite a execução de sistemas maiores que o total de memória disponível. Quando isso ocorre, as opções são restritas: ou você aumenta a memória principal, ou realoca programas para execução em outro servidor. Geralmente a lentidão em sistemas está relacionada com a falta de memória principal. Não que esse seja o problema principal, mas é o fator que deve ser verificado em primeira instância.

Sistemas operacionais possuem ferramentas diversas para o gerenciamento de memória. No caso dos sistemas Windows, a ferramenta *TaskManager* poderá ser utilizada para a verificação dos processos em execução, o total de memória

em uso e o total de memória sendo paginada. Permite também a verificação da carga de utilização dos processadores do computador, em que é possível observar se os processadores estão com muita ou pouca carga de trabalho.

Nos sistemas Linux existem diversas ferramentas para a gerência de memória. Algumas delas são mais elaboradas, outras mais diretas, mas todas possuem e apresentam as informações que precisamos para gerenciar o sistema e ver como está a utilização da memória no computador.

A figura seguinte nos mostra a tela do programa *htop*, num *netbook*, em que é possível ver alguns processos em execução, o total de memória em uso e disponível, a memória virtual em uso e disponível, o total de processos (*tasks*) e a média de carga do sistema (*Load average*).

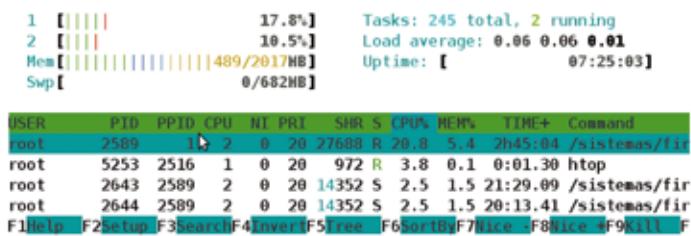


Figura 35 - Tela do Programa *htop* no GNU/Linux.
Fonte: Adaptado Luiz Antonio Silva de Paula (2011)

Dimitris Camargo (2012)



RECAPITULANDO

Neste capítulo, você conheceu os detalhes do gerenciamento de memória, e viu as atividades que são executadas pelo *hardware* e pelo sistema operacional. Foi possível ainda, verificar algumas maneiras de implementar o gerenciamento de memória e que, de um modo geral, podem influenciar no desempenho do computador, pois podem ter mais ou menos eficiência na gestão deste bem tão precioso que é a memória principal (RAM).

Com os conhecimentos apresentados, você poderá analisar com mais clareza uma situação real de utilização de memória num servidor de rede. Com os conhecimentos sobre a memória real e virtual, poderá realizar levantamentos de utilização de memória e concluir se o sistema como um todo está ou não necessitando do incremento de memória principal.

Gerenciamento de Dados

7



Neste capítulo que inicia, serão apresentadas as maneiras de organizar os arquivos em disco e de que forma os sistemas operacionais implementam o gerenciamento de arquivos. Você também conecerá os conceitos relacionados com a forma de alocação e recuperação de arquivos em disco, bem como uma breve descrição dos tipos de sistemas de arquivos (*filesystem*) disponíveis nos sistemas Unix/Linux e Windows.

O estudo deste capítulo permitirá que você seja capaz de:

- a) entender e compreender o que são arquivos em disco e seus tipos;
- b) entender o que é um sistema de arquivo (*filesystem*) e quais os tipos existentes;
- c) compreender como é a alocação e a recuperação de arquivos em disco;
- d) compreender e entender o que é um *i-node* nos sistemas Unix/Linux;
- e) compreender o que significa o Gerenciamento de arquivos;
- f) entender como é realizado o gerenciamento de arquivos no Unix/Linux;
- g) entender como é realizado o gerenciamento de arquivos no Windows.

Preparado para outra etapa de aprendizado? Com dedicação e interesse as chances de se tornar um entendedor do assunto são grandes. Fique atento aos conceitos e dicas, e sempre que puder esclarecer alguma informação, entre em contato com seu professor. Dialogando é que se aprende mais.

7.1 GERENCIAMENTO DE ARQUIVOS

Antes de dar início ao assunto, é importante conhecer as diversas estruturas de dados que compõem os arquivos, bem como as possíveis organizações internas. Em seguida, você irá conhecer os principais tipos de sistemas de armazenamento de arquivos, o que, a partir deste momento, será denominado de sistema de arquivos (*filesystem*).

Mas o que são arquivos?

Os arquivos são agrupamentos lógicos de informação, relacionados e armazenados em disco. Como o foco do capítulo é o gerenciamento de arquivos, você irá encontrar neste capítulo diversos assuntos referentes aos arquivos residentes em discos rígidos, apesar do conceito se aplicar também para uma unidade de Pen-drive, um DVD-ROM ou *Blu-ray*.

Um arquivo possui uma identificação pelo usuário através de um nome, formado por uma sequência de caracteres. Em alguns sistemas operacionais, a identificação dos arquivos é composta por duas partes separadas por um ponto: a parte após o ponto é chamada extensão do arquivo e serve para identificar o conteúdo. Esta característica é muito comum nos sistemas Windows, mas nos sistemas Unix/Linux as extensões nos nomes de arquivos não são levadas em consideração, apenas se existirem, e são para controle dos usuários ou aplicativos.

Os arquivos também podem possuir diferentes formas de organização, desde uma organização sequencial, em que os registros são lidos um após o outro, até uma organização indexada, onde os registros são lidos a partir de um índice. Veja na figura a seguir, um exemplo de duas organizações internas de arquivos.

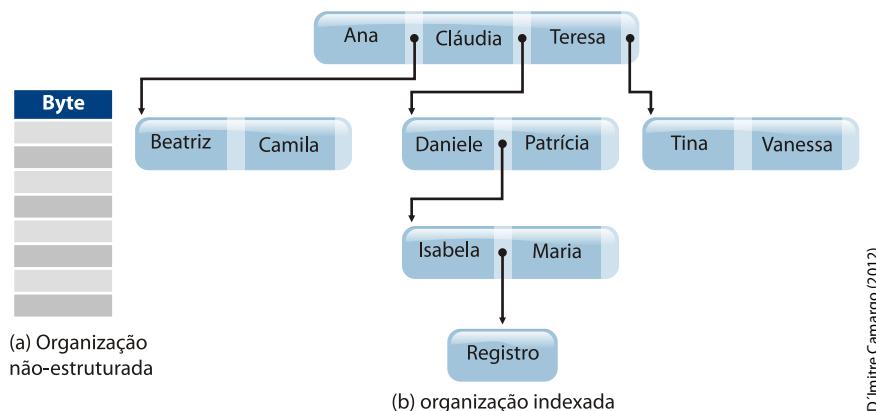


Figura 36 - Tipos de Organização Interna de Arquivos
Fonte: Adaptado de Machado e Maia (1997)

D'Imitre Camargo (2012)

A organização interna dos arquivos não é de responsabilidade dos sistemas operacionais, mas sim, dos sistemas que criaram e que utilizam os arquivos. O sis-

tema operacional se limita a criar um meio de armazenamento onde os arquivos podem ser gravados, alterados, consultados e excluídos.

Entretanto, os sistemas operacionais possuem várias formas de armazenar arquivos em discos. Mas o mais importante neste processo é saber como é feita a alocação de espaço em disco, pois este processo é determinante para a *performance* no acesso aos arquivos gravados em disco. Devido à maneira como a alocação de espaço em disco é realizada, esta determina fatores como: velocidade de gravação, velocidade de leitura, tempo de localização do arquivo em disco, dentre outras.

A menor unidade de alocação utilizada para gravação de arquivos é conhecida como um bloco de dados. Assim, gravar arquivos é uma operação que implica no conhecimento do endereço de blocos livres no disco e também na gravação e marcação destes blocos gravados em alguma estrutura de dados que permita ser consultada, para que não se grave informações em blocos já utilizados por outros arquivos.

Este controle de blocos livres no disco é o determinante dos sistemas de arquivos, e cada um possui a sua forma de gestão de blocos. É por isso que há diversos tipos de sistemas de arquivos.

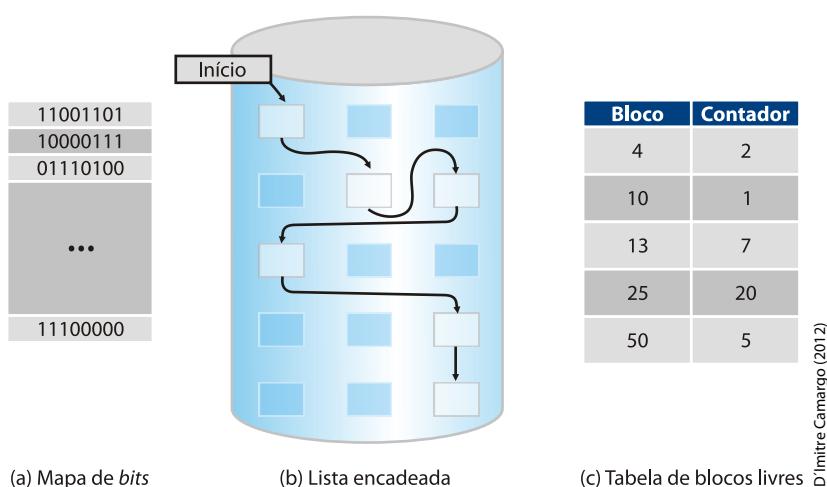
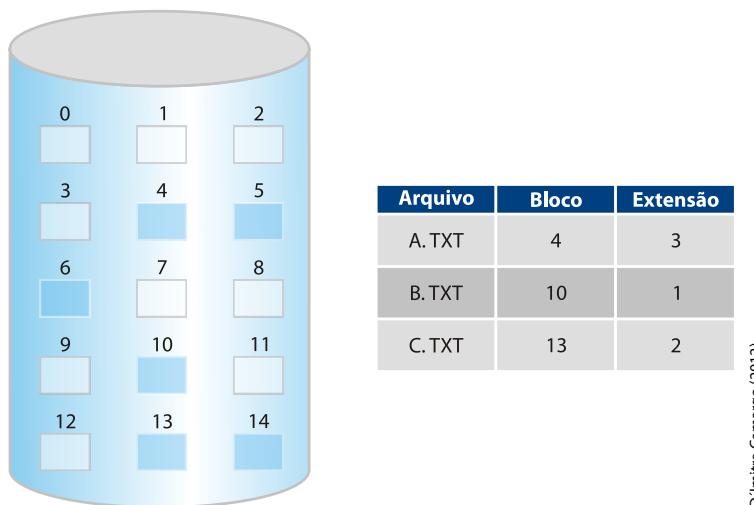


Figura 37 - Exemplos de Alocação de Blocos em Disco
Fonte: Adaptado de Machado e Maia (1997)

Na figura que você acabou de ver, é possível verificar algumas formas de alocação de blocos em disco. Em (a), tem-se alocação por mapa de *bits*, armazenando os endereços de blocos. Em (b), há a representação de uma técnica denominada Lista Encadeada, em que há uma estrutura de dados que indica qual o endereço do próximo bloco que pertence ao arquivo. Em (c), é possível visualizar uma tabela de blocos livres de disco.

A alocação de espaço em disco poderá ser feita no modo contínuo, ou seja, para gravar um arquivo qualquer, é necessário ter todos os blocos em disco, um atrás do outro. Neste modelo de alocação, não se pode ter blocos não utilizados no meio dos blocos do arquivo. Neste modelo há uma tabela auxiliar que mapeia as informações do arquivo, seu bloco inicial e também o total de blocos que ele usa. Veja um exemplo na figura seguinte.



D'Imitre Camargo (2012)

Figura 38 - Exemplo de Alocação Contígua de Blocos
Fonte: Adaptado de Machado e Maia (1997)

O modelo de alocação contígua de espaço em disco possui um problema muito sério. Imagine se você apagar alguns arquivos do disco. Os blocos utilizados por estes arquivos ficarão livres, causando assim um problema, pois para serem alocados novamente, somente será possível se forem arquivos com o mesmo tamanho destes blocos livres, o que é muito difícil de ocorrer.

Este problema é a fragmentação, ou seja, ao excluir arquivos num sistema de alocação contígua, ocorrem buracos de blocos não utilizados, causando a fragmentação.

Veja a representação de um fenômeno como este, na figura a seguir.

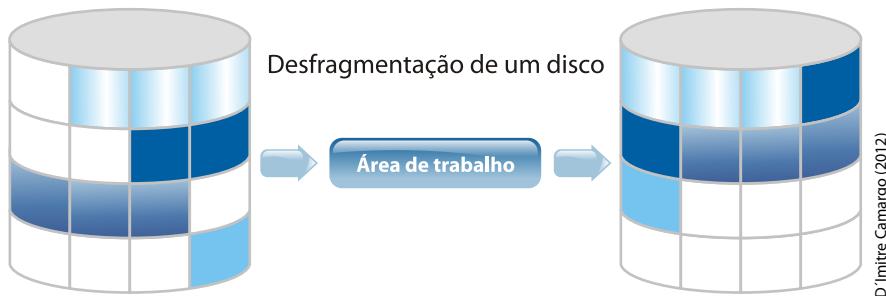


Figura 39 - Exemplo de Fragmentação em Disco
Fonte: Adaptado de Machado e Maia (1997)

D'Imitre Camargo (2012)

Ao lado esquerdo da figura que você acabou de visualizar, é possível identificar um disco fragmentado pelas exclusões de arquivos. Ao lado direito, tem-se o mesmo disco sem fragmentação, que foi obtido por meio de um processo de **Desfragmentação**, o qual utilizou uma área de trabalho temporária para o processo.

Outra maneira de alocação de arquivos em disco é a alocação encadeada. Neste modelo há uma tabela auxiliar que relaciona o nome do arquivo com o endereço do bloco inicial do mesmo. Então, por meio do encadeamento de blocos, que podem ser contíguos ou não, as informações do arquivo podem ser recuperadas.

Veja uma reprodução do modelo de alocação encadeada na figura a seguir.

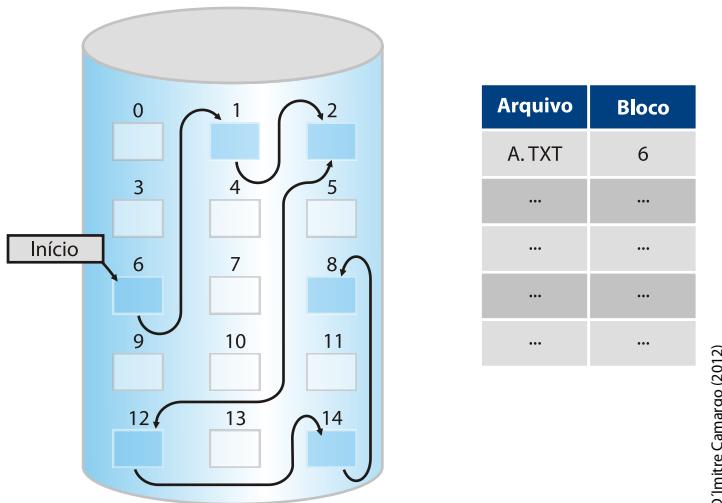


Figura 40 - Alocação Encadeada de Blocos em Disco
Fonte: Adaptado de Machado e Maia (1997)

A terceira maneira de alocação de arquivos em disco é por meio da técnica da utilização de índices. Esta técnica emprega o conceito de busca dos blocos por meio de uma tabela de índices de blocos. Nesta tabela constam todos os endereços de blocos utilizados pelo arquivo. É uma das formas mais eficientes de alocação de arquivos em disco, pois é muito rápida.

Veja, na figura seguinte, um modelo básico da alocação indexada.

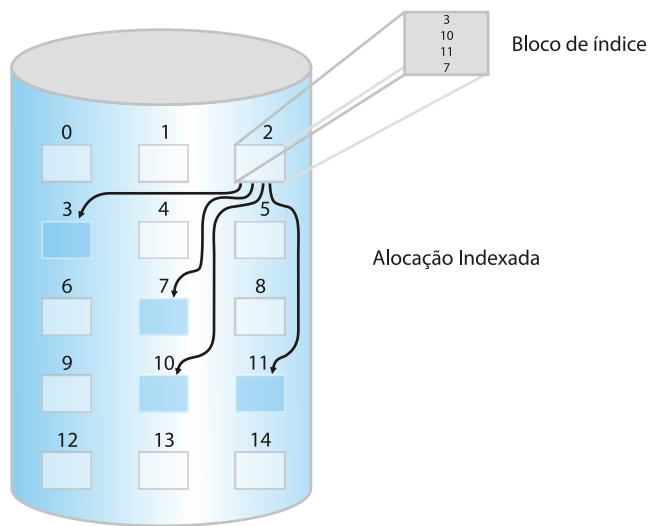


Figura 41 - Exemplo de Alocação Indexada de Blocos em Disco
Fonte: Adaptado de Machado e Maia (1997)

D'Imitre Camargo (2012)

Os modelos apresentados representam uma evolução na metodologia de alocação de arquivos em disco. Na sequência, você verá que uma é melhor que a outra, mas na prática, todos os modelos de alocação de arquivos possuem seus problemas.

No caso dos sistemas de arquivos Unix/Linux, o método de alocação de arquivos em disco se utiliza de uma estrutura de dados que engloba o conceito de uma lista encadeada junto com o conceito de índice. Essa estrutura de dados é denominada de *i-node*. Na figura a seguir, veja um modelo de alocação de um *i-node*, o qual possui os endereços de blocos alocados para o arquivo ou endereços para o próximo *i-node*, e assim sucessivamente.

Estrutura do i-node

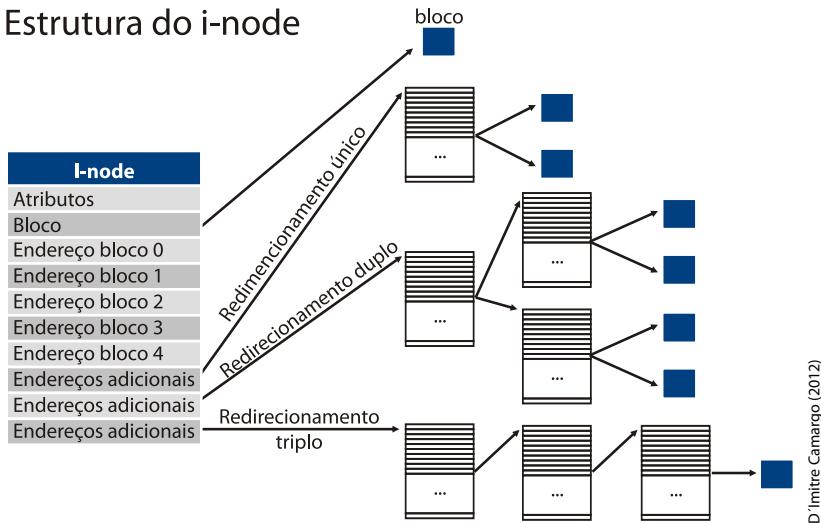


Figura 42 - Exemplo de Alocação de Blocos por um I-node
Fonte: Adaptado de Machado e Maia (1997)

O *i-node* será detalhado na sequência, quando veremos mais detalhes sobre os principais tipos de sistemas de arquivos.

E o que vem a ser sistema de arquivos?

Pode-se afirmar que sistema de arquivos é uma estrutura de dados organizada que possui a finalidade de armazenamento e recuperação de arquivos. O sistema de arquivos deve prover uma série de mecanismos de controle e gerenciamento, objetivando a integridade, a acessibilidade e a disponibilidade dos arquivos. De um modo geral, o sistema de arquivos é o tutor dos arquivos num sistema operacional.

As principais funções de um sistema de arquivos são:

- fornecer mecanismos/ferramentas para a manipulação de arquivos e diretórios;
- garantir a integridade dos arquivos e diretórios;
- otimizar o acesso aos arquivos e diretórios;
- permitir o acesso individual ou o compartilhado de arquivos e diretórios;
- possibilitar a recuperação de arquivos, em caso de problemas, na gravação ou leitura.

Como você viu, as funções não são nada simples, por isso é preciso lembrar que num servidor de rede podem haver centenas ou milhares de usuários acessando arquivos, e o controle de acesso aos arquivos torna-se uma tarefa fundamental, além das demais funções.

O sistema de arquivos do sistema operacional deve permitir aos usuários uma série de facilidades de acesso e trabalho com seus arquivos. Dentre as facilidades, é possível citar:

- a) poder criar, alterar, consultar ou excluir arquivos;
- b) definir as permissões de acesso aos seus arquivos;
- c) dar nome (nomear) aos seus arquivos;
- d) organizar seus arquivos em diretórios e subdiretórios;
- e) fazer *backups* de arquivos;
- f) recuperar arquivos em caso de deleção indevida ou em caso de danos.

Como os sistemas de arquivos são estruturas de dados em disco, organizadas com objetivo de manter arquivos, há sistemas com mecanismos mais otimizados que outros e que conseguem, por exemplo, ser mais rápidos na forma de ler ou gravar arquivos. Alguns sistemas de arquivos possuem ótimas ferramentas de recuperação em caso de danos, outros nem tanto. Há sistemas de arquivo que nem permitem a recuperação de arquivos, caso tenham sido deletados de forma indevida.

Os sistemas operacionais Unix/Linux suportam uma grande variedade de sistemas de arquivos (*filesystem*), dentre eles o Ext2, Ext3, Ext4 e o *Reiserfs*. Nos sistemas Windows, o sistema de arquivos predominante é o *NTFS*. No capítulo sobre Sistemas de Arquivos, o qual você irá ver adiante, haverá mais detalhes sobre os principais sistemas de arquivos utilizados em Unix/Linux e no Windows.

Veja mais detalhes e informações sobre sistemas de arquivos, ao consultar os seguintes links:



<<http://www.infowester.com/ntfs.php>>;
<http://web.mit.edu/rhel-doc/3/rhel-sag-pt_br-3/ch-ext3.html>;
<<http://www.guiafoca.org/cgs/guia/intermediario/ch-disc.html>>.

7.2 O I-NODE

O *i-node* ou nó índice é uma estrutura de dados com tamanho padrão de 128 bytes que descreve um arquivo, exceto o seu nome. O tamanho do *i-node* é definido na formatação do sistema de arquivos. Exemplo do comando: #mke2fs -t tamanho.

Alguns parâmetros no *i-node* são obrigatórios, como as permissões, o tamanho do arquivo e o endereçamento dos blocos alocados. Outros, embora úteis e quase sempre definidos, são opcionais, como o UID, GID, rótulos de tempo, etc.

A tabela seguinte mostra a estrutura de um *i-node*.

Tabela 2 - Estrutura de um *i-node*

BYTES	CAMPO	DESCRIÇÃO	BYTES	CAMPO	DESCRIÇÃO
0-1	i_mode	Permissões e atributos [1]	40-87	i_block	12 endereços de blocos
2-3	i_uid	UID: 16 bits menos significativos	88-91	i_block	Um endereço de bloco indireto simples
4-7	i_size	Tamanho do arquivo [2]	92-95	i_block	Um endereço de bloco indireto duplo
8-11	i_atime	Último acesso ao arquivo	96-99	i_block	Um endereço de bloco indireto triplo
12-15	i_ctime	Última modificação do <i>i-node</i>	100-103	i_generation	Número de geração (NFS)
16-19	i_mtime	Última modificação do arquivo	104-107	i_file_acl	Atributo estendido (ACL) do arquivo
20-23	i_dtime	Tempo de remoção do arquivo	108-111	i_dir_acl	ACL de diretório ou tamanho de arquivo [3]
24-25	i_gid	GID: 16 bits menos significativos	112-117	i_faddr	Informações de fragmentos [4]
26-27	i_links_count	Contador de <i>links</i>	118-119		Não usado
28-31	i_blocks	Contador de setores	120-121	i_uid_high	UID: 16 bits mais significativos
32-35	i_flags	Sinalizadores	122-123	i_gid_high	GID: 16 bits mais significativos

LEGENDA:

- [1] Contém sinalizadores (*flags*) de permissão e tipo: nove bits de permissão "rwx" - leitura, escrita e execução para o dono, grupo e outros; três bits definem o *sticky bit*, SGID e SUID; quatro bits identificam os tipos de arquivo (regular, diretório, dispositivo, *link* simbólico, etc.).
- [2] Se o arquivo tiver menos que 4GB; caso contrário, mostra os 32 bits mais significativos do tamanho—v. [3].
- [3] Caso o arquivo tenha 4GB ou mais, este campo mostra os 32 bits mais significativos do tamanho—v. [2].
- [4] O Ext2 não usa fragmentos.

O *i-node* contém dois registros para contar o tamanho do arquivo:

- a) (i) **i_size**, que mostra o tamanho em *bytes* (definido por dois campos de 32 bits);
- b) (ii) **i_blocks**, que, apesar do nome, mostra o número de setores ocupados pelo arquivo.

Agora que você conheceu os principais tipos de sistemas de arquivos, é necessário entender as atividades que envolvem o gerenciamento de arquivos pelo sistema operacional, o qual é o grande responsável pelos arquivos no computador.

Uma vez que os sistemas de arquivos já foram definidos e o sistema operacional já foi instalado, o acesso para criação de arquivos e diretórios fica liberado para usuários com as devidas permissões, ou seja, uma hierarquia de acesso é implementada pelo sistema operacional, a qual permite ou bloqueia a criação, a consulta, a exclusão ou a alteração de arquivos.



FIQUE ALERTA

Quando falamos do gerenciamento de arquivos não podemos esquecer que estes estão residentes em discos rígidos. Apesar dos dispositivos de redundância disponíveis hoje em dia, como o espelhamento de discos através do *RAID* nível 1, ou então com *RAID* nível 6 (onde pode-se perder até dois discos de um *array* de discos, ou seja, dispositivos que previnem a perda de dados), não podemos esquecer que todo servidor precisa de uma rotina de *backup*, pois não há gerenciamento de arquivos que resolva todos os problemas físicos. Uma rotina de *backup* é fundamental.

Nesta rotina, devem-se prever os dados mais importantes a serem copiados, a periodicidade da cópia e o meio de armazenamento do *backup*. Mas também, como regra básica, os arquivos de *backup* não devem ficar residentes no mesmo servidor, tampouco armazenados em outro disco. Todos os arquivos de *backup* devem ser retirados do servidor original, pois em caso de desastres, tais arquivos poderão ser restaurados em outro servidor.

Lembrem-se do caso de uma corretora de valores que tinha sua sede no *World Trade Center*. Esta corretora não pôde operar mais, nem mesmo em outro lugar, pois os sistemas desta empresa faziam *backup* na outra torre do complexo. Quando as duas torres foram destruídas pelo atentado de 11 de Setembro de 2001, todas as informações da empresa em documentos e em formato digital foram perdidas.

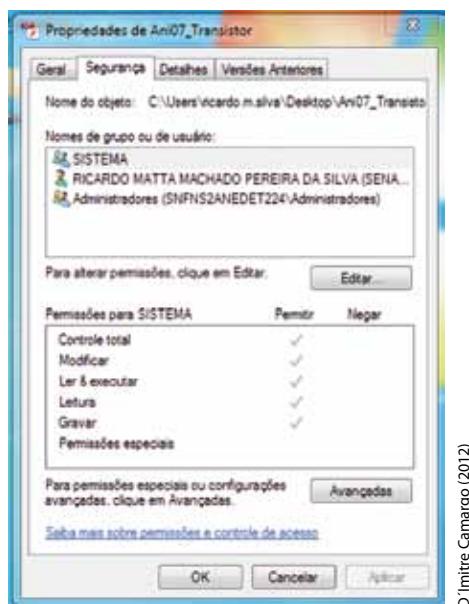
7.3 GERENCIAMENTO DE ARQUIVOS NO WINDOWS

Em sistemas Windows, as permissões de acesso ao sistema de arquivos são realizadas por meio do Windows Explorer, simplesmente navegando na estrutura de diretórios do sistema de arquivos. Ao escolher um diretório, basta clicar com o botão direito do *mouse* e o sistema irá lhe mostrar o conjunto de permissões de acesso do diretório selecionado. Este conjunto de permissões é o que se denomina de ACL – Access Control List, ou Lista de Controle de Acesso.

As permissões de segurança no sistema de arquivos NTFS, permitem ou negam ações nos arquivos e diretórios. Há possibilidade também de bloquear ou herdar permissões dos diretórios superiores. Desta maneira, as atividades de gerenciar acesso aos arquivos ficam facilitadas.

O controle do espaço em uso pelo sistema NTFS, assim como nos demais sistemas de arquivos, é controlado pelo próprio sistema operacional. A alocação de espaço em disco para novos arquivos e a liberação de espaço quando da exclusão de arquivos é uma atividade do próprio sistema operacional. A verificação do total de espaço utilizado e o espaço ainda disponível, nos sistemas Windows, poder ser realizada através do Windows Explorer, clicando-se com o botão direito em cima da partição C; por exemplo, em Propriedades.

Nesta mesma ferramenta há os *links* para as opções de manutenção do disco para realização de desfragmentações, e também para as definições de cotas de disco. Veja, na figura seguinte, o exemplo de uma lista de controle de acesso num diretório de um sistema de arquivos NTFS.



Dmitri Canargo (2012)

Figura 43 – Propriedades da Lista de Controle de Acesso – ACL no Windows – NTFS

No Windows, a definição de cotas de disco é realizada por volume e por usuário. Não se pode liberar cotas de disco para grupos de usuários, ou então cotas de disco somente para um diretório em específico. Deste modo, gerenciar cotas de disco em sistemas de arquivos NTFS é uma atividade trabalhosa.

Resumindo, nos sistemas Windows tem-se:

- a) administração de arquivos através da interface gráfico pelo Windows Explorer;
- b) o controle das permissões de acesso (ACL) poderá ser definido individualmente por arquivo ou por diretório, liberando-se ou negando-se permissões;
- c) as permissões são aplicadas para usuários específicos ou por grupo de usuários;
- d) o sistema permite herdar as permissões de diretórios superiores, ou então bloquear as permissões herdadas e então aplicar novas permissões de acesso;
- e) o sistema de arquivo poderá ser comprimido em tempo real, possibilitando compressão no volume todo, ou somente em um diretório individual;
- f) poderá também definir cotas de disco somente para usuários individuais e somente para o volume todo. Não são possíveis cotas por diretórios;
- g) as ferramentas de disco acessadas via Windows Explorer permitem a manutenção dos volumes, agendando uma verificação na próxima carga do sistema, fazendo desfragmentações e verificando a utilização dos volumes.

Acompanhe, a seguir, o Casos e Relatos que apresenta um exemplo sobre registro de arquivos em um banco de dados.



CASOS E RELATOS

Estouro de área em disco

O gerenciamento de arquivos, conforme foi visto, é uma tarefa do sistema operacional. Entretanto, o controle da quantidade de arquivos e do tamanho deles é uma das atividades que o administrador do servidor também deve realizar.

Num servidor de banco de dados, aconteceu com um usuário o estouro de área em disco, ao executar uma carga de registros remotamente para o servidor.

Foram tantos registros, que o arquivo de log do banco de dados estourou a área em disco disponível no servidor. Quando o sistema ficou sem espaço de trabalho, o *software* de banco de dados não conseguia mais realizar as transações. A única solução possível foi a cópia do arquivo de log para outro servidor e a remoção deste no servidor atual.

Após esta ocorrência, as atividades de carga de registros foram monitoradas com mais precisão, para evitar este tipo de acontecimento, pois se um sistema de arquivos ficar sem espaço, os processos que precisam acessar dados em disco, até mesmo para leitura, poderão parar de funcionar.

7.4 GERENCIAMENTO DE ARQUIVOS NO UNIX/LINUX

Para os sistemas Unix ou Linux, o gerenciamento de arquivos é uma atividade mais complexa do que no ambiente Windows. Isso ocorre devido à existência de vários tipos de sistemas de arquivos disponíveis e, também, pela necessidade de se conhecer os detalhes de cada sistema de arquivo, ao menos no processo de criação dos mesmos. Além de não existir em modo gráfico, todos os comandos são utilizados em modo de terminal.

Como você já conhece os tipos de sistemas de arquivos utilizados em Unix/Linux, é possível afirmar que, independente do tipo de sistema de arquivos, a organização dos diretórios é a mesma para todos eles, inclusive as definições e restrições nos nomes de arquivos de outras propriedades importantes.

A seguir, conheça algumas características importantes do sistema de arquivos no Unix/Linux:

- a) tamanho máximo do nome de arquivo é de 255 caracteres;
- b) pode conter mais de um ponto no nome do arquivo;
- c) diferencia maiúsculas de minúsculas (*case sensitive*);
- d) permite espaços no meio do nome dos arquivos;
- e) não existem extensões de arquivos como: .exe, .com, .bat, etc.

Os seguintes caracteres não podem ser utilizados em nomes de arquivos, pois permitem arquivos especiais, do tipo *Link simbólico*, *softlink* e *hardlink*:

! @ # \$ % ^ & * () { } [] “ ? | ; < > ` + - = \ / ..

O Linux marca alguns tipos de arquivos, conforme abaixo:

- a) arquivos executáveis possuem um * no final do nome;
- b) arquivos de *backup* possuem um ~ no final do nome;
- c) diretórios são marcados com um / no final do nome;
- d) arquivos do tipo *link* simbólico possuem um @ no final do nome;
- e) arquivos do tipo *socket* possuem um = no final do nome;
- f) arquivos do tipo *pipe* possuem um | no final do nome;
- g) diretórios ocultos possuem um . antes do nome.

Para visualizar estes caracteres nos nomes dos arquivos, basta digitar o comando **ls -F** e para visualizar os diretórios ocultos, digite **ls -a**.

Diversos tipos de arquivos não existem em outros sistemas, como o MsDOS, por exemplo. Veja na listagem seguinte os tipos de arquivos do Linux.

Arquivos Comuns: Suportam qualquer tipo de dado, seja ASCII, Unicode, arquivos comprimidos e até os programas executáveis (ou também chamados de arquivos binários).

Diretórios: São arquivos especiais que contém os nomes dos arquivos que estão armazenados ou organizados como um grupo. O agrupamento é arbitrário e você pode escolher a combinação desejada, ou seja, você pode definir os arquivos de seus diretórios.

Links simbólicos: Um *Link* é um arquivo que faz uma referência a outro arquivo ou diretório dentro do sistema de arquivos. Esta característica permite que um arquivo esteja em dois ou mais lugares ao mesmo tempo, na sua localização original e no lugar referenciado pelo arquivo de *link*.

Há dois tipos de arquivos de *Links*: O *Hard Link* cria novos nomes para um arquivo, associando assim dois ou mais nomes de arquivos para um mesmo *i-node* e este não pode ser visualizado. O *Soft Link*, ou link simbólico é o conjunto de arquivos que fazem referência ao arquivo original, contendo o caminho completo até o mesmo. Este tipo de arquivo pode ser visualizado com o comando **ls -F** ou **ls -l**.

Device (arquivos de dispositivos): São arquivos especiais que representam dispositivos no sistema, como um disco rígido IDE, por exemplo. Seria o arquivo **hda**, se este disco for o *Master* da primeira interface. Uma impressora paralela é um arquivo do tipo **lp0**. Os dispositivos de bloco, como os discos rígidos (**hda**),

são acessados em blocos de 1024 bytes por acesso. Já os dispositivos à caractere, como um terminal do tipo tty1 ou uma porta serial do tipo st0, são acessados *byte a byte*, ou seja, sequencialmente.

Sockets: São arquivos utilizados para comunicação entre processos, sendo estes processos executados na mesma máquina ou então em outro computador dentro de uma rede.

Pipes (dutos): São arquivos utilizados para intercomunicação entre processos, normalmente, processos locais.



Em geral, todos os arquivos do tipo *device* estão residentes abaixo do diretório /dev, que é um dos diretórios padrão do sistema Linux.

A estrutura de diretórios nos sistemas Unix/Linux é baseada em uma árvore de diretórios. Não existe o conceito de disco C: ou D: por exemplo. Na figura, veja uma estrutura típica de diretórios em um sistema Unix/Linux.

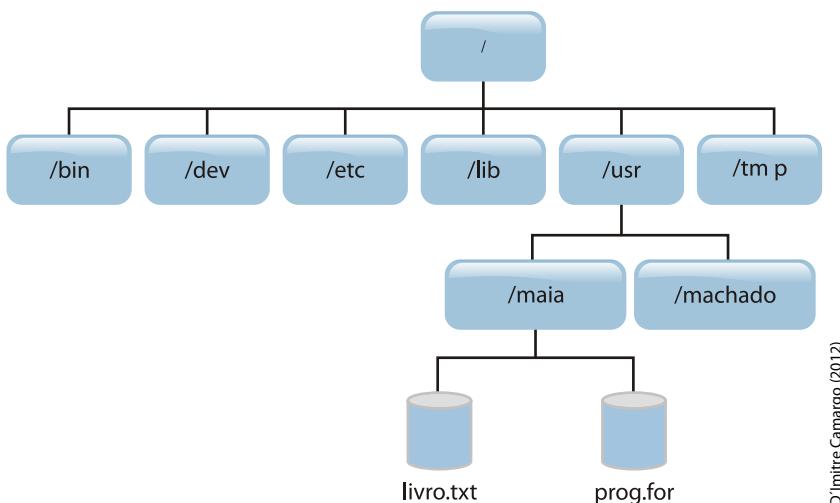


Figura 44 - Estrutura de Diretórios Típica. Sistemas Unix/Linux
Fonte: adaptado de Machado e Maia (1997)

As permissões de acesso aos arquivos em sistemas Unix/Linux é implementada de forma diferente do que nos ambientes Windows. Estas permissões aos arquivos e diretórios na estrutura das partições, num sistema GNU/Linux, obedecem ao modelo adotado nos sistemas Unix. Dentro deste modelo de permissões, há três categorias básicas para acesso aos arquivos e diretórios, que são:

- permissões de acesso do dono do arquivo;

- b) permissões de acesso do grupo ao qual o arquivo pertence;
- c) permissões de acesso aos demais usuários.

O **dono do arquivo** é normalmente quem cria o arquivo ou aquele definido pelo *root*. O **grupo do arquivo** é normalmente o grupo primário ao qual o seu dono pertence.

Para cada tipo de categoria que você acabou de conhecer, ainda há três tipos básicos de permissões, que são:

PERMISSÃO ABREVIATURA VALOR EM OCTAL		
Leitura	r	4
Escrita	w	2
Execução	x	1

Quadro 4 - Três tipos básicos de permissão

Permissão Abreviatura Valor em Octal

Leitura r 4

Escrita w 2

Execução x 1

Existem também permissões especiais que possuem funções diferentes das citadas anteriormente. Estas permissões são as seguintes:

SetUID: Se ativado em arquivos, ao ser executado será com o perfil do dono do arquivo. Não é usado para diretórios.

SetGID: Se ativado em arquivos, ao ser executado será com o perfil de algum membro do grupo do arquivo. Se ativado em diretório, os arquivos criados neste diretório terão seu grupo definido para o mesmo grupo do diretório.

StickyBit: Se ativado em diretório, os arquivos dentro deste diretório somente poderão ser excluídos pelos seus respectivos donos. Não é usado para arquivos comuns.

As permissões especiais possuem também valores no formato Octal:

Permissão Abreviatura Valor em Octal

Setuid s 4

Setgid s 2

Sticky t 1

As permissões efetivas em um arquivo no sistema são então obtidas pela soma de todas as permissões que você acabou de conhecer, aplicadas em todas as categorias, ou seja, para o 'dono', 'grupo do dono' e 'outros usuários'.

Na figura seguinte, você verá a representação de todas as permissões vistas no formato binário e como elas são tratadas, efetivamente, pelo sistema.

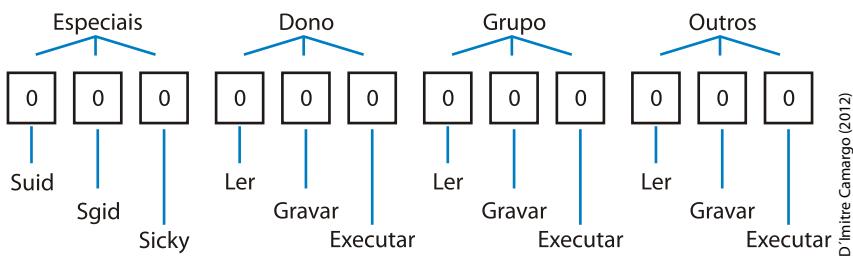


Figura 45 - Modelo de Permissões no Unix/Linux.
Fonte: Adaptado de Luiz Antonio Silva de Paula (2005)

Exemplos de permissões:

```
-rwsr-xr-x 1 root admin 26616 2005-04-19 14:48 /usr/bin/passwd
```

A figura que você viu, possui as seguintes permissões:

rws – Leitura, Escrita e *Suid* para o dono (dono é o usuário *root*);

r-x – Leitura e Execução para usuários do grupo do dono (grupo *admin*);

r-x – Leitura e Execução para os demais usuários.

A seguir, tem-se uma pequena listagem de arquivos na estrutura de diretórios de um sistema Linux, com a estrutura de permissões (ACL) apresentada individualmente por arquivo:

```
# ls -l /usr/sbin
total 13504
-rwxr-xr-x 1 root root 47276 2005-09-05 08:16 ab
lrwxrwxrwx 1 root root 2 2006-03-06 20:00 ab2 -> ab
-rwxr-xr-x 1 root root 6284 2005-12-12 11:54 accept
-rwxr-xr-x 1 root root 15240 2005-01-05 14:30 accessdb
-rwxr-xr-x 1 root root 18456 2004-11-01 08:26 acpid
```

O gerenciamento de permissões de acesso nos sistemas Unix/Linux poderá ser realizado em linha de comando, por meio das ferramentas *chmod* e *chown*. A primeira permite a mudança das permissões de acesso com relação à leitura, escrita ou execução, tanto para o dono, grupo ou demais usuários.

Já a ferramenta *chown*, permite a mudança na definição do dono do arquivo ou do grupo do arquivo. Deste modo, estas duas ferramentas conseguem gerenciar todas as características importantes do controle de acesso aos arquivos.

O gerenciamento do espaço em disco utilizado em sistemas Unix/Linux poderá ser realizado por meio da interface em modo terminal, através de comandos, ou também via interface gráfica, por diversos aplicativos.

A seguir, veja um exemplo da verificação da utilização do espaço em disco num sistema Linux, realizada por meio do comando *df-h*:

#**df -h**

Sist. Arq.	Size	Used	Avail	Use%	Montado em
/dev/sda4	60G	47G	11G	82%	/
tmpfs	1009M	4,0K	1009M	1%	/lib/init/rw
udev	1005M	236K	1005M	1%	/dev
tmpfs	1009M	0	1009M	0%	/dev/shm
/dev/sdb1	7,5G	7,1G	404M	95%	/media/usb
/dev/sda1	80G	74G	6,9G	92%	/ntfs



**VOCÊ
SABIA?**

Nos sistemas Unix/Linux, mesmo que seja indicado que um sistema de arquivos esteja com 100% de utilização, o sistema ainda reserva 5% (cinco porcento) de espaço livre para uso restrito do usuário administrador, no caso, o usuário *root*. Isto foi pensado para que o administrador possa resolver esta situação com um mínimo de espaço em disco para realizar esta tarefa, caso contrário, nem mesmo o administrador poderia resolver o problema.

Do mesmo modo, é possível perceber as mesmas informações por meio de uma ferramenta gráfica denominada *gnome-system-monitor*. Veja, na figura seguinte, as informações sobre os sistemas de arquivos disponíveis no computador em análise.

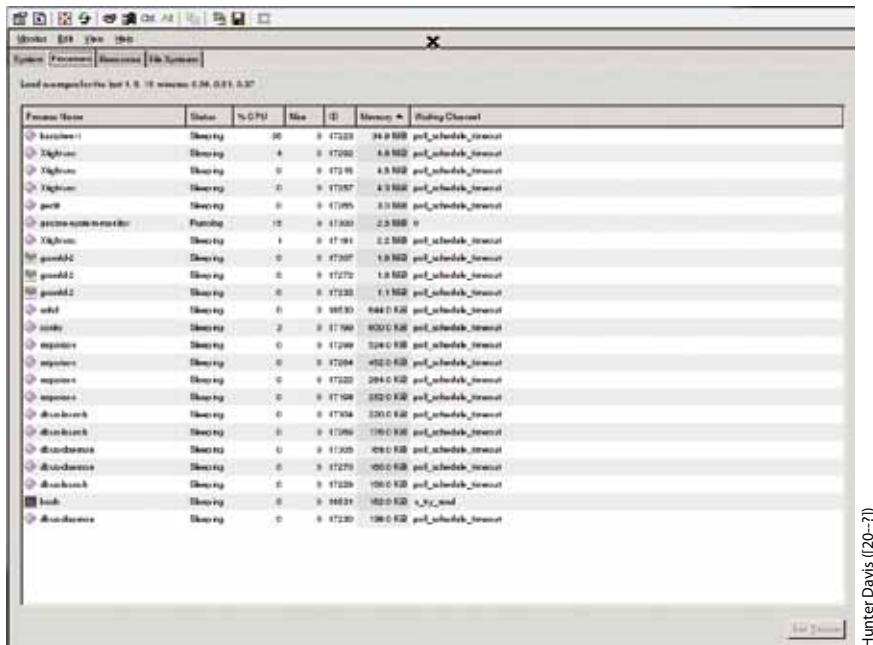


Figura 46 - Tela do Gnome System Monitor
Fonte: Adaptado de Luiz Antonio Silva de Paula (2011)

Como você pode ver, a ferramenta de visualização dos sistemas de arquivos apresenta diversas informações importantes para o gerenciamento de arquivos, mostrando as quantidades de espaço em uso e também o espaço ainda livre para uso. É importante também ressaltar que é possível ter todos os tipos de sistemas de arquivos instalados no sistema, sendo esta informação obtida na visualização da coluna *Tipo*, conforme a figura anterior.



RECAPITULANDO

Neste capítulo, foi possível conhecer os conceitos sobre gerenciamento de arquivos, que é uma das atividades do sistema operacional. Dos conceitos abordados, você estudou desde a definição de arquivos e diretórios e os tipos mais comuns de sistemas de arquivos, até exemplos de como gerenciar e obter informações sobre os sistemas de arquivos, tanto no Windows como no Linux.

Por meio dos conhecimentos abordados, você poderá gerenciar servidores de rede com relação aos aspectos do gerenciamento de arquivos e as questões que envolvem a segurança lógica dos arquivos diretórios e também da necessidade da rotina de *backup* dos servidores.

Gerenciamento de Acesso ao *Hardware*

8



Neste capítulo que inicia, você terá a oportunidade de conhecer os conceitos fundamentais sobre o gerenciamento de acesso ao *hardware* do computador. Você também verá que a função de acesso ao *hardware* é uma atividade do sistema operacional, além de saber como ele faz o acesso ao *hardware*, utilizando o conceito de camadas de *software*, dividindo tarefas em vários módulos do sistema, chamados de *drivers* de dispositivos e subsistemas de entrada e saída.

Após aprender os conceitos citados, você será capaz de:

- a) entender e compreender como funciona o acesso ao *hardware* do computador;
- b) compreender como o sistema operacional realiza o acesso ao *hardware*;
- c) compreender e entender o que é um *driver* de dispositivo e para que ele é utilizado;
- d) entender e compreender como é a arquitetura de um sistema Unix/Linux;
- e) entender e compreender como é a arquitetura de um sistema Windows.

Como você pode perceber, este será um capítulo muito interessante! Preparado para mais uma etapa de aprendizado? Lembre-se de que quanto mais você questionar sobre os conceitos estudados, mais você estará reforçando seu conhecimento sobre o assunto em debate.

8.1 ACESSO AO *HARDWARE*

É do conhecimento de muitos, por definições e conceitos de sistemas operacionais, que o acesso ao *hardware* do computador não é direto. Afinal, é para isso que os sistemas operacionais foram desenvolvidos, ou seja, para acessarem o *hardware* e fazê-lo trabalhar para o benefício do usuário.

Um sistema operacional possui diversas funções, e todas são fundamentais para que o sistema computacional funcione corretamente. A propósito, o sistema computacional é formado por *hardware* e *software*. Dessa forma, já que o gerenciamento de acesso ao *hardware* é uma função do sistema operacional, será apresentado de que maneira os sistemas operacionais Unix/Linux e Windows realizam esta tarefa em nosso benefício.

Nos sistemas Unix/Linux não há como acessar o *hardware* diretamente. É preciso antes passar pelo Kernel do sistema. Você sabe o que é Kernel? É o núcleo do sistema operacional Unix/Linux. Nele residem todos os módulos que implementam as gerências de recursos que precisamos, como as seguintes:

- a) gerenciamento de memória;
- b) gerenciamento de arquivos;
- c) gerenciamento de dispositivos.

Na figura a seguir, veja uma representação das camadas de *software* de um sistema Linux que envolvem o *hardware* do computador.

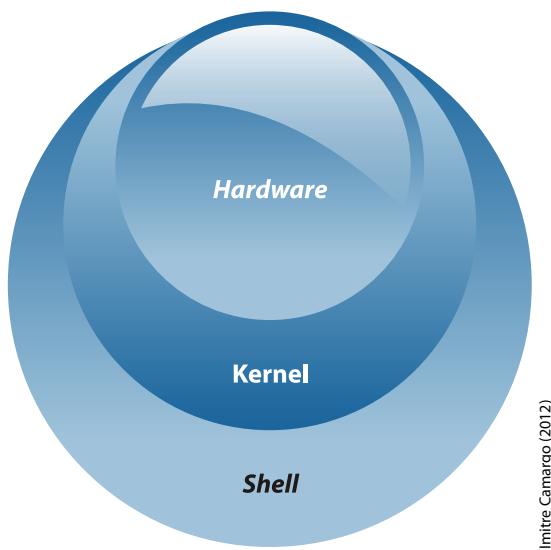


Figura 47 - Modelo de Camadas de *Software* num Sistema Linux
Fonte: Adaptado de Paula (2005)

Depois de conhecer o gerenciamento de memória e de arquivos, chegou o momento de conhecer o gerenciamento do *hardware*, com foco nos demais dispositivos que existem nos computadores.

Você sabe como se dá o acesso a um dispositivo de *hardware*?

O acesso deve partir de um programa do usuário, ou também do próprio sistema operacional. Quando um processo (que é um programa em execução) solicita um recurso de algum dispositivo de *hardware*, ele deve se comunicar com o subsistema de entrada/saída, ou subsistema de E/S. Este subsistema de Entrada/Saída então se comunica com o *driver* de dispositivo. Este *software* (driver de dispositivo) é quem se comunica com o controlador responsável pelo *hardware* instalado no computador.

Como você deve ter percebido, trata-se de um modelo em camadas, uma se comunicando com a outra, em que cada uma possui uma responsabilidade, uma função. Este modelo é particularmente útil, pois permite a segmentação de tarefas, e cada camada pode ser construída por pessoas ou equipes diferentes, como o que ocorre no mundo Linux.

Deste modo, é possível então criar novos dispositivos de *hardware* para coloca-los nos computadores, bastando somente escrever um novo *Device Driver* para ele, e então conectá-lo com o módulo de Entrada/Saída do sistema operacional. Assim, os programas de usuários poderiam acessar o novo *hardware*.

Na figura seguinte, veja uma demonstração das camadas de *software* necessárias para o funcionamento do sistema operacional.

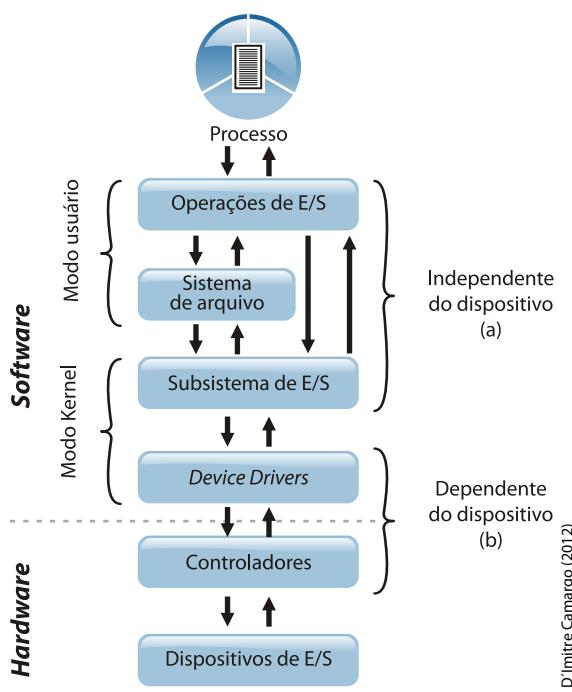


Figura 48 - Modelo de camadas de *software* para acesso ao *hardware*
Fonte: Adaptado de Machado e Maia (1997)



**SAIBA
MAIS**

Tenha em mente que nem sempre um novo dispositivo de *hardware* poderá ser suportado pelo sistema operacional. Para se manter atualizado sobre suporte dos sistemas operacionais e aos novos dispositivos de *hardware* lançados no mercado, consulte os fabricantes de sistemas operacionais quanto ao suporte para um novo *hardware*.

Para isso, acesse:

<<http://www.microsoft.com>>;
<<http://www.ibm.com/aix>>;
<<http://kernel.org>>;
<<http://www.apple.com/mac>>.

Apesar de parecer simples, o modelo de comunicação entre camadas de *software* no sistema operacional segue regras bem rígidas e muito bem definidas. Se não fosse assim, seria uma verdadeira desordem e ninguém conseguiria escrever um novo *device driver* para o Linux.

Na próxima figura, o conceito apresentado sobre a comunicação entre camadas de *software*, até chegar aos dispositivos de *hardware*, passando pelos *drivers* de dispositivos. É possível perceber, no modelo, que os *device drivers* são dependentes do dispositivo, ou seja, na verdade eles são construídos especificamente para cada dispositivo de *hardware* instalado no computador.

De uma maneira geral, para cada *hardware* instalado, deve-se ter um *device driver* instalado e reconhecido pelo sistema operacional. Caso contrário, não há como acessar o *hardware*, pois como visto, irá faltar algum *software* no modelo de comunicação de camadas.

Na sequência, a figura apresenta como cada *device driver* se encaixa no modelo de camadas de *software*, até chegar a um dispositivo de *hardware*.

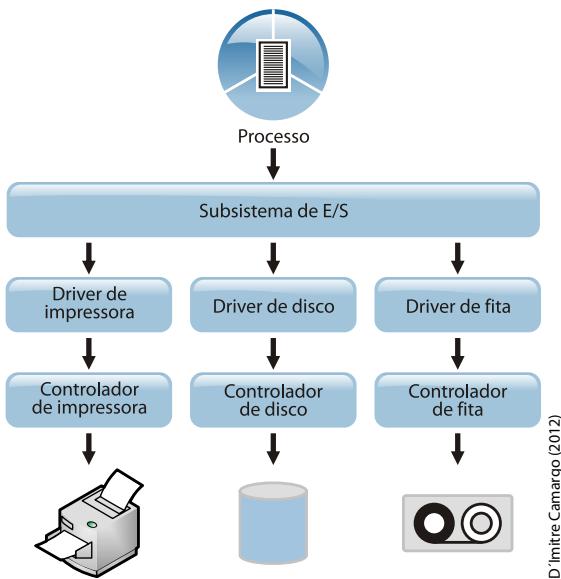


Figura 49 - Modelo de camadas com *driver* de dispositivos
Fonte: Adaptado de Machado e Maia (1997)

Quando a rotina de gerenciamento de arquivos necessita que um arquivo seja carregado em memória, ela solicita aos subsistemas de E/S um bloco a ser lido do disco. O subsistema então se comunica com o *device driver* do disco onde o arquivo se encontra, e solicita ao *hardware* controlador de discos a leitura de setores que contenham o bloco de informações solicitado.

Veja na figura a seguir, uma ilustração do processo de comunicação para acessar um arquivo.

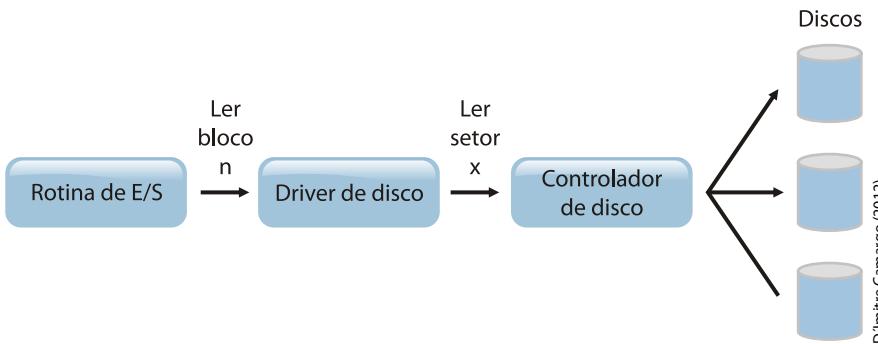


Figura 50 - Modelo de comunicação para acessar um arquivo
Fonte: Adaptado de Machado e Maia (1997)

O modelo de uma arquitetura de acesso ao *hardware* em camadas favorece a implementação de novos recursos aos sistemas operacionais. Na medida em que novos *hardwares* forem sendo desenvolvidos, estes deverão ser suportados através de novos *device drivers* e *softwares* de apoio (quando necessários).

**VOCÊ SABIA?**

O acesso ao *hardware* sempre deverá ser realizado através dos sistemas operacionais e, devido a este fato, uma tentativa de acesso direto por um programa de usuário pode comprometer a estabilidade e a segurança do sistema. É muito importante manter os sistemas operacionais atualizados, caso o seu servidor receba constantes atualizações no *hardware*.

Na arquitetura dos sistemas operacionais Windows também é implementado um modelo de camadas, em vários níveis. Neste sistema, para uma aplicação Cliente obter acesso de algum recurso do *hardware*, precisa passar por pelo menos quatro níveis, descritos a seguir.

- a) **Nível de aplicação de usuário:** Onde são executados os processos de usuários, que podem ser aplicações Win32 nativas do Windows, programas do antigo sistema OS/2 e aplicações Posix.
- b) **Fronteira do Modo usuário/Modo Kernel:** Neste nível, a biblioteca de *link* dinâmico NTDLL.DLL é quem faz a interface do Modo Usuário para o Modo Kernel.
- c) **Serviços do Sistema:** Neste nível, existem vários *drivers* que se comunicam diretamente com o Kernel do Windows. O *driver* para o sistema de arquivos se conecta diretamente ao Hal.dll, enquanto o *driver* de vídeo acessa o *hardware* diretamente, sem passar pelo Kernel do Windows ou pelo Hal.dll.
- d) **Nível de Abstração do Hardware:** Aqui é implementada a camada de abstração do *hardware*, a qual é executada pela biblioteca Hal.dll (*Hardware Abstraction Layer – Camada de Abstração do Hardware*). Esta camada realiza as solicitações oriundas do Kernel do Windows, acessando diretamente o *hardware*, logo abaixo.

Na arquitetura Windows, uma camada intermediária de abstração do *hardware* tem a função de esconder o *hardware* do resto do sistema. Ao mesmo tempo em que facilita acessos das camadas superiores, realizando as traduções de chamadas de *software* para chamadas de *hardware*, ela se torna um ponto crítico do sistema, pois em caso de falha nesta camada, todo o sistema fica comprometido.

**FIQUE ALERTA**

Se você sabe de programas de usuários que fazem acesso direto ao *hardware*, procure evitar que estes programas sejam executados para não deixar em risco o servidor de rede. Não há justificativas plausíveis para que um programa tenha acesso direto ao *hardware*, somente em alguns casos de recuperação de desastres em discos rígidos, ou então na tentativa de intrusão no sistema. Fique alerta!

Na próxima figura, você verá um modelo da arquitetura Windows, em que é possível visualizar os níveis de camadas envolvidos e os seus componentes.

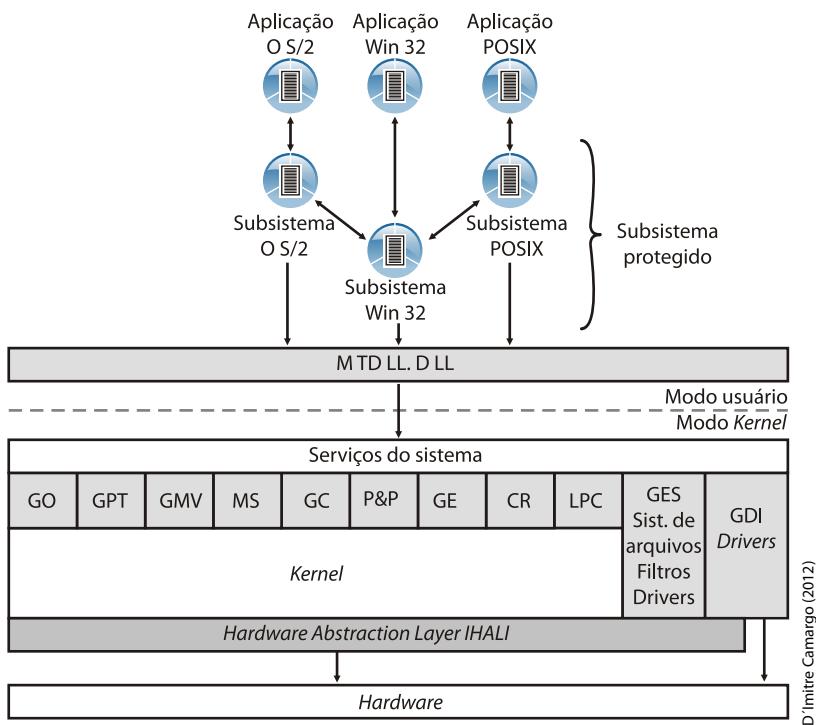


Figura 51 - Arquitetura do Windows
Fonte: Adaptado de Machado e Maia (1997)

Percebe-se que, independente da arquitetura do *hardware* ou do sistema operacional, não há como acessar dispositivos de *hardware* diretamente. Sempre haverá necessidade de um acesso intermediário no sistema operacional.

Seja no Windows ou no Unix/Linux, deve haver *drivers* de dispositivos específicos que mapeiam o dispositivo para o sistema operacional e que liberem os seus recursos para utilização por nossos programas. Acompanhe um caso de atualização do driver de vídeo, na situação seguinte.



CASOS E RELATOS

Atualizando *driver* de vídeo no windows

Certa vez, num sistema Windows, foi atualizado um *driver* de vídeo para que o servidor pudesse suportar maior resolução gráfica. O *driver* foi atualizado a partir do site do fabricante e estava em acordo com a placa gráfica instalada no servidor.

Após a atualização, o sistema ficou instável, chegando a congelar todos os processos, e a única solução possível foi a reinicialização do servidor, direto no botão. Sabemos que esta ocorrência é possível porque na arquitetura de acesso ao *hardware* do Windows, o *driver* de vídeo possui acesso direto e caso tenha problemas, o sistema todo fica comprometido.

A solução foi proceder à recuperação do servidor por meio de uma reinstalação completa do sistema operacional e, neste caso, não houve a perda de dados, pois o conteúdo dos arquivos em disco não foi comprometido.

As novas versões do Windows possuem mecanismos que ajudam a evitar este problema, uma vez que os fabricantes precisam certificar seus *drivers* para o sistema operacional.

Como regra geral, todos os novos recursos de *hardware* instalados em servidores de rede, por exemplo, precisam também ter seus *device drivers* instalados conjuntamente, caso os mesmos não estejam presentes no sistema operacional.

Outro fator importante para seu entendimento é que todas as configurações que são realizadas num sistema operacional, seja Unix/Linux ou Windows, somente podem ser realizadas por usuários com acesso privilegiado. Nos sistemas Windows estas atividades somente podem ser feitas por usuários com nível de Administrador.

Em sistemas Unix/Linux, as atividades de instalação de novos *device drivers* ou compilação de um novo Kernel, somente são realizadas pelo usuário *root* (nesses sistemas, o administrador é o próprio usuário).



RECAPITULANDO

Neste capítulo que você acabou de estudar, viu como o gerenciamento de acesso ao *hardware* é realizado pelos sistemas operacionais, trabalhando num modelo de camadas, onde um *software* se comunica com outro, para que todos possam se beneficiar dos recursos.

O modelo de camadas permite o conceito de abstração do *hardware*, onde os *softwares* nas camadas superiores não precisam conhecer os detalhes do *hardware*, mas somente requisitar os dados necessários.

Foi observada também a importância de não deixar um *software* acessar diretamente o *hardware*, pois este pode danificar um sistema.

Com estes conhecimentos, você está mais preparado para administrar servidores de rede, pois já sabe que o suporte para novos *hardwares* deve ser implementado pelo sistema operacional e, caso seja necessário, este deve ser atualizado.

Mecanismos de Segurança

9



Neste capítulo serão apresentados alguns mecanismos de segurança aplicados aos servidores de rede. Nesse sentido, o conceito de segurança será dividido em dois aspectos. No primeiro, você conhecerá os conceitos de segurança relacionados ao *hardware* de servidores de rede e ao seu ambiente. No segundo, serão apresentados os conceitos de segurança lógica para servidores de rede.

E ao finalizar este capítulo, você estará apto para:

- a) entender e compreender os conceitos sobre os mecanismos de segurança física e lógica relacionados com servidores de rede e seu ambiente;
- b) entender e compreender os conceitos básicos de segurança física e lógica;
- c) conhecer os mecanismos básicos sobre a segurança física de servidores;
- d) conhecer os mecanismos básicos sobre a segurança lógica de servidores;
- e) entender e compreender as boas práticas de segurança, ao aplicar segurança física e lógica para servidores de rede e seus ambientes.

9.1 SEGURANÇA FÍSICA E LÓGICA

Quando o assunto é segurança, seja física ou lógica, é preciso pensar de forma mais abrangente possível, pois vários aspectos relacionados a procedimentos do dia a dia das pessoas influenciam a segurança em sistemas de informação.

Como exemplo, uma empresa poderia ter um ambiente físico e lógico de alta segurança, com controles de acesso, senhas trocadas com periodicidade, proteções lógicas nos sistemas, enfim, uma série de mecanismos de segurança, sendo que isso tudo não adiantaria em nada se o administrador da rede desta empresa não cuidasse de fatores simples e pessoais, como: uma senha de acesso privilegiado; senhas de fácil descoberta; ou também levando e trazendo programas do trabalho para sua casa e vice-versa.

Estes procedimentos quebram qualquer arranjo de segurança pois, afinal de contas, todo tipo de segurança possui um ponto fraco. A segurança, em termos gerais, é tão forte quanto seu elo mais fraco. É igual a uma corrente. Por isso, devemos pensar em segurança de um modo mais geral, não somente limitando ao que fazemos ou utilizamos como ferramentas de trabalho, como servidores de rede, microcomputadores, *pen-drives*, etc.

No final da década de 90, muitas empresas criavam salas especiais para colocar os equipamentos de tecnologia, e o acesso era muito restrito. Praticamente somente analistas e gerentes das áreas de tecnologia tinham acesso. Entretanto, as salas precisam ser limpas, então, quando as senhoras da limpeza precisavam limpar a sala dos computadores, alguém entrava com elas e acompanhava. Com o decorrer do tempo e fruto da rotina diária, ninguém mais acompanhava o serviço.

Quer saber o que poderá acontecer de errado numa situação como esta? Então acompanhe o caso a seguir.



CASOS E RELATOS

O problema da limpeza

Numa certa manhã, todos os terminais de acesso aos sistemas da empresa pararam de funcionar. Foi aquela correria pra tentar descobrir o que houve, pois tudo estava em *No-break*, a sala era de acesso restrito, etc.

Após procurar por todos os lados na sala de equipamentos, verificaram que uma tomada elétrica da CPU estava desconectada da energia. Ela foi desconectada, conforme relato da senhora que fazia limpeza, quando

passava uma vassoura atrás do gabinete da CPU, que estava com muita poeira. Como não aconteceu nada, ela continuou com seu serviço.

A moral da história mostra que não há segurança de acesso e *No-break* que suporte uma vassoura de limpeza. Essa situação mostra que, por mais simples que sejam os procedimentos de segurança, nunca se deve deixá-los de lado, pois numa falha como esta, tudo pode ficar comprometido. Após aquela ocorrência, os próprios analistas se encarregaram da limpeza da sala de computadores.

Hoje em dia, as conexões elétricas e de *racks* de equipamentos são mais seguras, e alguns modelos possuem dispositivos que impedem uma desconexão simples, mas quando o assunto é segurança, sempre se deve estar atento.

9.2 MECANISMOS DE SEGURANÇA

A segurança física para servidores de rede envolve o *hardware* do servidor e o ambiente em que está instalado. Neste sentido, vários aspectos de segurança devem ser observados e os mecanismos que atendem aos quesitos de segurança precisam ser implementados.

Com relação ao **ambiente físico de servidores de rede**, é necessário saber:

- a) o ambiente físico precisa conter controle de umidade, temperatura e poeira, devendo possuir equipamentos para este fim, como condicionadores de ar, desumidificadores ou umidificadores, com filtro de proteção para poeira e fumaça;
- b) o ambiente deve possuir um sistema básico de controle de incêndio, pois os servidores de rede com média ou alta especialização no *hardware* geram bastante calor, se possível, deve-se instalar detectores e alarmes de incêndio;
- c) controle de acesso individual, onde somente pessoas autorizadas poderão ter acesso ao ambiente, e cuja solução seria o uso de chaves automáticas com controle biométrico de identificação e com certificação digital;
- d) instalação elétrica adequada, planejada e que atenda à demanda de carga dos servidores de rede e aos ativos de rede, como *switchs*, roteadores e *modems*.



iStockphoto (20-2)

Figura 52 - Leitor Biométrico para Controle de Acesso

Com relação ao **hardware de servidores de rede**, é necessário saber:

- a) servidores de *rack* instalados em *rack* de servidores adequados para o acondicionamento do servidor e conforme as especificações dos fabricantes;
- b) servidores de mesa, ou tipo *Desktop*, devem ser instalados também em *rack* com prateleiras;
- c) alimentação elétrica adequada e com suporte à carga total de todos os equipamentos que operarem no ambiente, incluindo sistema de aterramento, polarização correta de tomadas e nas quantidades suficientes para a ligação dos equipamentos;
- d) servidores devem ser ligados à rede elétrica, se possível por meio de duas fontes redundantes, em que cada uma deve ser conectada em circuitos elétricos distintos e com alimentação proveniente de um sistema de *No-break* ou, no mínimo, com estabilização;
- e) servidores de rede, sempre que possível devem possuir dispositivos redundantes como interfaces de rede, controladoras de disco e discos rígidos;
- f) os gabinetes devem ser mantidos fechados sob chaves, com acesso restrito da equipe de ambiente;
- g) o acesso para manutenção deve ser realizado sob supervisão de pessoas do ambiente do servidor, nunca deixando técnicos trabalharem sozinhos nos ambientes;
- h) em manutenções que envolvam a substituição de peças que exijam o desligamento completo do servidor, o mesmo deve ser desligado (logicamente) antes, devendo este procedimento ser agendado previamente, para não comprometer os trabalhos dos usuários ou possíveis perdas de dados;

i) em todas as situações de manutenção física no *hardware* de servidores, os técnicos devem utilizar pulseira antiestática, para não comprometer o sistema com possíveis cargas estáticas e consequentemente acarretar em danos em memórias, discos magnéticos e demais componentes.

Em muitos casos, nas instalações onde os servidores de rede residem, podem não haver as condições ideais de segurança, no entanto, elas devem ser perseguidas e obtidas com o decorrer do tempo. Servidores de rede, em geral, possuem grandes responsabilidades e, muitas vezes, armazenam informações valiosas para as empresas.

A perda de dados, ou mesmo do tempo de inatividade na restauração de um servidor de rede, pode custar muito mais do que a implantação dos dispositivos de segurança, conforme apresentados neste livro didático.

Veja mais informações sobre segurança, acessando os *links* a seguir:



<<http://www.cert.br>>;
<<http://www.iti.gov.br/twiki/bin/view/Certificacao/CertificadoConceitos>>;
<<http://sergurancalinux.com>>;
<<http://www.linhadefensiva.org>>.

9.3 MECANISMOS DE SEGURANÇA LÓGICA

Praticamente todos os sistemas operacionais de rede possuem diversos mecanismos de segurança lógica. Seja um sistema operacional Windows ou Unix/Linux, a segurança lógica deve ser implementada, e se os mecanismos de segurança não forem suficientes, poderão ser adquiridos por terceiros. Neste caso, tem-se como exemplo os sistemas Antivírus, em que este tipo de *software* de segurança não faz parte dos sistemas operacionais.

A segurança lógica também pode ser pensada em níveis de implementação, desde os dispositivos onde estão guardados os dados, como discos rígidos, unidades de fita, DVD-ROM, até o acesso inicial de um usuário no processo de login.

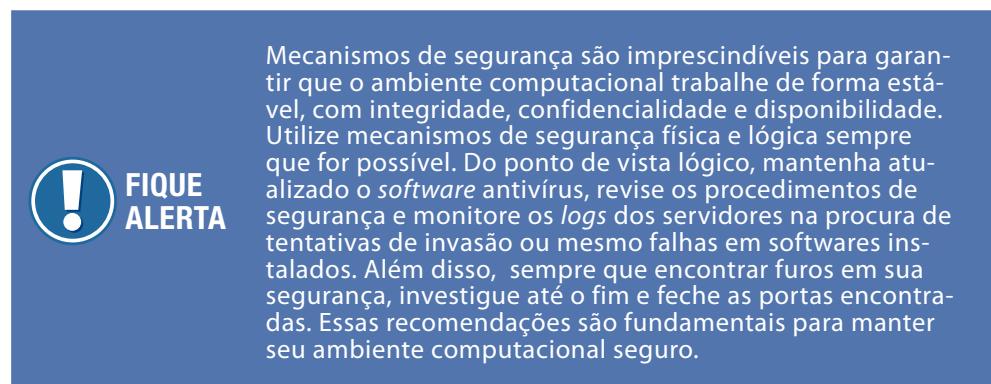
Um fator a ser pensado na segurança lógica de servidores é que podemos implementar um nível elevado de segurança, aplicando-se também dispositivos para alta disponibilidade. Desta maneira, alta disponibilidade de um servidor também poderia ser pensada como um fator de segurança, pois o *hardware* ga-

rante a disponibilidade. A integridade e confidencialidade dos dados devem ser garantidos por outros mecanismos do sistema.

Conforme já visto, não existe sistema de segurança perfeito, mas ainda assim é necessário ficar atento às senhas de acesso aos sistemas.

Servidores de rede devem ser mantidos e administrados por pessoas restritas, ou seja, não pode ou não deve haver muitas pessoas responsáveis por um servidor de rede ou mesmo um grupo de servidores. Isso é importante porque as senhas de acesso dos administradores dos sistemas operacionais são tão importantes quanto o próprio servidor físico e suas informações.

Deste modo, deve haver regras claras e bem definidas para as senhas administrativas, e todos os administradores dos servidores devem ter ciência delas e saberem como proceder em cada caso.



Mecanismos de segurança são imprescindíveis para garantir que o ambiente computacional trabalhe de forma estável, com integridade, confidencialidade e disponibilidade. Utilize mecanismos de segurança física e lógica sempre que for possível. Do ponto de vista lógico, mantenha atualizado o *software* antivírus, revise os procedimentos de segurança e monitore os *logs* dos servidores na procura de tentativas de invasão ou mesmo falhas em softwares instalados. Além disso, sempre que encontrar furos em sua segurança, investigue até o fim e feche as portas encontradas. Essas recomendações são fundamentais para manter seu ambiente computacional seguro.

Objetivando melhorar a segurança lógica, conheça os principais mecanismos que podem e devem ser implementados em servidores de rede:

- a) as senhas dos usuários administradores de rede, como a do *root* em sistemas Unix/Linux ou a do Administrador em sistemas Windows, devem ser de conhecimento somente dos responsáveis direto dos servidores envolvidos e devem obrigatoriamente ser trocadas de 30 em 30 dias;
- b) senhas administrativas devem possuir um tamanho com mais de 8 caracteres, sendo constituídas por números e letras, com maiúsculas e minúsculas e não devem referenciar alguma data, local específico, nome de pessoas, animais, palavrões, apelidos, etc.
- c) os servidores de rede devem utilizar sistemas de arquivos com *array* de redundância de discos *RAID*, nos níveis 1, 5, 6 ou 10, onde o mais indicado para utilização seria o *RAID* nível 6, pois suporta até a perda de dois discos físicos do conjunto no *array*.

- d) configurar os sistemas operacionais para gravar em *log* ações consideradas críticas no sistema, como deleção de arquivos, formatações de discos, *backups* e, até mesmo, registrar os acessos indevidos;
- e) configurar os sistemas operacionais para permitir logon direto no servidor somente para os administradores do ambiente e somente de dentro da rede interna do servidor, bloqueando acessos remotos de outras redes, como por exemplo, da Internet;
- f) não instalar *softwares* desnecessários em servidores de rede, deixando somente os *softwares* que serão de fato utilizados pelos usuários ou pelos administradores do ambiente;
- g) não deixar *softwares* com portas de rede abertas para conexão de redes remotas, caso não seja estritamente necessário, como exemplo, de um servidor WEB que atende somente usuários e sistemas da Intranet, onde mesmo este servidor tendo conexão com redes remotas, deve-se bloquear o acesso através de *firewall* no servidor ou nas configurações internas dos *softwares*;
- h) para redes médias ou grandes, em que pode haver uma grande quantidade de usuários, um sistema de autenticação centralizado de usuários e grupos deve ser utilizado, como por exemplo, sistemas LDAP para Unix/Linux e Active Directory para ambientes Windows;
- i) os sistemas utilizados internamente, ou mesmo disponibilizados para acesso remoto, devem autenticar e autorizar usuários e todas as conexões com informações importantes, como de Login e Senha. Devem, ainda, trafegar sob criptografia, com a utilização de certificados digitais rodando, como o protocolo HTTPS;
- j) para sistemas Unix/Linux, os administradores devem mapear todos os programas executáveis, ou mesmo *scripts* do sistema, que tenham as permissões de SetUID ou SetGID definidas. Estas permissões especiais devem ser controladas, pois podem servir como porta para invasão do sistema. Esta verificação deve ser realizada periodicamente, em todos os sistemas de arquivos dos servidores;
- k) instale sistemas antivírus em servidores de rede para prevenir proliferação de vírus e programas suspeitos que podem ter sido instalados remotamente ou deixados nos servidores junto com outros *softwares* para infestação da sua rede.

Enfim, podemos ver que existe uma grande quantidade de procedimentos e mecanismos de controle que podemos implementar nos servidores de rede, os quais irão melhorar muito a segurança.

Na figura a seguir podemos ver a imagem de um *Data Center*. *Data Center* é um local onde são acondicionados centenas de servidores de rede e equipamentos de comunicação, como roteadores, *switches* e *modems*.



Figura 53 - Data Center

Normalmente os racks de servidores ficam sob um assoalho elevado com furos. Por meio destes furos, o ar-condicionado refrigerado sobe e passa por eles, refrigerando os servidores de rede. No alto dos racks devem constar os dispositivos de fluxo de ar que retiram o ar quente. No teto, deve conter os sensores de detecção de fumaça e de temperatura, em caso de incêndio.

Os *Datacenters* são os locais mais apropriados para colocar os servidores de rede, pois possuem estruturas completas de segurança de acesso físico e lógico, contando com vários dispositivos que permitem o funcionamento do ambiente de forma ininterrupta. Geralmente os *Datacenters* apresentam as seguintes características:

- a) sistemas de *No-Break* de grande capacidade;
- b) grupo Gerador para o fornecimento de energia em caso de pane na rede elétrica;
- c) dispositivos de controle de acesso biométrico;
- d) sistemas de *Firewall* para proteção da rede de computadores;
- e) sistemas de monitoração da temperatura, de fumaça e de umidade;
- f) sistemas de monitoração dos *racks* dos servidores, dos próprios servidores e também de seus subsistemas de disco, fontes de alimentação, dentre outros.



VOÇÊ SABIA?

Os bancos são as empresas que mais investem em tecnologia da informação e principalmente em segurança, por se preocuparem em cuidar do dinheiro de seus clientes. Segundo a FEBRABAN – Federação Brasileira de Bancos, em 2010 foram gastos R\$ 22,026 bilhões de reais com tecnologia da informação. E somente em segurança, o valor estimado foi de R\$ 2 bilhões de reais. Estes dados mostram o quanto a segurança da informação é valiosa e o quanto é necessário pensar em segurança de maneira responsável, pois boa parte das informações sigilosas ficam armazenadas no mundo digital.

Mesmo que o orçamento para investir em segurança seja pequeno, os procedimentos lógicos apresentados podem auxiliar muito na implementação da segurança dos servidores.

Os administradores de servidores de rede devem perseguir os quesitos de segurança nos equipamentos sob sua responsabilidade, implementando configurações, verificando *logs* de acesso, fechando portas, conferindo acessos e tentativas de invasão, etc. Estas atividades não são difíceis de realizar, porém, asseguram, sob o ponto de vista lógico, um nível de segurança aceitável nos seus servidores de rede.



RECAPITULANDO

Neste capítulo foram apresentados os conceitos que envolvem os mecanismos de segurança, especificamente, os mecanismos de segurança física, que são capazes de garantir a estabilidade nos sistemas computacionais, pois são elementos físicos, tais como: componentes redundantes em servidores de rede, *no-breaks*, sistemas de ar-condicionado, alarmes contra incêndio, dentre outros, que garantem o sistema e o ambiente.

Você também conheceu os mecanismos de segurança lógica, os quais podem ser implementados num sistema operacional, independente de recursos financeiros, pois todos os recursos de *software* já estão disponíveis para uso. Conheceu, ainda, os diversos dispositivos lógicos de segurança que, se aplicados e utilizados diariamente, implementarão segurança no ambiente computacional.

Estes conceitos, assim como os que você conheceu, são de grande relevância para seu conhecimento, pois das atividades de administração de servidores de rede, as relacionadas com segurança são as mais importantes e relevantes, onde o desafio diário é manter seu ambiente seguro, tanto física quanto logicamente.

Trabalhando com Discos e Sistemas de Arquivos

10



Nesta parte do conteúdo, serão apresentados os tipos de sistemas de arquivos mais utilizados em sistemas operacionais, bem como a forma como os dispositivos são montados no Linux. Você estudará também os tipos de discos de armazenamento e como preparar os discos para receberem o sistema de arquivos.

Ao finalizar este estudo, você terá subsídios para:

- a) conhecer os tipos de sistemas de arquivos;
- b) compreender o que é uma área de troca ou *swap*;
- c) compreender o que é um disco scsi, sata e ide;
- d) saber criar partições e formatar partições;
- e) saber montar e desmontar um dispositivo no Linux;
- f) gerenciar um sistema de arquivo.

¹ JOURNALING

Permite ao sistema operacional gravar log de toda e qualquer alteração, antes mesmo que esta seja gravada no disco. Desta forma, ajuda o sistema a não sofrer perda de dados.

10.1 SISTEMAS DE ARQUIVOS

Você sabe o que são sistemas de arquivos? Os sistemas de arquivos são estruturas lógicas criadas após a formatação do disco rígido, permitindo que arquivos sejam criados e manipulados pelos usuários. Os sistemas também permitem que o sistema operacional possa controlar o acesso aos discos, leitura e gravação.

Os sistemas de arquivos foram projetados para serem robustos e flexíveis.

A seguir, conheça os tipos de sistemas de arquivos.

10.1.1 TIPOS DE SISTEMAS DE ARQUIVOS

Os sistemas de arquivos são variados para os diversos tipos de sistemas operacionais, seja em uma arquitetura aberta ou fechada. A escolha correta do sistema de arquivo dependerá da finalidade do equipamento. Uma característica importante para os sistemas de arquivos é a existência de suporte a *journaling*¹. A *journaling* tem por finalidade recuperar um sistema mediante desastres que venham a acontecer no disco. Desta forma, os sistemas de arquivos atuais que possuírem este suporte são os preferidos. Conheça alguns destes sistemas.

Ext2 – Second extended file system: Este sistema é uma atualização dos sistemas EXT, que possuíam algumas limitações e por isso foram substituídos pelo EXT2. Este tipo de sistema é apropriado para disco, disquetes e *pen-drives*, ou seja, dispositivos de bloco. O EXT2 é o sistema de arquivo padrão do Linux.

Uma importante atualização em relação ao sistema EXT foi a alteração do tamanho máximo da partição, que passou para 2TiB. Os arquivos também tiveram seu tamanho máximo alterado para 2GB. Este sistema, por não ter suporte a *journaling*, foi substituído pelo EXT3.



VOCÊ
SABIA?

TiB significa tebibyte. 1 TiB equivale a 1.099.511.627.776 bytes.

Ext3 – Third extended file system: Este sistema possui as mesmas características dos sistemas EXT2, porém, com o acréscimo do suporte ao *journaling*.

Reiserfs: Este sistema é de recente criação, mas já está sendo o mais usado nas distribuições Linux atualmente. O seu desempenho é melhor que os EXT3, principalmente quanto ao uso de uma grande quantidade de arquivos pequenos. Também possui suporte ao *journaling*.

Uma desvantagem deste sistema é que consome muito processamento da CPU.

Xfs: Assim que foi desenvolvido, este sistema era proprietário, ou seja, possuía um dono e para usar este sistema de arquivo era necessária a aquisição de licença de uso. Mas logo seu código foi aberto e compilado para o Linux. Seu uso é recomendado em sistemas que usam banco de dados, por sua velocidade de gravação. Também possui suporte ao *journaling*.

JFS: Este sistema de arquivo foi criado pela IBM para ser utilizado em servidores corporativos. Utiliza uma estrutura *inode* para gravar a informação dos blocos de cada arquivo no disco. O JFS hoje possui seu código aberto e está na sua segunda versão, denominada JFS2. Ele continua com a estrutura *inode*, só que em árvores binárias, o que deixa a busca de informações mais rápida.

Swap: Este sistema também é conhecido como memória virtual, ou seja, a *swap* funciona como uma auxiliadora da memória RAM. Sabendo que só a memória principal é processada, quando a memória RAM está sobrecarregando o sistema, esta retira automaticamente as informações que não estão sendo utilizadas e envia para a memória virtual, liberando espaço na memória RAM principal. Por realizar esta troca de dados entre a memória física e virtual, também é conhecida como ‘área de troca’.

Vfat: Este sistema também é conhecido como FAT16 e FAT32, bastante utilizado no sistema operacional Windows, pen-drives e cartões de memória. Não possui suporte ao *journaling* e nem atributos de permissão de arquivos e pastas e causa bastante desperdício de disco.

NTFS – New technology file system: Este sistema de arquivo é padrão para o Windows NT da Microsoft, mas também é utilizado em Windows 7 e Windows XP. Não possui suporte ao *journaling*, mas possui atributos de permissão de arquivos e pastas, porém, são mais lentos que os sistemas FAT32. Com o NTFS, o problema de desperdício de disco com o VFAT foi resolvido.

Para que os sistemas de arquivo sejam criados, é necessário que existam partições criadas no disco rígido. Nas próximas páginas, você verá como estas partições são criadas e como gerenciar o sistema de arquivo após sua criação.

10.2 AGRUPAMENTO DOS ARQUIVOS

Você está lembrado que o sistema de arquivo cria uma estrutura para que o sistema operacional possa controlar o acesso ao disco? Pois agora você aprenderá como essas partições são criadas e como são gerenciadas.

A criação de partições e formatação se dá, preferencialmente, no momento em que é instalando o sistema Linux de sua preferência, seja qual for a distribui-

² DISPOSITIVO

No Linux, dispositivos são os componentes dos hardwares e do sistema operacional.

³HOT-SWAP

Esta tecnologia permite que a troca do disco seja efetuada sem a necessidade de desligar o computador.

ção GNU/Linux. Os diferentes tipos de sistemas de arquivos possuem suas próprias particularidades, mas todos possuem o mesmo propósito, que é ler e gravar. Conheça um pouco sobre os dispositivos de armazenamento.

Dispositivos: O Linux possui suporte a diversos dispositivos²: disco SCSI, disco IDE, disquetes, CD-ROM, PEN-DRIVE, etc. Estes dispositivos podem ser formatados como sistema de arquivo padrão do Linux (o EXT2 ou EXT3) ou, ainda, em outro tipo de sistema de arquivo de sua escolha, como os do tipo *journaling* ou *reiserfs*, ou os oriundos da Microsoft FAT, FAT16, FAT32 e NTFS. O Linux é um dos poucos sistemas que possui uma grande variedade de sistema de arquivo à disposição do usuário.

Discos: Os discos são os locais utilizados para o armazenamento dos dados e sistema operacional. São nos discos que estão configuradas as partições. Saiba um pouco mais sobre os tipos de discos existentes.

IDE – Integrated Device Electronics

O IDE foi o primeiro disco a ser utilizado e era, até pouco tempo, o mais utilizado devido ao seu baixo custo (se comparado aos discos SCSI), além de possuir uma capacidade de armazenamento boa.

As placas *motherboard* (placas-mãe) possuíam duas conexões para os discos IDE, uma primária e outra secundária, e tais conexões eram utilizadas por discos ou CD-ROM. Em cada conexão IDE é possível colocar dois discos ou um disco e um CD-ROM. Para realizar esta configuração, é necessário configurar o disco ou CD-ROM com *jumper*, informando que um será o primário master e o segundo, o primário escravo. Para a segunda conexão o princípio é o mesmo.

SCSI – Small Computer System Interfaces

Este tipo de disco possui uma *performance* e durabilidade maior e melhor que os discos IDE. Por este motivo custam mais caros e são geralmente utilizados em servidores. As placas-mãe mais antigas necessitavam de uma controladora SCSI externa conectadas à PCI, para conexão com o disco SCSI. As placas-mãe atuais já possuem a controladora acoplada. Ao contrário do IDE, que permitia apenas quatro discos (dois em cada conexão), o SCSI permite a instalação de até 15 tipos de dispositivos diferentes, ou seja, disco, CD-ROM, unidade de fita *dat*, entre outros. Outra particularidade dos discos SCSI é a funcionalidade *hot-swap*³.

SATA – Serial Advanced Technology Attachment

Este tipo de disco é o mais utilizado no momento, surgiu em meados do ano 2000, tornando-se referência de mercado, assim que os fabricantes de *motherboard* deixaram de colocar em suas placas as conexões IDE. O disco sata é mais rápido que os IDE e sua performance é semelhante aos discos SCSI. Possui também a funcionalidade *hot-swap*.

A desvantagem do SATA é que uma conexão ou canal só pode ser utilizada por apenas um dispositivo disco, CD-ROM, etc.

Agora que você já conhece os tipos de discos e suas particularidades, saberá como os discos são mostrados ou nomeados no Linux.

Nos sistemas Linux, o local padrão dos dispositivos é /dev.

nomeação da localização dos discos:

/dev – localização do dispositivo;

/hd – faz referência a um disco ide;

/sd – faz referência a um disco scsi ou sata.

nomeação do Disco ide:

/dev/hda – interface primária master;

/dev/hdb – interface primária escrava;

/dev/hdc – interface secundária master;

/dev/hdd – interface secundária escrava.

nomeação do Disco scsi/sata:

O funcionamento é o mesmo dos discos IDE.

/dev/sda – disco no primeiro canal;

/dev/sdb – disco no segundo canal;

/dev/sdc – disco no terceiro canal.

A quantidade de disco SCSI conectados em um equipamento (servidor) poderá chegar até o máximo de 15 discos. Já os discos sata dependerão da quantidade de conexões sata disponíveis na placa *motherboard*.

10.3 PARTICIONAMENTO

Ao instalar um dispositivo de bloco (disco), é necessário, antes de utilizá-lo, fazer a formatação e criar, no mínimo, uma partição para o funcionamento do sistema de arquivo. É possível criar outras partições, mas não é obrigatório. Os sistemas Linux aceitam a criação de até quinze partições, que são representadas por um número inteiro, como o exemplo a seguir.

/dev/hda1 – isso quer dizer um disco na ide primária master na partição 01. Se existirem outras partições na mesma ide, o número continuará HDA2, HDA3, HDA4, até fechar quinze.

Para os discos SCSI e SATA, o funcionamento é o mesmo.

/dev/sda1 – quer dizer um disco no primeiro canal na partição 01, se existirem outras partições será SDA2, SDA3, até fechar quinze.

10.3.1 TIPOS DE PARTIÇÕES

As partições ou subdivisões de um disco funcionam como um contêiner para o sistema de arquivo, e indicam onde começa e termina o sistema de arquivo. As do Linux, por exemplo, podem ser do tipo primária e estendida.

PRIMARIA

Um disco rígido pode conter até quatro partições primárias, sendo que uma partição obrigatoriamente deverá existir e estar ativa. As partições estarão dispostas da seguinte forma:

Visualizando as partições IDE

/dev/hda1, HDA2, HDA3 até fechar quinze no máximo, sendo que uma desta deverá estar ativa e com sistema operacional.

Visualizando as partições SCSI/SATA

/dev/sda1, SDA2, até fechar quinze no máximo, sendo que uma desta deverá estar ativa e com sistema operacional.

ESTENDIDAS

As partições estendidas são partições primárias divididas em outras partições, chamadas de unidades lógicas. Nessas partições não podem conter sistemas de arquivo, e só pode existir uma partição estendida, que irá ocupar o lugar de uma partição primária. Da mesma forma que as partições primárias funcionam como contêiner para as partições estendidas, as partições estendidas funcionam como contêiner para as partições lógicas.

Por só poder existir quatro partições (ou três primárias e uma única estendida que ocupará o lugar de uma primária) em um disco padrão, tem-se o seguinte exemplo:

/dev/hda1 – primária
/dev/hda2 – primária
/dev/hda3 – primária
/dev/hda4 – estendida

Dividindo a partição estendida em partições lógicas, em que cada partição receberá um número inteiro que iniciará em 5 e irá até 15, tem-se o exemplo a seguir:

/dev/hda1 – primária
/dev/hda2 – primária
/dev/hda3 – primária
/dev/hda4 – estendida
/dev/hda5 – lógica
/dev/hda6 – lógica
/dev/hda7 – lógica
Até
/dev/hda15 – lógica

Resumindo: dentro de um disco é possível ter três partições primárias, uma estendida e doze partições lógicas, sendo um total de 15 partições possíveis em um disco.

SWAP

Outro tipo de partição é o *swap*, também conhecido como área de troca. Esta partição é utilizada como memória virtual para o Linux, que é somada à memória física auxiliando a troca entre a memória física e o disco.

O tamanho da partição *swap* deverá ser o dobro da quantidade de memória física existente no equipamento. Um exemplo é um servidor que possui 512MB de memória física, neste caso, a configuração da partição *swap* será de 1024MB (portanto, o dobro da memória física).

10.3.2 CRIANDO PARTIÇÕES

Como já visto, as partições são criadas preferencialmente na instalação do sistema operacional, mas é possível realizar, também, após o término do procedimento. Existem diversos programas que permitem dividir o disco em partições.

FDISK

O FDISK é um programa utilizado para executar as seguintes operações: criar, listar, apagar e alterar partição. Para a execução deste programa utilizam-se alguns parâmetros, conforme apresentados a seguir.

Uso:

```
# fdisk <dispositivo>
```

Opções do FDISK:

As opções do FDISK mais utilizadas são as mencionadas no quadro seguinte.

OPÇÃO	DESCRIÇÃO
a	Ativa partição
d	Apaga partição
l	Lista as partições ativas no disco
n	Nova partição
p	Tabela de partição em memória
q	Sai do fdisk e não salva as alterações realizadas
r	Altera o tipo da partição
w	Salva as alterações realizadas no disco

Quadro 5 - Opções do fdisk

Para realizar alteração do tipo da partição com a opção "r", é necessário saber qual o número de representação de cada sistema de arquivo e partição. Para visualizar a lista dos tipos, utiliza-se a opção "l".

Para criação de uma nova partição, é necessário acompanhar os passos a seguir, em que será utilizado um disco SATA canal 1:

Passo 1

Após executar o FDISK, será mostrado o prompt do FDISK. Então, pressione "m" e tecle ENTER.

Passo 2

Em seguida, você deve escolher entre estendida "l" e primária "p". Ao escolher a estendida, o sistema irá numerar automaticamente cada partição. Ao escolher a primária, selecione entre 1-4 e depois informe o cilindro inicial e o cilindro final, ou informe em megabytes ou em gigabytes. Ao escolher em megabytes, informe +1024M, mas se escolher gigabytes informe +1G.

Você deverá ter o cuidado de informar as letras "M" e "G" em maiúsculo. Veja um exemplo:

```
# fdisk /dev/sda
command (m for help) n
command action
l logical (5 or over)
p primary partition (1-4)
p
partition number (1-4) 2
first cylinder (407-1045, default 407):407
last cylinder or +size or +sizeM or +sizeK (407-1045, de-
fault 1045):+100M
```

Passo 3

Para visualizar a partição criada, selecione-se a opção "p".

Para apagar e ativar a partição, escolha a letra de acordo e informe o número da partição.

Dessa forma, estará criada uma partição primária. Mas, se desejar criar uma partição estendida, escolha a opção "l". Os passos seguintes serão os mesmos da criação da partição primária.



**SAIBA
MAIS**

Quer saber um pouco mais sobre a história dos sistemas de arquivos e partições, e as vantagens e desvantagens de particionar os discos? Então acesse o seguinte endereço: <<http://www.vivaolinux.com.br/artigo/Esquemas-de-particionamento-e-sistemas-de-arquivos>>.

10.3.3 FORMATAÇÃO

Você sabe o significado de formatação? Formatar significa preparar o disco para que o sistema operacional tenha condições de ler e gravar as informações no disco. As formatações estão divididas em dois tipos: primeiro, a formatação física, que é realizada na criação do disco rígido, ou seja, na fábrica. Esta formatação cria setores, cilindros, trilhas e ainda separa as trilhas defeituosas (*bad block*). A formatação lógica é necessária para o reconhecimento do sistema operacional, não altera a estrutura criada pela formatação física e poderá ser realizada diversas vezes.

Veja, a seguir, alguns comandos para formação dos discos.

MKFS – *MAKE FILE SYSTEM*

Este comando é utilizado para formatar as partições criadas por meio do FDISK, e irá formatar com os sistemas nativos EXT2, EXT3 e MSDOS.

Uso:

```
# mkfs [-t tipo] [opções] <dispositivo>
```

TIPO
EXT2
EXT3
MSDOS

Quadro 6 - Tipos de fdisk

OPÇÕES	DESCRIÇÃO
-c	Ver <i>bad block</i>
-L	Configura nome para o dispositivo Linux
-n	Configura nome para o dispositivo MSDOS
-q	mkfs trabalha com pouca saída no vídeo
-u	mkfs trabalha com máxima saída no vídeo

Quadro 7 - Opções do mkfs

Acompanhe um exemplo:

Formatando uma partição com sistema de arquivo EXT2 e com o nome DA-DOS.

```
# mkfs -t ext2 -L dados /dev/sda3
```

MKSWAP – MAKE SWAP

Este comando é utilizado para formatar a partição como área de troca (*swap*). É importante enfatizar que para formatar uma partição como área de troca, esta deve ser criada no FDISK com o tipo 82, como já foi mostrado.

Uso:

```
# mkswap /dev/sda3
```

Ao final, deve-se ativar a partição *swap* com o comando:

```
# swapon
```

10.3.4 ENDEREÇAMENTO DOS ARQUIVOS

Guardar as informações no disco deve ser de forma organizada e facilitada de acesso. É por estas características que os sistemas operacionais são robustos e uma maneira de organizar as informações dentro dos discos é distribuir os arquivos em diretórios e subdiretórios. Esta distribuição vale para todos os sistemas operacionais Windows, Linux, etc.

INODES

É uma pequena unidade de informação do disco, que possui informações detalhadas sobre os arquivos, informando o dono, o grupo, o tamanho, a permissão de acesso, a data da criação, etc. Os INODES também informam a localização correta do arquivo no disco e cada arquivo deve possuir um inode. Eles recebem números finitos partindo de 01, no momento da formatação.

HIERARQUIA DOS DIRETÓRIOS

Os diretórios são distribuídos no Linux em forma de árvore, só que ao contrário, pois no topo é que está a base de tudo, chamada de raiz ou *root* e representada por “/”.

Acompanhe, a seguir, detalhes dos diretórios mais importantes.

/ - raiz ou *root*, base do sistema de arquivos;

/bin - possui todos os arquivos executáveis, inclusive o kernel do Linux;

/dev - possui os dispositivos do sistema;

/etc - possui os arquivos de configuração;

/home - diretório dos usuários;

/lib - biblioteca do Linux;

/media - diretório de montagem para mídias removíveis;

/mnt – diretório de montagem para sistemas de arquivos temporários;

/proc – informações do sistema operacional;

/opt – possui aplicativos extras;

/root – é o *home* do super usuário;

/sbin – arquivos do sistema utilizados apenas pelo usuário *root*;

/srv – possui aplicativos extras;

/tmp – diretório temporário, suas informações são removidas automaticamente a cada *reboot*;

/usr – possuem arquivos dos usuários, este diretório é a 2^a maior hierarquia de diretórios no Linux;

/var – informações do sistema (*log, e-mail, print*, etc.).

Toda esta hierarquia foi criada em 1994 e definida como **FHS – File System Hierarchy Standard**.

10.3.5 GERENCIANDO O SISTEMA DE ARQUIVO

Para realizar tarefas importantes como montar e desmontar, verificar a capacidade e a integridade dos dispositivos, diversos programas são utilizados. Nesta sessão, vamos apresentar alguns.

DF

O comando DF verifica o espaço total e a utilização de um sistema de arquivo.

```
# df [opções] <dispositivo>
```

OPÇÕES	Descrição
-i	Valores em inodes
-k	Valores em kilobytes
-h	Valores em M (megabytes) G (gigabytes)

Quadro 8 - Opções do DF

DU

O comando **Disk Usage** detalha a utilização do disco por diretórios.

```
# du [opções] <arquivo>
```

OPÇÕES	Descrição
-a	Mostra arquivos e diretórios
-h	Mostra em M (megabytes) G (gigabytes)
-s	Mostra espaço total ocupado

Quadro 9 - Opções do DU

FSCK

O comando FSCK é utilizado para verificar e corrigir erros no sistema de arquivo.

```
# fsck [opções] <dispositivo>
```

OPÇÕES	Descrição
-A	Verifica os sistemas contidos no /dev/fstab
-c	Verifica os setores defeituosos
-t tipo_sist	Verifica por tipo de sistema
-p	Repara o sistema automaticamente
-y	Executa sem realizar perguntas

Quadro 10 - Opções do fsck

⁴ DUMP

É uma ferramenta utilizada para realização de backup de disco inteiro.

A opção “-y” deve ser executada acompanhada de outra opção, exemplo:

```
# fsck -y -p /dev/sda2
```

Existem outras opções do comando fsck. Para conhecê-las, execute o comando:

```
# man fsck
```

O arquivo /etc/fstab mantém informações de quais sistemas de arquivos serão montados no processo de carga do sistema. (RIBEIRO, 2009, p. 242).

10.3.6 MONTANDO DISPOSITIVOS

O sistema de arquivos do Linux permite que um ou mais dispositivo extra seja utilizado, partindo do diretório raiz. Desta forma, é possível utilizar HDs, unidades de CD-ROM, *pendrives* e outros dispositivos externos ao equipamento. Todos esses dispositivos serão identificados como um diretório e estarão montados dentro do diretório “/mnt”. Estes diretórios, que são montados com dispositivos, são chamados de ponto de montagem.

Os dispositivos podem ser montados de duas formas: a primeira, é através do arquivo /etc/fstab junto com a carga do sistema operacional e a segunda, através do comando mount e umount, após a carga do sistema operacional. Vamos a cada uma das opções.



FIQUE ALERTA

Nunca retire unidades removíveis pen-drive ou disquetes montadas em seu disco, sem antes desmontá-los, pois os dados podem ser perdidos.

/ETC/FSTAB

Este arquivo é responsável por montar dispositivos na inicialização do sistema operacional e desmontar no momento de desligamento do sistema operacional.

Na inicialização do sistema operacional os campos do “fstab” são analisados e o sistema monta os dispositivos contidos no arquivo.

Tabela 3 - Exemplo arquivo /etc/fstab

<FILE SYSTEM>	<MOUNT POINT>	<TYPE>	<OPTIONS>	<DUMP>	<PASS>
proc	/proc	proc	defaults	0	0
/dev/sda1	/	ext3	defaults	0	1
/dev/sda5	swap	swap	swap	0	0

Analise, a seguir, cada campo do arquivo "fstab".

- a) **File System:** Indica o dispositivo a ser montado.
- b) **Mount Point:** Indica qual o local que o dispositivo será montado (diretório).
- c) **Type:** Indica qual será o sistema de arquivo que o dispositivo será montado.
- d) **Options:** Indicam quais permissões o dispositivo montado terá. Vamos analisar cada opção deste campo.

OPÇÕES	
auto	Dispositivo será montado na inicialização do sistema.
noauto	Não monta o dispositivo na inicialização do sistema.
ro	O dispositivo será montado só para leitura.
rw	O dispositivo será montado como leitura e gravação.
exec	O dispositivo executa arquivos binários.
noexec	O dispositivo não executa arquivos binários.
User	Permite a qualquer usuário montar o dispositivo, mas só o usuário que montou o dispositivo pode desmontar.
users	Permite a qualquer usuário montar e desmontar o dispositivo.
nouser	Somente o usuário root (super-usuário) pode montar e desmontar.
Sync	Transferência síncrona.
Async	Transferência assíncrona.
Dev	Dispositivo de caractere (conexão serial).
Suid	Habilita o bit suid e sgid para os executáveis do dispositivo.
nosuid	Desabilita o bit suid e sgid para os executáveis do dispositivo.
defaults	Configuração padrão: rw, suid, exec, auto, nouser e async.

Quadro 11 - Opções do fstab

- a) **Dump⁴:** Indica se o dispositivo montado terá *backup* ou não.

DUMP	
0	Ext2
1	Demais sistemas

Quadro 12 - Opções dump

- b) ***Pass***: Indica se o dispositivo montado será checado no momento de inicialização do sistema operacional.

PASS	
0	Não analisa
1	Analisa antes do sistema raiz
2	Analisa depois do sistema raiz

Quadro 13 - Opções *pass*

De acordo com Ribeiro (2009), o Linux suporta diversos sistemas arquivos locais e remotos.

MOUNT

O comando *mount* é utilizado para montar dispositivos após a carga do sistema operacional.

Uso do *mount*:

```
# mount <opções> dispositivo <diretório ou ponto de montagem>
```

O comando *mount* também pode ser executado de outras formas:

```
# mount <opções> dispositivos
```

Ou

```
#mount <opções> diretório
```

Nestes dois casos, antes do dispositivo ser montado, o arquivo “/etc/fstab” é lido pelo sistema para verificar as configurações do dispositivo a ser montado.

OPÇÕES DO MOUNT

-a	Monta todos os dispositivos que estão contidos no arquivo “fstab”.
-r	Monta os dispositivos para que sejam apenas lidos.
-w	Monta os dispositivos para que sejam lidos e gravados.
-t <tipo de sistema de arquivo>	Msdos, vfat, ntfs, ext2, ext3, reiserfs, iso9660, nfs, smbfs.

Quadro 14 - Opções do *mount*

Confira um exemplo:

```
# mount -t ext2 /dev/fd0 /mnt/floppy
```

Neste exemplo mostrado, é montada a unidade de disquete, com sistema de arquivo ext2. O disquete está no dispositivo “**/dev/fd0**” e será montado em “**/mnt/floppy**”.

Agora acompanhe a situação a seguir, em que é utilizado um pendrive.



CASOS E RELATOS

Desmontar pen-drive

Em sistema Linux, ou em outro sistema operacional qualquer, desmontar o pen-drive ou qualquer outro dispositivo removível é muito importante. Este fato aconteceu com um aluno que estava terminando o seu curso de graduação, ao realizar seu TCC (Trabalho de Conclusão de Curso).

No dia da entrega de seu trabalho, o aluno fez algumas alterações no trabalho, porém, estava com muita pressa, retirou o pen-drive da unidade sem desmontar e foi até uma copiadora para realizar a impressão do mesmo. Ao abrir o arquivo para impressão, deu a última analisada no arquivo e verificou que todas as alterações realizadas anteriormente não foram gravadas.

UMOUNT

Este comando faz o contrário do “mount”, ou seja, desmonta o dispositivo montado pelo *mount*.

Uso **umount**:

```
# umount <opções> dispositivo  
Ou  
# umount <opções> diretório
```

OPÇÕES	
-a	Desmonta todos dispositivos contidos no /etc/mtab
-t	Desmonta dispositivos de um determinado sistema de arquivo.

Quadro 15 - Opções do *umount*

Veja um exemplo:

```
# umount /media/cdrom
```

No exemplo mostrado, o CD-ROM que foi montado no diretório /media/cdrom está sendo desmontado.



RECAPITULANDO

Neste capítulo, você viu um pouco do funcionamento dos sistemas de arquivos e seus tipos. Conheceu também os dispositivos e como são montados e desmontados, bem como os tipos de discos para armazenamento do sistema operacional. Aprendeu ainda, a gerenciar um sistema de arquivo, a formatar os discos e até a hierarquia dos diretórios nos sistemas Linux.

Anotações:

Administrando Sistemas

11



O assunto que será abordado neste capítulo irá explicar como se administra um sistema operacional para rede. Também será apresentado à você como criar contas de usuários, grupos de usuários e administrar estes objetos após serem criados.

E para encerrar o conteúdo deste capítulo, você saberá como se determinam os espaços no disco para usuários e grupos, para que usuários não lotem os discos com informações desnecessárias.

Após conhecer os conteúdos citados, você terá capacidade para:

- a) criar e administrar contas de usuários;
- b) criar e administrar grupos de usuários;
- c) compreender as permissões no sistema Linux;
- d) compreender a importância das quotas de disco.

E para dar início ao primeiro aprendizado desta parte do livro, você sabia que quotas de disco no Linux são limitações de espaço em disco disponível para os usuários em determinada partição? Mais detalhes sobre essa e outras informações você estudará nas próximas páginas.

11.1 ADMINISTRAÇÃO SISTEMA OPERACIONAL PARA REDE

A administração de rede dos sistemas operacionais é uma tarefa relativamente fácil, mas que requer um pouco de atenção. Uma boa parte do tempo do administrador do sistema estará relacionada aos usuários e suas contas e tarefas rotineiras de *backup*.

11.1.1 CONTAS DE USUÁRIOS

Administrar as contas de usuários é criar, remover, bloquear, etc., as contas dos usuários. No Linux são armazenadas em um arquivo chamado *passwd* que está localizado no “/etc/passwd”. Este arquivo possui a conta do usuário, nome, grupo, diretório *home*, etc. A seguir, conheça um pouco mais sobre o *passwd*.

PASSWD

Como já visto, este arquivo possui a conta de todos os usuários cadastrados no sistema e sua primeira conta é de um usuário muito especial: o *root*. Analise o arquivo seguinte.

```
# nano /etc/passwd
```

```
root:x:0:0:root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
Debian-exim:x:101:103::/var/spool/exim4:/bin/false
```

Redes in Vídeo (20-?)

Figura 54 - Arquivo *passwd*

Analizando a primeira linha da figura, tem-se:

```
root:x:0:0:root:/Bin/bash
```

Cada informação do arquivo *passwd* é separada por “:”.

No quadro a seguir, você poderá entender o significado de cada elemento do arquivo.

LOGIN	NOME DA CONTA DO USUÁRIO PARA ENTRAR NO SISTEMA.
X	Este “x” representa a senha do usuário. Como este arquivo é muito utilizado para verificação de nome de usuário, pasta <i>home</i> e outras informações (mesmo a senha estando criptografada), tornou-se vulnerável então por motivos de segurança e as senhas dos usuários não estão mais neste arquivo, e sim no arquivo “/etc/shadow”.
Id do usuário	Este campo representa o id do usuário. O id “zero” representa que o usuário é um administrador do sistema (<i>root</i>), do número “1 até 99” são de uso administrativo utilizados para algumas contas que precisam poderes para executarem algumas tarefas administrativas. Os usuários comuns são cadastrados com número automaticamente de id, a partir de “1000”.
Id do grupo	Este campo indica a qual o grupo o usuário pertence.
Nome do usuário	Representa o nome do usuário, e também aceita espaço.
Diretório home	Faz referência a um número único para código do grupo.
Shell	Indica qual <i>Shell</i> o usuário utilizará para a execução de suas aplicações. Por padrão é utilizado o “/Bin/bash”, mas podemos utilizar outros <i>Shell</i> . Se colocarmos a expressão <i>false</i> , exemplo “/Bin/false”, o usuário não terá permissão para acessar o sistema.

Quadro 16 - Detalhamento do arquivo *passwd*Figura 55 - Detalhes do arquivo *passwd*

SENHAS

As senhas utilizadas no Linux são criptografadas de forma que invasores não consigam decifrar por meio de ataques, porém, com ataque de força bruta as senhas podem ser decifradas. Por tal motivo, são trocadas do arquivo */etc/passwd* para */etc/shadow*, garantindo que um ataque de força não decifre a senha, pois o invasor terá primeiro que acessar o arquivo *shadow*, que só o *root* tem acesso, para depois tentar decifrar a senha.

Note que no exemplo foi criado um usuário “senai” com senha “123”, e depois foi criado o usuário “pedro” com a mesma senha “123”. Apesar das senhas serem iguais a criptografia será diferente, como você pode conferir na figura seguinte.

```
senai:$6$HdF3RBf0$R8pg/25AbxStXWE26H6MnJ,10v.ds0X37T8RLmxRv144331108e2Y3nJHCRAK63
pedro:$6$R3M1UuJ2$Kfc52jVHI2EmKwxCU1eINr,V/24GPfxBk/Onu1LUUs25wA61s60cASFedGUZVt
```

Dmitri Camargo (2012)

Figura 56 - Senhas criptografadas

passwd

Essa informação é utilizada para alterar ou criar senhas de usuários.

Uso:

```
# passwd <usuário>
```

Dessa forma, o sistema irá solicitar uma nova senha para o usuário.

Nota: o *root* pode alterar a senha de todo e qualquer usuário, mas o usuário altera apenas a sua própria senha.

```
root@Asterisk:/# passwd pedro
Digite a nova senha UNIX: [REDACTED]
```

Dmitri Camargo (2012)

Figura 57 - Alterando senha



FIQUE ALERTA

Ao criar senhas para sua conta, utilize senhas fortes com caracteres numéricos e alfa, nunca utilize seu nome ou 123456, pois esta é a senha mais utilizada no mundo.

11.1.2 CRIANDO CONTAS DE USUÁRIOS

Criar contas de usuários nos sistemas Linux é muito simples, bastando conhecer os comandos necessários. Há duas formas de criar as contas de usuários. A primeira é por meio do *useradd*. Para acessar esta opção você terá que passar alguns parâmetros para a criação do usuário. A segunda maneira é mais fácil, utilizando o comando *adduser*. Desta forma, o sistema solicita os dados do usuário.

Conheça um pouco mais sobre o comando *adduser* a seguir.

ADDUSER

É um comando utilizado para criar usuários no Linux.

Uso:

```
# adduser <nome do usuário>
```

Conheça o passo a passo de como criar usuários no Linux.

Passo 1

Ao digitar o comando, o sistema solicita a senha para o usuário.

```
root@Asterisk:/# adduser curso
Adicionando usuário 'curso' ...
Adicionando novo grupo 'curso' (1005) ...
Adicionando novo usuário 'curso' (1005) com grupo 'curso' ...
Criando diretório pessoal '/home/curso' ...
Copiando arquivos de '/etc/skel' ...
Digite a nova senha UNIX: [REDACTED]
```

D'Imitrie Camargo (2012)

Figura 58 - Criação usuário senha

Passo 2

Após inserir a senha para o usuário, basta pressionar ENTER, para que o sistema solicite que a senha seja redigitada.

```
root@Asterisk:/# adduser curso
Adicionando usuário 'curso' ...
Adicionando novo grupo 'curso' (1005) ...
Adicionando novo usuário 'curso' (1005) com grupo 'curso' ...
Criando diretório pessoal '/home/curso' ...
Copiando arquivos de '/etc/skel' ...
Digite a nova senha UNIX:
Redigite a nova senha UNIX: [REDACTED]
```

D'Imitrie Camargo (2012)

Figura 59 - Criação usuário redigitando a senha

Passo 3

Após redigitar a senha do usuário, pressione novamente ENTER, e o sistema irá solicitar o nome completo do usuário.

```
Modificando as informações de usuário para curso
Informe o novo valor ou pressione ENTER para aceitar o padrão
Nome Completo []: 
```

Figura 60 - Criação usuário, nome completo do usuário

Dmitri Camargo (2012)

Passo 4

Uma vez inserido o nome completo do usuário, pressione ENTER e o sistema irá solicitar o número da sala. Esta informação pode ser deixada em branco, bastando apenas pressionar ENTER ou informar um número, fazendo referência a uma sala. Exemplo: 01 CPD, 02 tesouraria e assim por diante.

```
Informe o novo valor ou pressione ENTER para aceitar o padrão
Nome Completo []: curso de redes
Número da Sala []: 10 
```

Figura 61 - Criação usuário, número da sala

Dmitri Camargo (2012)

Passo 5

Após inserir o número da sala, pressione ENTER, e o sistema irá solicitar o fone de trabalho.

```
Modificando as informações de usuário para curso
Informe o novo valor ou pressione ENTER para aceitar o padrão
Nome Completo []: curso de redes
Número da Sala []: 10
Fone de Trabalho []: 48 3239-6800 
```

Figura 62 - Criação de usuário, número de telefone

Dmitri Camargo (2012)

Passo 6

Para inserir o número de telefone do usuário, pressione ENTER, e o sistema irá solicitar o telefone doméstico ou residencial.

```
Modificando as informações de usuário para curso
Informe o novo valor ou pressione ENTER para aceitar o padrão
Nome Completo []: curso de redes
Número da Sala []: 10
Fone de Trabalho []: 48 3239-6800
Fone Doméstico []: 48 3239-6840 
```

Figura 63 - Criação usuário, telefone residencial

Dmitri Camargo (2012)

Passo 7

Após inserir o número do telefone residencial do usuário, pressione ENTER, e o sistema irá solicitar outras informações que fazem referência ao usuário. Fica a critério de cada administrador informar este campo, se não informar nada, pressione ENTER.

```
Modificando as informações de usuário para curso
Informe o novo valor ou pressione ENTER para aceitar o padrão
Nome Completo []: curso de redes
Número da Sala []: 10
Fone de Trabalho []: 48 3239-6800
Fone Doméstico []: 48 3239-6840
Outro []: [
```

D'Imitre Camargo (2012)

Figura 64 - Criação usuário, outras informações

Após inserir outras informações (ou não), pressione ENTER, e o sistema irá finalizar o cadastro do usuário no sistema.

Passo 8

```
Modificando as informações de usuário para curso
Informe o novo valor ou pressione ENTER para aceitar o padrão
Nome Completo []: curso de redes
Número da Sala []: 10
Fone de Trabalho []: 48 3239-6800
Fone Doméstico []: 48 3239-6840
Outro []:
A informação está correta? [S/n] [
```

D'Imitre Camargo (2012)

Figura 65 - Criação usuário, finalização

Passo 9

Pressione "S" e o usuário estará cadastrado.



CASOS E RELATOS

Senha fraca

Certa vez, um funcionário da Empresa infoX, recentemente demitido da instituição, resolveu, de alguma forma, causar um prejuízo para a empresa. Foi então que ele teve a ideia de tentar descobrir a senha de algum administrador do sistema. Realizou diversas tentativas dentre os funcionários que possuíam senhas com perfil administrativo e, sem sucesso, foi então que teve a idéia de tentar descobrir a senha de seu amigo que

também possuía perfil administrativo, já que eram amigos íntimos e ele conhecia a sua família, esposa e filhos. Com estas informações ficou mais fácil a descoberta da senha. A senha que seu amigo utilizava era o nome da esposa e filho juntos.

Por sorte não foi realizado nenhum estrago, pois o laço de amizade falou mais alto.

USERMOD

Este é um comando utilizado para realizar alterações nas contas de usuários.

Uso:

```
# usermod <opções> conta do usuário
```

Opções:

- d Altera o diretório home do usuário;
- c Altera o nome do usuário;
- g Altera o número do grupo do usuário;
- s Altera o *Shell* do Linux;
- L Usado para bloquear a conta do usuário;
- U Desbloqueia a conta do usuário.

```
# usermod -c "pedro de Souza" pedro
```

No exemplo que você acabou de ver, foi alterado o nome do usuário da conta “pedro”.

```
#usermod -L pedro
```

Já nesse outro exemplo, foi bloqueado o usuário Pedro. Após este comando, se for verificado o arquivo “/etc/shadow”, é possível notar que foi posto este sinal “!” na frente da senha do usuário.

USERDEL

Comando utilizado para remoção de uma conta de usuário.

Uso:

```
# userdel <opções> conta do usuário
```

Opções:

- r Apaga o diretório *home* do usuário

```
# userdel pedro
```

No exemplo, o comando *userdel* irá apagar apenas o usuário “pedro”.

```
# userdel -r pedro
```

Neste exemplo, o usuário “pedro” será removido, bem como o seu diretório *home* (/home/pedro).



VOCÊ SABIA?

Ao executar o comando *userdel -r* você estará removendo todos os arquivos contidos no diretório *home* do usuário apagado. Se contiver informações importantes, você não conseguirá recuperá-las.

SU (*SWITCH USER*)

Para que um usuário possa realizar tarefas administrativas, é necessário que este tenha permissões (e também para que não seja necessário fazer Login com um usuário administrador).

Uso:

```
# su
```

Figura 66 - Comando su

Dmitri Camargo (2012)

Após digitar o comando *su*, o sistema solicita a senha do usuário *root*.

ID

O comando id é utilizado para verificar informações do usuário.

Uso:

id usuário

Opções:

-g exibe o id do grupo principal do usuário

-G exibe o id de todos os grupos do usuário

-u exibe o id do usuário

-Gn exibe os nomes dos grupos do usuário

id -Gn ctaí

No exemplo que você acabou de ver, foram apresentados os nomes dos grupos do usuário ctaí.

OUTROS COMANDOS PARA USUARIOS

A seguir, você conhecerá uma lista de outros comandos utilizados para gerência de usuários.

Groups: exibe grupos de um determinado usuário.

Uso: # groups <usuário>

Users: exibe usuários ativos no sistema.

Uso: # users

É importante você saber que para criar um usuário com poderes de super usuário, é necessário seguir os seguintes passos:

adduser teste

passwd teste

Após usuário e senha criados, você deve editar o arquivo *passwd*, alterando o id do usuário e o id do grupo.

Antes

teste:x:1006:100::/home/teste:/bin/bash

Depois

teste:x:0:0::/home/teste:/bin/bash

Realizadas as alterações no arquivo "/etc/passwd", o usuário-teste possui poderes de super usuário.



**SAIBA
MAIS**

Quer saber mais sobre administração de sistemas Linux? Através do livro de Rubens E. Ferreira Linux, Guia do Administrador do Sistema, você conhece as mais variadas formas de se administrar um sistema, algumas dicas de criação de usuários e grupos e muito mais. Vale a pena!

11.2 GERENCIANDO GRUPOS

Os grupos dos usuários são de grande importância para a administração do sistema, facilitando as configurações de permissões de acesso aos diretórios e arquivos. Uma vez permitido a um grupo acessar um determinado diretório, você estará dando permissão para um conjunto de usuários cadastrado neste grupo. O arquivo responsável por guardar os grupos é o *group*, localizado em "/etc/group". Cada informação do arquivo *group* é separada por ":".

Veja um exemplo do arquivo "/etc/group" na figura seguinte.

```
sambashare:x:108:  
senai:x:1001:ctai,pedro
```

D'Imitrie Camargo (2012)

Figura 67 - Arquivo group

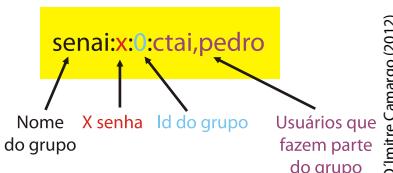


Figura 68 - Detalhes do arquivo group

De acordo com o quadro seguinte, entenda melhor o que a figura que você acabou de ver representou.

NOME DO GRUPO	Faz referência ao nome dado ao grupo de usuários.
X	Faz referência à senha que por ventura o grupo venha possuir, as senhas dos grupos não estão mais neste arquivo pelos mesmos motivos das senhas de usuários do arquivo “passwd”. As senhas dos grupos estão no arquivo “gshadow”, localizados em “/etc/gshadow”.
ID DO GRUPO	Faz referência a um número único para código do grupo. Este número é o mesmo contido no arquivo <i>passwd</i> .
USUÁRIOS DO GRUPO	Faz referência a todos os usuários cadastrados no grupo.

Quadro 17 - Detalhamento do arquivo *group*



SAIBA MAIS

Existem distribuições Linux que, ao ser criado o usuário, automaticamente é criado um grupo de mesmo nome.

Conheça, a seguir, alguns comandos bastante utilizados no dia a dia dos usuários Linux. Os comandos aqui detalhados irão ajudar na criação de grupos, alteração de contas de usuários, dentre outras funções cotidianas.

GROUPADD

Este comando é utilizado para criar grupos de usuários.

Uso:

```
# groupadd <grupo>
# groupadd senai
```

No exemplo apresentado foi criado o grupo senai.

GROUPDEL

É o comando utilizado para remover um grupo cadastrado no sistema.

Uso:

```
# groupdel <nome do grupo>  
# groupdel senai
```

No exemplo apresentado foi apagado do sistema o grupo senai.

CHAGE

Comando utilizado para alterar a validade das contas dos usuários no Linux que possuem validade por tempo indefinido.

Uso:

```
# chage <opções> conta do usuário
```

Opções:

- E Altera o tempo de validade da conta, deve estar neste formato (MM/DD/YYYY)
- I Verifica configurações de contas de usuários.

```
# chage -E 01/11/2012 ctai
```

Neste exemplo, foi alterada a validade da conta do usuário ctai para o dia 01 de Janeiro de 2012.

GPASSWD

O gpasswd é um comando utilizado para a realização de tarefas relacionadas aos grupos, como adicionar usuário, inserir senhas para o grupo e outras funcionalidades.

Uso:

```
# gpasswd <opções> <usuário> grupo
```

Opções:

- a inclui usuário ao grupo
- d remove usuário do grupo
- r remove senha do grupo
- A define um administrador para o grupo
- M define usuários que serão administradores do grupo
- R desativa o acesso ao grupo através do comando newgrp

Para inclusão de senha para o grupo, utiliza-se o comando:

```
# gpasswd <grupo>
# gpasswd -a ctaí senai
```

Neste exemplo, foi incluído o usuário ctaí no grupo senai.

GROUPMOD

Utilizado para realizar modificações nas características dos grupos existentes no sistema.

Uso:

```
# groupmod <opções> grupo
```

Opções:

- g Realiza a troca do id do grupo para um número inexistente
- n Realiza a troca do nome do grupo

```
# groupmod -g 10010 senai
```

No exemplo apresentado, foi alterado o id do grupo para 10010.

É importante salientar que para verificar o "id" existente, basta visualizar o arquivo "/etc/group".

11.3 PERMISSÕES DO SISTEMA

As permissões possuem uma importância fundamental em sistemas multiusuário para que cada usuário acesse apenas os dispositivos ou arquivos que ele possa utilizar, como o CD-ROM, arquivos ou diretórios. As permissões de acesso em cada arquivo ou diretório no Linux estão divididas em três tipos, conforme você pode conferir na figura seguinte.

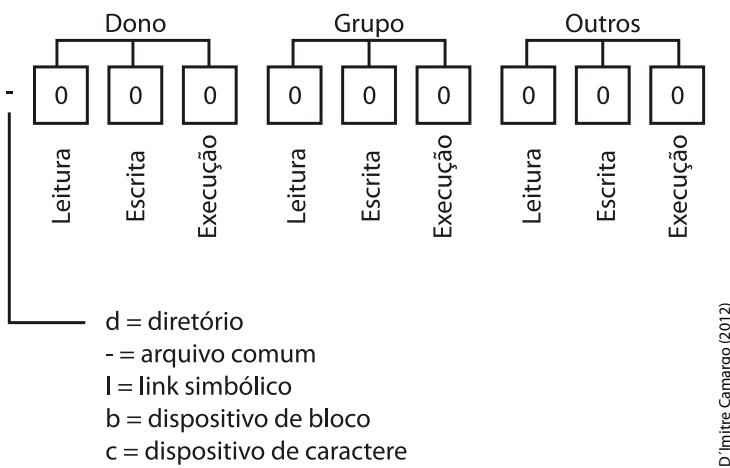


Figura 69 - Permissões

D'Imitre Camargo (2012)

Conforme figura que você acabou de conferir, entenda que:

Permissão de dono: Esta permissão normalmente é para o usuário criador do arquivo.

Permissão de grupo: Esta permissão normalmente é para o grupo ao qual o arquivo pertence.

Permissões de outros: Esta permissão é destinada aos usuários que não são donos do arquivo e nem fazem parte do grupo de donos.

Cada tipo de permissão possui três tipos de acesso, representados pelas letras r, w e x:

- a) leitura (r);
- b) escrita (w);
- c) execução (x).

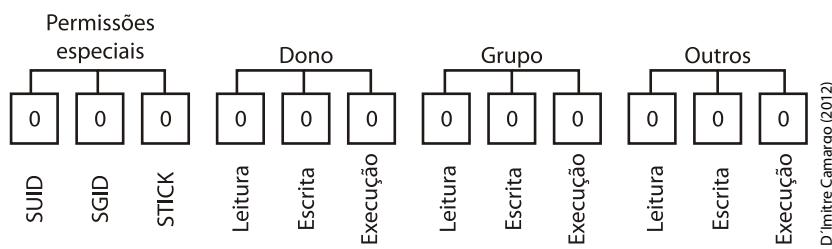
As permissões nos arquivos e diretórios (representadas pelos tipos de acessos apresentados) possuem variações. Confira no quadro a seguir que variações são essas.

	LEITURA	ESCRITA	EXECUÇÃO
ARQUIVO	Lê o arquivo	Altera arquivo	Executa arquivo como programa
DIRETÓRIO	Lista diretório	Cria/apaga arquivo no diretório	Lê/grava arquivos no diretório

Quadro 18 - Variações das permissões

Os arquivos e diretórios, além de possuírem as permissões básicas leitura, escrita e execução, também possuem as permissões chamadas de especiais, que podem ser adicionadas ou não. Estas permissões são gravadas em uma parte do disco e representadas por 12 caracteres binários, que iremos analisar.

A seguir, conheça um pouco mais sobre permissões especiais.



Permissões especiais: As permissões especiais são utilizadas em arquivos comuns, arquivos executáveis e diretórios. Este tipo de permissão é um complemento às permissões básicas (rwx).

Suid (set user id):

Este bit é utilizado apenas em arquivos executáveis. Permite que o arquivo seja executado com as permissões do dono do arquivo e as permissões de root, não importando quem esteja executando.

Sgid (set group id):

Este bit é utilizado em diretórios. É encarregado de fazer com que todos os arquivos que estão dentro de um diretório façam parte do mesmo grupo de diretório.

Stick:

Este bit também é conhecido como 'colado memória', ou seja, os arquivos que recebem este bit em sua permissão são postos próximos à memória, para uma rápida execução.

Os bits especiais são representados pelas letras s e t:

SUID = s;

SGID = s;

STICK = t.

Como os bits especiais são utilizados com pouca frequência, o "s" que representa o SUID e SGID é substituído pelo "x" do campo dono e grupo do arquivo ou diretório. O "t", que representa o STICK, é substituído pelo "x" no campo outro do arquivo ou diretório.

Como você viu, as permissões podem ser representados pelas letras r,w ex em binários, e também podem ser representadas de forma octal, o que facilita o entendimento do usuário.

A tabela a seguir apresenta as permissões. A representação binária se faz apenas pelos três primeiros binários 1,2,4, que dá um total de 7.

Zero ou Um	Zero ou Um	Zero ou Um
0 = 0	0 = 0	0 = 0
1 = 4	1 = 2	1 = 1

Figura 71 - Binários

D'Imitre Camargo (2012)

Tabela 4 - Tabela de permissões

OCTAL	BINÁRIO	LETROS	
0	000	--	Sem permissão
1	001	-x	Execução
2	010	-w-	Escrita
3	011	-wx	Escrita e execução
4	100	r-	Leitura
5	101	r-x	Leitura e execução
6	110	rw-	Leitura e escrita

Veja um exemplo:

-rwxr-x-- ctaí senai aula.sh

O exemplo que você viu, representa um arquivo comum que possui leitura, escrita e execução para o dono ctaí, leitura e execução para o grupo senai e os demais não possuem permissão no arquivo aula.sh.

As permissões também podem ser representadas pelos octetos 750.

rxw 4+2+1 = 7

r-x 4+0+1 = 5

--- 0+0+0 = 0

Veja a seguir um exemplo com bits especiais.

-rwsr-x--- **ctai** **senai** **aula.sh**

O exemplo representa um arquivo comum, que possui leitura, escrita e execução para o dono ctaí, leitura e execução para o grupo senai e os outros não possuem permissão no arquivo aula.sh. Possui também o bit especial SUID “s”, que faz que o arquivo aula seja executado como root.

As permissões também podem ser representadas pelos octetos 4750.

s 4+0+0 = 4

rxw 4+2+1 = 7

r-x 4+0+1 = 5

--- 0+0+0 = 0

11.3.1 CHMOD

Este comando é utilizado para alterar as permissões de arquivos e diretórios. As alterações das permissões dos arquivos e diretórios podem ser realizadas através das letras e dos números octal. Para representar as classes de dono, grupo e outros utilizamos as letras u (dono), g (grupo), o (outros) e a (todos) e “+ - =” para as operações e as letras r (leitura), w (escrita), x (execução), X másculo (executar tudo), s (SUID/SGID) e t (STICK).

CLASSE	OPERAÇÕES	PERMISSÕES
u = dono	+ = adiciona	r = leitura
g = grupo	- = diminui	w= escrita
o = outros	= com exatidão	x = execução
a = todos		X = para todos
		s = SUID/SGID

Quadro 19 - Chmod

Uso:

```
#chmod <opções> <permissões tabela> <arquivo>
```

Opções:

- c mostra informações dos arquivos em modificação;
- f não apresenta mensagens de erro;
- R atua recursivamente em todos os subdiretórios, se houverem;
- v mostra os detalhes das alterações dos arquivos.

Permissões com números octal.

```
# chmod 777 aula.txt
```

No exemplo que você conferiu, foram concedidas as permissões de leitura, escrita e execução para o dono. A leitura, escrita e execução para o grupo, e leitura, escrita e execução para os demais.

As permissões que você acabou de conferir também poderiam ser utilizadas em forma de letras, conforme exemplo a seguir.

```
# chmod a=X aula.txt  
# chmod 755 aula.txt  
Ou  
# chmod u=rwx,go=rx aula.txt
```

Neste exemplo, foram concedidas as permissões de leitura, escrita e execução para o dono, leitura, e execução para o grupo e outros.

É importante informar que ao executar o comando # chmod +x aula.txt, a permissão execução será concedida a todas as classes dono, grupo e todos, pois não foi informada qual seria a classe.

11.3.2 CHOWN

Este comando é utilizado para alterar as permissões do dono do arquivo ou diretório, além de também alterar o grupo.

Uso:

```
# chown <opções> <usuário novo>.<grupo novo>  
<arquivo>
```

-v apresenta detalhes das alterações realizadas;

-c apresenta detalhes dos arquivos em modificações;

-R atua recursivamente.

Veja um exemplo:

```
# chown ctaisenai aula.txt
```

No exemplo, o *chown* irá alterar o dono do arquivo para o usuário *ctaisenai*.

```
# chown ctaisenai aula.txt
```

No exemplo que você viu, o *chown* irá alterar o dono do arquivo e alterar o grupo para o grupo do usuário *ctaisenai*.

É importante você saber que ao colocar “.” após o dono, sem informar o grupo, o comando irá assumir o grupo do dono.

```
# chown ctaisenai aula.txt
```

No exemplo, o *chown* irá alterar o dono para o usuário *ctaisenai*, e o grupo *senai* para o arquivo *aula.txt*.

```
# chown ctaisenai aula.txt
```

Neste exemplo, o *chown* irá apenas alterar o grupo deixando intacto o dono do arquivo *aula.txt*.

11.3.3 CHGRP

Este comando é utilizado para alterar o grupo do arquivo ou diretório.

Uso:

```
# chgrp <opções> arquivo
```

Opções:

-v apresenta detalhes das alterações realizadas;

-c apresenta detalhes dos arquivos em modificações;

-R atua recursivamente.

Veja um exemplo:

```
# chgrp -R senai /etc
```

Neste exemplo, o comando chgrp irá alterar o grupo de todos os arquivos e diretórios para senai dentro do diretório /etc recursivamente.

CHATTR (CHANGE ATTRIBUTE)

Este comando tem a função de modificar os atributos dos arquivos e diretórios.

Uso:

```
# chattr <opções> <modo> <arquivo>
```

Opções:

- v apresenta detalhes das alterações realizadas;
- R atua recursivamente.

Modos:

- + adiciona;
- retira;
- = exato.

Acompanhe no quadro a seguir a função de cada atributo.

A	Não permite a atualização da hora de acesso do arquivo. Em diretórios, seus arquivos internos não terão a hora de acesso modificada.
A	Só permite adicionar informações no arquivo (Append-Only). Em diretórios, só permite a adição de arquivos e, em todos os casos, estes arquivos não podem ser excluídos.
C	Este atributo informa ao Kernel para comprimir em disco o conteúdo do arquivo. No momento da leitura o Kernel, descompacta e entrega os dados sem a compressão.
D	Sincroniza a gravação de dados em disco somente para diretórios.
D	Não permite o <i>backup</i> do arquivo pelo programa Dump.
E	Atributo experimental para compressão de dados. Não utilizar.
I	Em diretórios, indica que o mesmo estará sendo indexado por algoritmos do tipo "hashed trees". Não utilizar.
I	Torna o arquivo imutável. Nada pode ser feito com ele, somente pode ser lido.

J	Faz com os dados do arquivo sejam escritos no <i>Journaling</i> do ext3, antes que o próprio arquivo seja gravado em disco, se o <i>Filesystem</i> estiver montado com a opção “data=ordered” ou “data=writeback”. Não possui efeito se o <i>filesystem</i> for montado com a opção “data=journal”.
S	Faz com que, ao apagar o arquivo, seus blocos sejam zerados em disco, impossibilitando assim a sua recuperação (<i>undelete</i>).
S	Sincroniza a gravação do arquivo em disco, em sistemas Ext2. Não possui efeito sobre diretórios.
T	Altera a hierarquia do diretório na estrutura do <i>filesystem</i> . É válido somente para diretórios e para testes do Kernel 2.5.46 (instável), no sistema de alocação de blocos Orlov.
T	Não permite que os blocos finais do arquivo, que não estejam completos (fragmentos) sejam mesclados com outros arquivos, no caso de <i>filesystems</i> que suportam o tail-merging. Não suportado para <i>filesystems</i> Ext2 ou Ext3 (ainda).
U	Marca o arquivo como recuperável, ou seja, poderá ser recuperado (<i>undelete</i>).
X	Modo experimental para compressão. Não utilizar.
Z	Marca o arquivo como recuperável, ou seja, poderá ser recuperado (<i>undelete</i>).

Quadro 20 - Tabela de atributos

Veja um exemplo:

```
# chattr +AaEsS aula.txt
```

No exemplo visto, o comando chattr está adicionado os atributos “AaEsS” para arquivo aula.txt

```
# chattr +i -A aula.txt
```

Neste exemplo, o comando chattr está adicionado o atributo “i” e retirando o atributo “A” do arquivo aula.txt.

11.3.4 LSATTR

Este comando é utilizado para listar os atributos dos arquivos e diretórios. Pode ser utilizados com as opções de arquivo ou não.

Uso:

```
# lsattr <opções> <arquivo>
```

Opções:

-R lista recursivamente;

-a lista todos os arquivos comuns e ocultos;

-d lista diretórios como arquivos.

11.4 QUOTAS DE DISCO

Você sabe o que são cotas (ou quotas, que é a forma de como o comando é escrito) de disco? As cotas de disco são utilizadas para realizar um gerenciamento dos espaços dos discos, pois muitas são comprometidas principalmente em servidores de e-mail, servidores de arquivos, etc. Por meio de cotas, o administrador consegue determinar o espaço exato que cada usuário ou grupo irá utilizar no disco de um servidor.

Veja a seguir como implementar as cotas de disco.

11.4.1 IMPLEMENTANDO AS COTAS DE DISCO

Para habilitar a gerência de cota para um dispositivo, é necessário editar o arquivo “/etc/fstab”, adicionando os parâmetros “usrquota” para cotas de usuários e “grpquota” para cotas de grupos de usuários. Veja como:

```
#nano /etc/fstab  
/dev/sda3 /usr ext2 defaults,usrquota,grpquota 02
```

Os parâmetros usrquota e grpquota devem ser adicionados logo após o parâmetro defaults, separados por vírgula, de acordo com o exemplo que você acabou de ver.

Após realizar alteração no arquivo “fstab”, é necessário criar dois arquivos: o “quota.user” e o “quota.group”. Estes arquivos guardarão o banco de dados das cotas criadas e deverão ser criados na raiz do sistema que irá implementar a cota, como no exemplo que está sendo utilizado. O dispositivo é /dev/sda3 e está montado em /usr. Devemos criar os arquivos em: “/usr”.

É importante saber que estes arquivos deverão ter permissão de apenas leitura e escrita para o root.

Criando os arquivos:

```
# touch /home/quota.user  
# touch /home/quota.group  
Alterar permissões:  
# chmod 600 /home/quota.user  
# chmod 600 /home/quota.group
```

Após a criação dos bancos, deve-se dar um *start* no banco criado, por meio do comando “quotacheck –avug”. Este comando irá verificar dentro do arquivo “fstab” à procura do usrquota e grpquota e iniciar o banco de cotas.

```
#quotacheck –avug
```

Após a execução do comando anterior, você deverá verificar se o banco foi iniciado, por meio do seguinte comando:

```
# ls -lga /usr
```

Para ter certeza que os bancos foram iniciados, o tamanho dos arquivos quota.user e quota.group não poderá ser zero. Assim, habilita-se o serviço de cotas.

```
#quotaon –a
```

Uma vez criados e iniciados os bancos de cotas, e iniciado o serviço de cota, é o momento de colocar o serviço de cotas para ser iniciado no *boot* do sistema. Para isso, é necessário primeiro verificar se não existe o arquivo “quotas” dentro de “/etc/rc.d”. Se este não existir, deverá ser criado, pois será um arquivo de *script* de inicialização do serviço de cota.

Supondo que o arquivo não exista, deverá ser criado e adicionado às linhas a seguir.

```
# nano /etc/rc.d/quotas
#!/Bin/bash
/Bin/quotaon –avug
```

Saia do arquivo, salvando-o, e altere a permissão deste arquivo.

```
# chmod 755 /etc/rc.d/quotas
```

Após a criação dos scripts de inicialização, você deve associar estes scripts a um runlevel que vai ser executado na inicialização do sistema. Então, você deverá utilizar o runlevel 3, que inicia e termina a carga em modo texto com suporte à rede. Utilize também o runlevel 5, que dá suporte a rede em modo gráfico.

Você poderá realizar isto utilizando um link simbólico. Veja!

```
#ln –s /etc/rc.d/quotas /etc/rc.d/rc3.d/S10quotas
#ln –s /etc/rc.d/quotas /etc/rc.d/rc5.d/S10quotas
```

O primeiro comando, dos dois que você acabou de ver, cria um *link* simbólico do “quotas” com runlevel 3. O “S” significa que ele será executado na inicialização e após o nono script ser executado.

O segundo comando realiza a mesma tarefa, porém, muda o runlevel para 5.

Para o bom funcionamento, é preciso realizar uma rotina de verificação no sistema de cotas. O ideal é realizar a verificação uma vez por semana, quando nenhum usuário estiver utilizando o sistema. Deve ser executado o comando crontab com o “parâmetro –e”, que irá habilitar o arquivo “cron” para ser editado e adicionar a linha seguinte no final do arquivo.

```
# crontab -e  
0 2 * * 0 /bin/quotacheck -avug
```

Salve.

Estando na linha o comando /bin/quotacheck –avug, este será executado uma vez por semana, às 2 horas da madrugada.

11.4.2 LIMITANDO ESPAÇO

Nesta etapa, você aprenderá a limitar o espaço a ser utilizado pelo usuário. Os limites podem ser de quatro tipos. O **primeiro é o limite físico**, ou seja, um limite total de espaço, também chamado de “user hard limit”, em que o usuário não recebe aviso que seu espaço está no fim, impedindo-o de realizar a gravação. O **segundo é o limite leve**, conhecido também por “user soft limits”. Neste tipo de limite, o usuário receberá o aviso que seu espaço está acabando.

O **terceiro é o limite físico por grupo** ou “group hard limit”. Este tipo limita espaço para um determinado grupo de usuários. Por fim, o **quarto é o limite leve por grupo**, em que os usuários do grupo recebem a informação que o espaço está acabando.

QUOTA

Este comando é utilizado para mostrar as cotas existentes para um usuário ou grupo.

Uso:

```
# quota <opções> usuário ou grupo
```

Opções:

- u cota padrão de um usuário;
- g cota padrão de um grupo;
- q mostra as cotas excedidas;
- v mostra todas as cotas.

Veja um exemplo:

```
# quota -v ctaí
```

Neste exemplo, o programa “quota” irá mostrar as cotas do usuário ctaí.

QUOTAON

Este comando é utilizado para habilitar a gerência de cotas em um dispositivo já configurado.

Uso:

```
# quotaon <opções> <dispositivo>
```

Opções:

- a habilita a gerência para todos dispositivos existentes no arquivo “fstab”;
- g habilita a gerência para o grupo em um dispositivo;
- u habilita a gerência para um usuário em um dispositivo;
- v mostra onde tem gerência habilitada.

Veja um exemplo:

```
# quotaon -avug
```

No exemplo que você viu, o comando “quotaon” está habilitando a gerência de cotas para todos os usuários e grupos nos dispositivos configurados no “fstab”.

QUOTAOFF

Este comando é utilizado para desabilitar a gerência de cotas em um dispositivo.

Uso:

```
# quotaoff <opções> dispositivo
```

Opções:

- a habilita a gerência para todos dispositivos existentes no arquivo "fstab";
- g habilita a gerência para o grupo em um dispositivo;
- u habilita a gerência para um usuário em um dispositivo.

Veja um exemplo:

```
# quotaoff -agu /dev/sda3
```

É importante informar que, uma vez desabilitada a gerência de quotas, antes de reiniciar, é necessário rodar o comando "quotacheck" para atualizar o banco de cotas.

QUOTACHECK

Este comando é utilizado para verificar os dispositivo e construir o banco de dados "quotas". Como já foi informado, este comando deve ser utilizado uma vez por semana.

Uso:

```
# quotacheck <opções> dispositivos
```

Opções:

- a realiza varredura em todos os dispositivos existentes no arquivo "fstab";
- g grupo constrói o banco de cotas para um grupo;
- u usuário constrói o banco de cotas para um usuário;
- v mostra os procedimentos.

Saiba que se não for informado o usuário e grupo, este comando irá construir o banco de cotas de todos os usuários e grupos.

É importante você também saber que antes de utilizar o comando "quotacheck", é necessário desabilitar o gerenciamento de cotas, para depois inicializá-lo.

¹ PERÍODO DE GRAÇA

Quando a cota de um determinado usuário excede, este terá um período para apagar os arquivos desnecessários, a fim de liberar espaço. Esse período é chamado de 'Período de Graça'.

Veja um exemplo:

```
# quotaoff -a
# quotacheck -aug
# quotaon
```

Caso não siga esta orientação, você poderá perder todas as informações.

EDQUOTA

Este comando é utilizado para determinar os espaços para usuários e grupos de usuários.

Uso:

```
# edquota <opções> <usuário ou grupo>
```

Opções:

- g determina cota para grupo;
- u determina cota para usuário;
- p copia a configuração de um usuário para outro;
- t configura o **período de graça**¹ para grupo ou usuário e deve ser acompanhado do “-g” ou “-u”.

Veja um exemplo:

```
#edquota -u cta1
```

Ao executar o comando, o editor de texto irá abrir o “edquota”, conforme demonstrado a seguir:

```
Quotas for user: cta1
/dev/sda3: blocks in use: 150, limits (soft=20000,
hard=22000)
Inodes in use: 130,limits (soft=0,hard=0)
```

Altere os tamanhos *soft* e *hard* para o que desejar, e saia do arquivo salvando.

Para usar o Período de Graça, o princípio é o mesmo:

edquota -tu cta1

Realize as alterações e saia salvando.

REPQUOTA

Este comando é utilizado para gerar relatórios das cotas dos dispositivos.

Uso:

repquota <opções> <dispositivo>

Opções:

- a relatório de todos os dispositivos;
- u relatório por usuário;
- g relatório por grupo;
- v monta cabeçalho descritivo.

Veja um exemplo:

repquota -va



RECAPITULANDO

Este capítulo apresentou à você diversas orientações de como criar contas e grupos de usuários, bem como, administrá-las. Você viu como permitir o acesso de usuário e grupos e arquivos ou diretórios. Por último, você estudou as cotas de disco, aprendendo como criar uma cota para determinado usuário ou grupo e a sua importância para o sistema, além da importância de gerenciar os bancos de cotas.

Sistemas Operacionais

12



Neste capítulo do livro didático, serão apresentados os sistemas operacionais de rede e os tipos mais importantes de sistemas de rede, além dos detalhes sobre a instalação de um sistema operacional de arquitetura aberta e fechada.

E ao final deste capítulo, você estará apto para:

- a) compreender os tipos de sistemas de rede;
- b) compreender os requisitos para atualização ou instalação;
- c) instalar um sistema operacional de arquitetura aberta;
- d) instalar um sistema operacional de arquitetura fechada.

Preparado para encerrar esta última etapa? Lembre-se de que o diálogo com seu professor sobre o conteúdo estudado tem muito a contribuir para a evolução do seu aprendizado. Evite deixar dúvidas. Seja curioso e discuta sobre os temas abordados.

¹ SERVICE PACK

É um pacote de correção para um determinado programa ou para um sistema operacional.

12.1 SISTEMAS OPERACIONAIS DE REDE

Os sistemas operacionais de redes são *softwares* que trabalham em servidores para administrar informações como contas de usuários, segurança e outras funcionalidades de uma rede. Têm como finalidade o compartilhamento de recursos, como o compartilhamento de arquivos e de impressoras.

Os sistemas operacionais de rede também são conhecidos como **Network Operating System – NOS**.

Alguns dos sistemas operacionais de rede, como Linux, Unix, Microsoft Windows 2000 Server, Microsoft Windows 2003 e 2008 Server, dentre outros, podem ser atualizados para novas versões sem a necessidade de uma reinstalação total.

O sistema que será tratado na instalação é um Linux, com distribuição Debian Squeeze e Microsoft Windows 2008 Server. Acompanhe!

Microsoft Windows NT

Não possui mais atualizações para este sistema, sua última atualização foi para o *Service Pack 6*. Trata-se de uma arquitetura fechada.

Microsoft Windows 2000 Server

Não possui mais atualizações para este sistema. Sua última atualização foi para o *Service Pack 3*. Trata-se de uma arquitetura fechada.

Microsoft Windows 2003 Server

Este sistema está em funcionamento até o presente momento e é muito utilizado no mercado corporativo. Sua atualização está no *Service Pack 2*. Não há notícias sobre novas atualizações até o momento. Trata-se também de um sistema de arquitetura fechada.

Microsoft Windows 2008 Server

Trata-se do produto mais recente da Microsoft e sua atualização está no *Service Pack¹ 1*. Está sendo bastante utilizado no mercado e acredita-se que irá ocupar o espaço do Windows 2003. Também possui uma arquitetura fechada.

12.1.1 LINUX

É um sistema de rede de arquitetura aberta bastante utilizado em servidores e possui diversas distribuições, como Debian, Ubuntu, entre outros. Suas atualizações são diretas nos servidores repositórios e sem nenhum custo adicional. São os sistemas de rede mais utilizados no mercado corporativo, além do UNIX e o NOVELL, por exemplo.

Para realizar a instalação ou atualização de um sistema operacional de rede é necessário seguir alguns cuidados antes da atualização. Veja, a seguir, que cuidados são esses.

Requisitos do sistema

Nesta etapa, deve-se verificar a compatibilidade de todos os *hardwares* existentes no equipamento com o novo sistema.

Atualizar ou instalar

Deve-se analisar a possibilidade de atualizar o sistema ou se será necessário reinstalar o sistema todo.

Domínio

No caso de um servidor de domínio, verificar a existência de *backup* dos arquivos do domínio.

Sistema de arquivo

Defina qual sistema de arquivo será utilizado. Poderá ser: ntfs, fat, fat32, ext2 ou ext3.

Logs

Analizar os *logs* do sistema antigo para verificação de erros que possam prejudicar atualização do sistema.

Backup

Realizar *backup* dos arquivos do servidor e relação de impressoras , caso este seja o servidor de impressão.



**SAIBA
MAIS**

Quer saber mais sobre os sistemas operacionais de rede da Microsoft? Acessando o endereço a seguir, você encontrará todas as informações pertinentes aos produtos da Microsoft, bem como informações de atualização dos sistemas operacionais de rede.

<<http://www.microsoft.com>>.

12.2 INSTALAÇÃO SISTEMA OPERACIONAL DE ARQUITETURA ABERTA

É possível definir um sistema operacional de arquitetura aberta como sendo um sistema de código livre, que pode ser copiado, alterado, reproduzido e distribuído sem a necessidade de pagar por sua licença.

² BIOS

Basic Input/Output System (Sistema Básico de Entrada/Saída) é um programa com a responsabilidade de acesso ao *hardware* do equipamento.

Um *software* deve atender a algumas exigências para ser considerado livre, tais como:

- a) que seja executado para toda e qualquer função;
- b) que possa ser distribuído, contribuindo para o conhecimento de todos;
- c) que esteja disponível para ser copiado;
- d) que seu código esteja disponível para análises.

Todo o *software* livre ou aberto também possui licença, mas licença de *software* livre, como por exemplo, o GNU/GPL licença pública geral.

O sistema operacional de arquitetura aberta a ser utilizado neste material didático é o sistema Linux distribuição Debian Squeeze. Conheça mais alguns detalhes a seguir.

12.2.1 PROCEDIMENTOS INICIAIS

A instalação dos sistemas de arquitetura aberta (Linux) pode até parecer complicada, mas é muito simples, necessitando apenas ter especial atenção em cada passo da instalação. Antes de começar a instalação do sistema Linux, você deve estar atento para as seguintes informações:

- a) se o equipamento a ser instalado no Linux possuir algum sistema operacional ativo, faça *backup*;
- b) drives como placa de vídeo, rede, etc. podem ser necessários;
- c) CD ou pen-drive contendo a imagem da distribuição escolhida;
- d) se o equipamento faz parte de uma rede, tenha em mãos: o nome da máquina, o número do IP, a máscara de rede, *gateway*, DNS e domínio.

12.2.2 CONFIGURAÇÃO DO *BOOT*

Para que a instalação do novo sistema possa ser iniciada por meio da unidade de CD-ROM, é preciso fazer algumas configurações no *setup* do equipamento (BIOS).

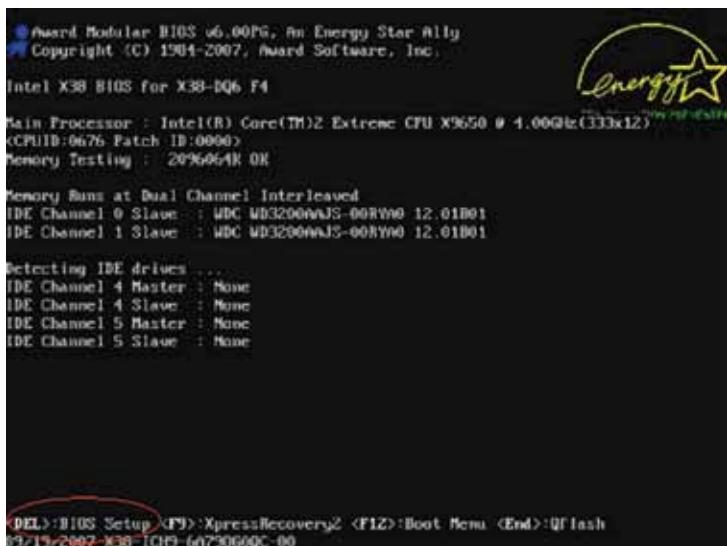
Para saber como realizar a configuração do *boot*, siga os passos seguintes.

Passo 1

Ligue o equipamento e no processo de inicialização da BIOS², pressione a tecla DEL.


FIQUE ALERTA

Em alguns equipamentos a tecla de *setup* pode ser F2 ou F11.

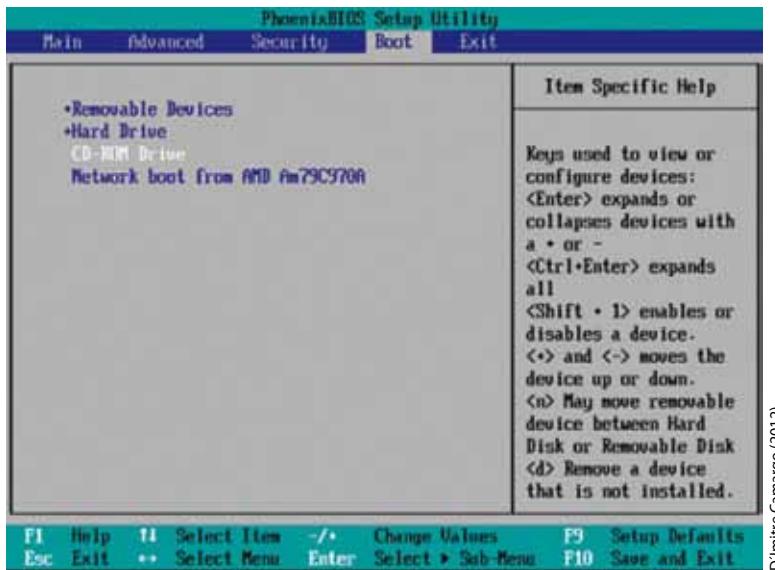


Dimitre Camargo (2012)

Figura 72 - Tela da BIOS

Passo 2

Selecione a aba de *BOOT* e mova o cursor até a opção *CD-ROM drive*.



Dimitre Camargo (2012)

Figura 73 - Tela BIOS Setup aba Boot

Passo 3

Com as teclas + / -, altere a ordem dos dispositivos de *boot*, de maneira que a unidade de CD-ROM tenha preferência durante o processo de inicialização.



Figura 74 - Tela BIOS Setup aba Boot

Passo 4

Após realizar alteração na ordem de inicialização do *boot*, para que inicialize por meio da unidade de CD-ROM, pressione tecla F10 para que as alterações sejam salvas.

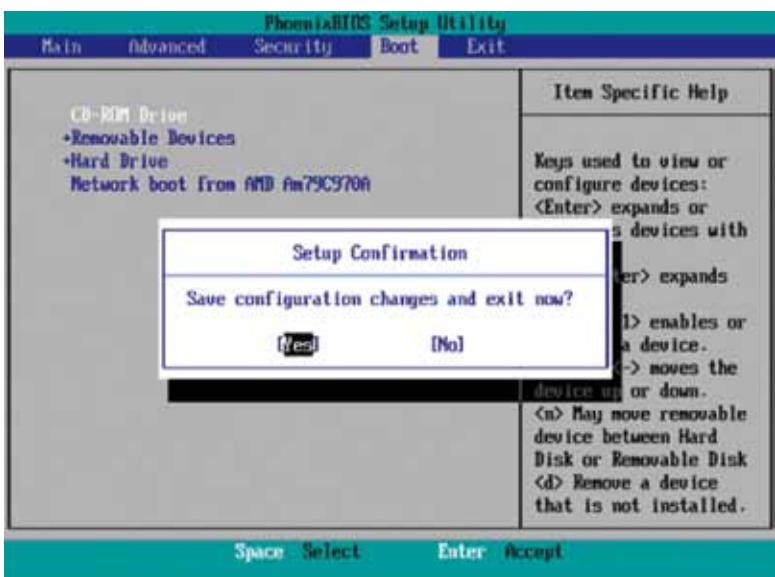


Figura 75 - Salvando configuração Setup

12.2.3 INICIANDO A INSTALAÇÃO DO SISTEMA LINUX

Após ter realizado as configurações na BIOS do equipamento, coloque um disco com a instalação do sistema operacional Linux (distribuição à sua escolha) na unidade de CD-ROM, e aguarde o início da instalação do sistema.

É importante lembrar que neste material didático todas as configurações foram baseadas na distribuição Linux Debian.



VOCÊ SABIA?

Foi em 1983 que Richard Stallman criou a primeira fundação de software livre: a *Free Software Foundation*.

TIPOS DA INSTALAÇÃO

Install – Instalação em modo texto.

Graphical Install – Instalação em modo gráfico.

Advanced Options – Opções avançadas.

Help – Ajuda.

Agora siga algumas etapas para a instalação.

Passo 1

Selecione “Install” e pressione ENTER.



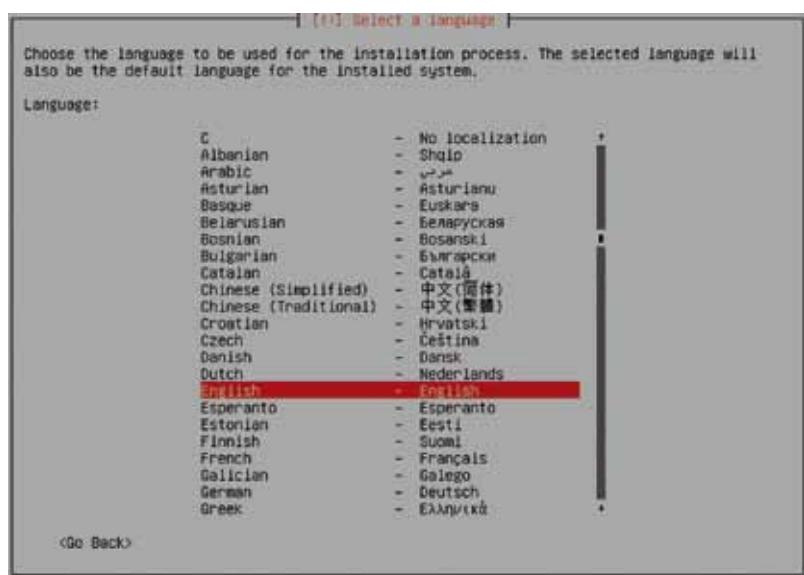
D'Inítre Camargo (2012)

Figura 76 - Menu BOOT

Passo 2

Idioma

Nesta etapa, você deve escolher o idioma para o processo de instalação. Servidores de rede, ao contrário de estações de trabalho, devem ser instalados na língua inglesa, o que dificulta o acesso de pessoas sem conhecimento no sistema. Selecione *English – English*. Desta forma, serão evitadas traduções erradas ou até traduções literais de termos em inglês, que poderão dificultar a navegação no sistema de arquivos. Posteriormente, selecione o Idioma e pressione ENTER.



D'Imitre Camargo (2012)

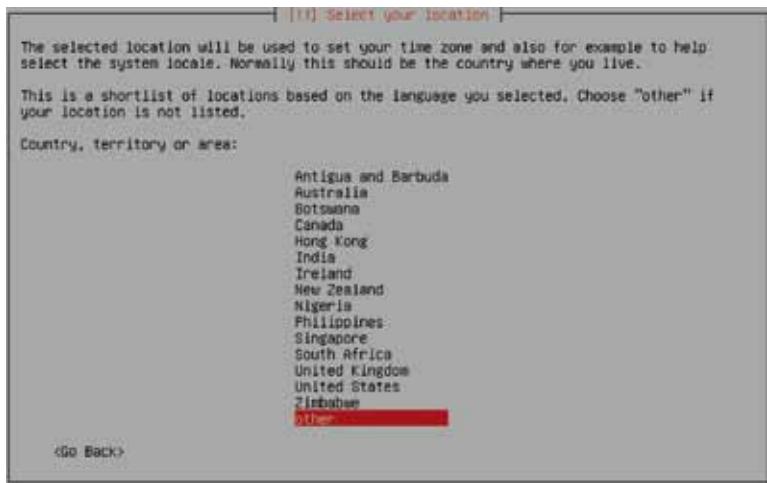
Figura 77 - Escolha do Idioma

Passo 3

Localização geográfica

Nesta etapa, você deve selecionar a sua localização, são três telas. Note que na primeira tela não existe a opção *South America* (America do Sul) então, você deve escolher "Other".

Selecione "Other" e pressione ENTER.



D'Imitre Camargo (2012)

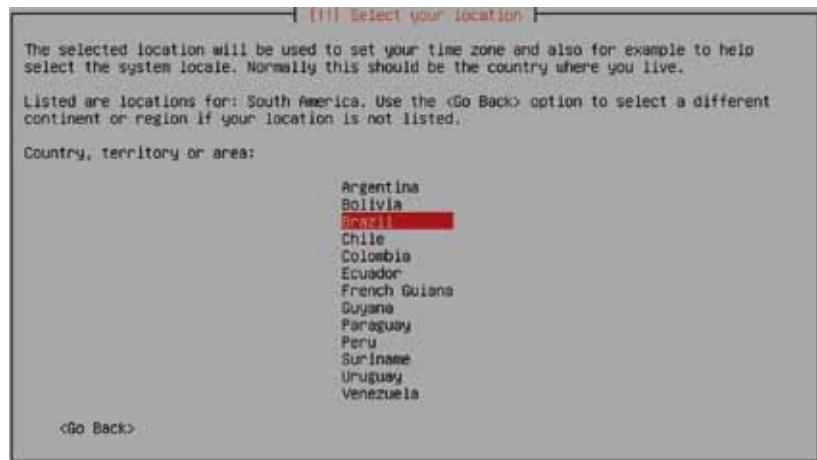
Figura 78 - Localização Geográfica I



D'Imitre Camargo (2012)

Figura 79 - Localização Geográfica II

Na terceira tela, selecione "Brazil" e pressione ENTER.



D'Imitre Camargo (2012)

Figura 80 - Localização Geográfica III

Na terceira tela, selecione “United States – en_US.UTF-8” e pressione ENTER.



D'Imitre Camargo (2012)

Figura 81 - Configurações Locais IV

12.2.4 LAYOUT DO TECLADO

Nesta etapa, você deve selecionar a opção mais adequada para o sistema. Se o teclado possuir a tecla ç, selecionar a opção *Brazilian (ABNT2 layout)*, mas caso não possua, selecione o *layout* de acordo com o manual do fabricante.

Passo 1

Selecione “Brazilian (ABNT2 layout)” e pressione ENTER.



Figura 82 - Layout do Teclado

Terminadas as configurações iniciais, o processo de instalação irá efetuar uma série de verificações de forma a identificar os dispositivos do sistema (CD-ROM, rede, etc.) sem a necessidade de interação com o usuário.

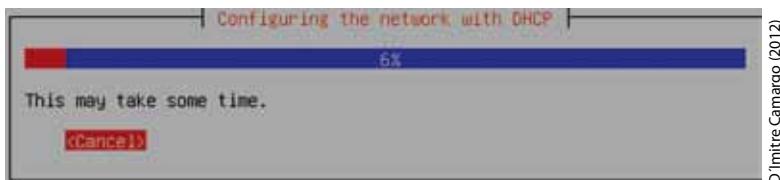


Figura 83 - Tela de Verificação de Dispositivo

CONFIGURAÇÃO DA REDE

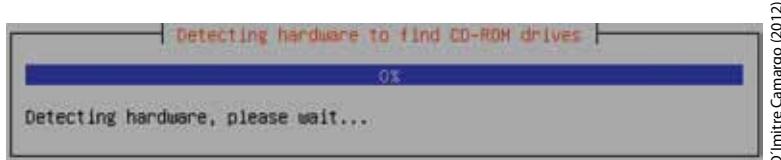
Nesta etapa, duas situações podem acontecer: a primeira, se existir um servidor DHCP na rede, o endereço IP será configurado automaticamente. A segunda, caso não exista o servidor DHCP, será exibida uma tela com erro.

Passo 1

Na primeira tela, o sistema tentará configurar o endereço IP para o servidor de maneira automática, por meio de um servidor DHCP.

³ MÁSCARA DE REDE

É um endereço de 32 bits usado para separar um endereço IP em duas partes, endereço de rede e endereço de host (máquina).



Dimitre Camargo (2012)

Figura 84 - Configuração Rede DHCP

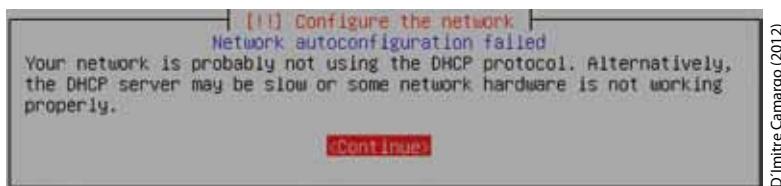
⁴GATEWAY

É o ponto de entrada e saída da rede local, ou seja, a comunicação com a Internet é feita através do gateway. Na maioria das vezes, o gateway da rede é o roteador.

Passo 2

Caso não possua um servidor DHCP na rede, o sistema apresentará uma tela indicando erro na configuração automática da rede.

Selecione “continue” e pressione ENTER.



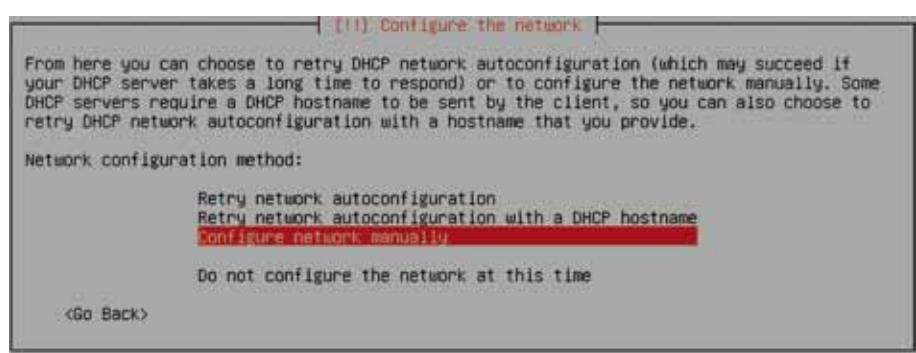
Dimitre Camargo (2012)

Figura 85 - Erro na Configuração da Rede

Passo 3

Após pressionar ENTER, na opção “continue” uma tela de configuração manual de rede será apresentada.

Selecione “Configure Network Manually” e pressione ENTER.



Dimitre Camargo (2012)

Figura 86 - Configuração de Rede Manual

Nas telas seguintes serão solicitadas as configurações da rede como: endereço IP, nome do equipamento, máscara de rede e DNS. Lembra dos procedimentos iniciais, em que era importante anotar estas informações? Você irá utilizá-las a seguir.

Passo 4

Informe o “IP address” e pressione ENTER.

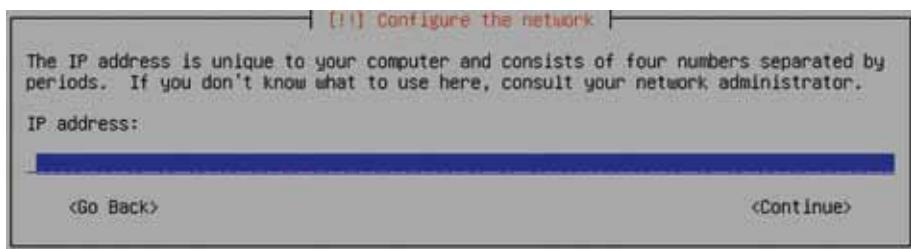


Figura 87 - IP Address

D'Imitre Camargo (2012)

Passo 5

Na tela a seguir, você deve informar o endereço de máscara de rede³.

Informe a “Netmask” e pressione ENTER.

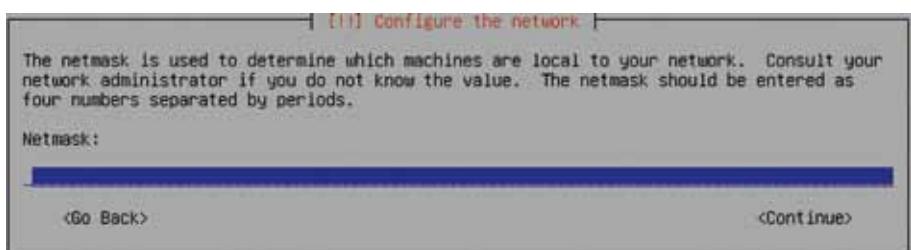


Figura 88 - Máscara de Rede

D'Imitre Camargo (2012)

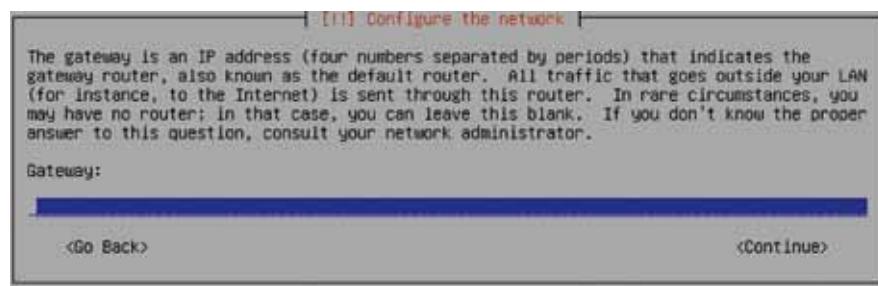
Passo 6

Nesta tela, deve ser informado o endereço *gateway*⁴ da rede.

Informe o “Gateway” e pressione ENTER.

⁵ DNS

Domain Name System (Sistema de Nomes de Domínio) os servidores de nomes fazem a conversão de nomes de máquinas para endereço IP e endereços IP para nomes de máquinas.



Dimitre Camargo (2012)

Figura 89 - Gateway da Rede

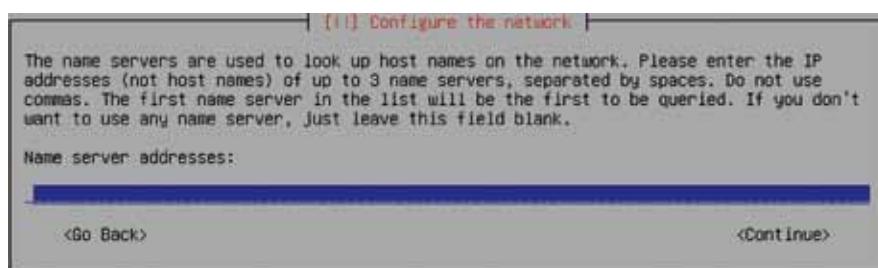
⁶ DOMAIN NAME

Domain Name (ou servidor de domínio): é o gestor dos recursos da rede, como por exemplo, administração de contas de usuários, administração de computadores, autenticação de usuários através da validação de senhas, políticas de segurança, etc.

Passo 7

Nesta, configure o endereço do servidor DNS⁵.

Informe o “Name Server Addresses” e pressione ENTER.



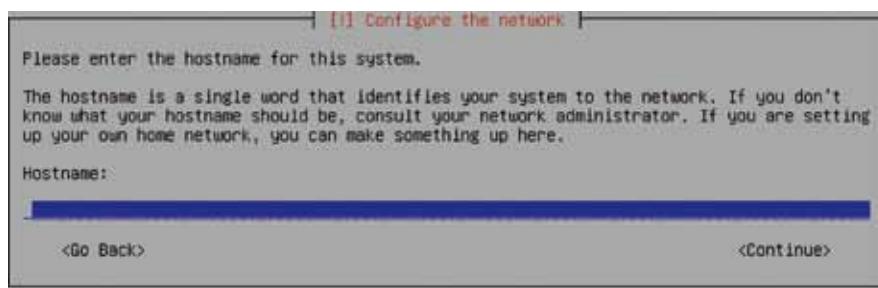
Dimitre Camargo (2012)

Figura 90 - Endereço DNS

Passo 8

Nesta tela, você deve informar o nome do equipamento para sua identificação na rede.

Informe o “Hostname” e pressione ENTER.



Dimitre Camargo (2012)

Figura 91 - Nome do Equipamento

Passo 9

Nesta, deve ser informado o domínio ao qual o equipamento irá fazer parte, caso exista.

Informe o “Domain Name⁶”, selecione “continue” e pressione ENTER.

Informe a senha do “root” e pressione ENTER.

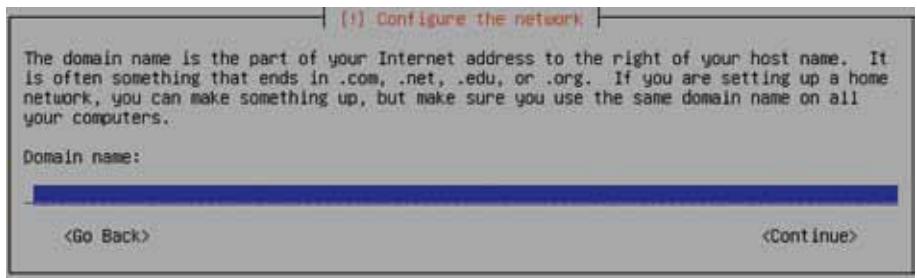


Figura 92 - Nome do Domínio

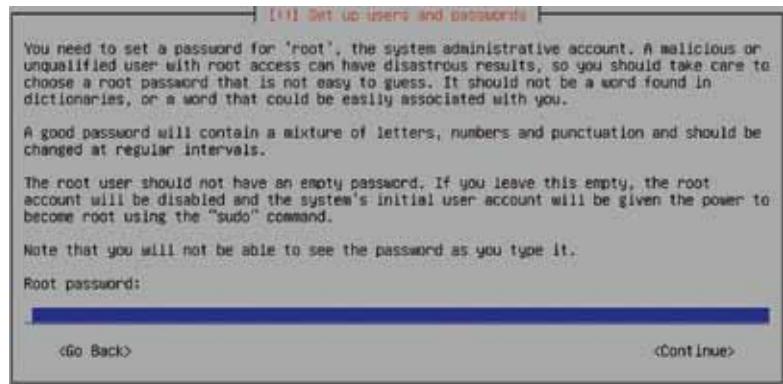
CONFIGURAÇÃO DE USUÁRIO E *PASSWORD*

É nesta etapa da configuração que se realiza a criação de usuários e suas senhas. Um usuário muito importante para o sistema é o usuário “root” ou super usuário. O usuário root é o que faz todas as instalações e modificações no sistema após sua instalação. Também será criado, nesta etapa, o primeiro usuário para utilização do Linux.

A senha para o usuário root deverá conter, no mínimo, 8 caracteres (incluindo números e letras e maiúsculas e minúsculas). É importante guardar em local bem seguro. Siga os passos a seguir.

Passo 1

Em “root password” insira a senha do root e pressione ENTER.



Dmitre Camargo (2012)

Figura 93 - Senha do root

Passo 2

Nesta tela, será necessário repetir a senha do *root* para confirmação.

Em "Re-enter password to verify:" repita a senha e pressione ENTER.



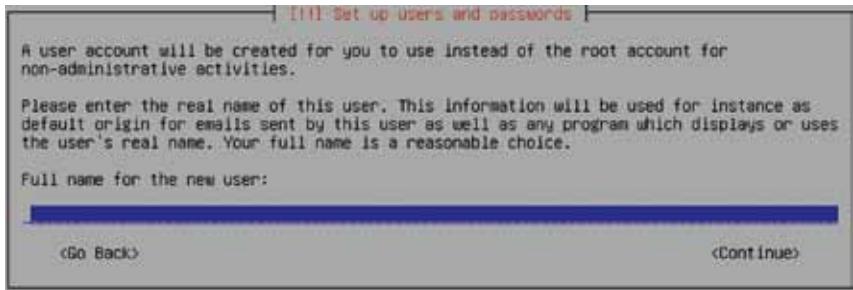
Dmitre Camargo (2012)

Figura 94 - Repetindo a senha do root

Passo 3

Nesta tela será criado o primeiro usuário para utilização do sistema operacional. Deve-se incluir o nome completo e, logo após, o apelido para o usuário e sua senha. Após a instalação do sistema, é possível criar outros usuários com o auxílio do comando "adduser", que será mostrado na parte de administração do sistema de rede. Este usuário não terá poderes de super usuário.

Em "Full name for the new user:", insira o nome completo do novo usuário e pressione ENTER.



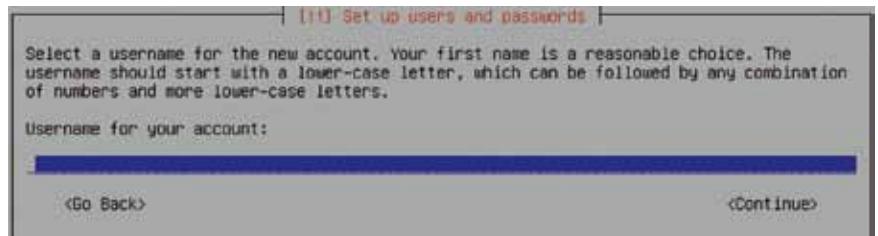
D'Imitrie Camargo (2012)

Figura 95 - Criando novo Usuário

Passo 4

Nesta tela, deve-se escolher um apelido para o usuário, pode ser apenas o primeiro nome, ou qualquer nome de fantasia.

Em "Username for your account:" insira o apelido do usuário e pressione ENTER.

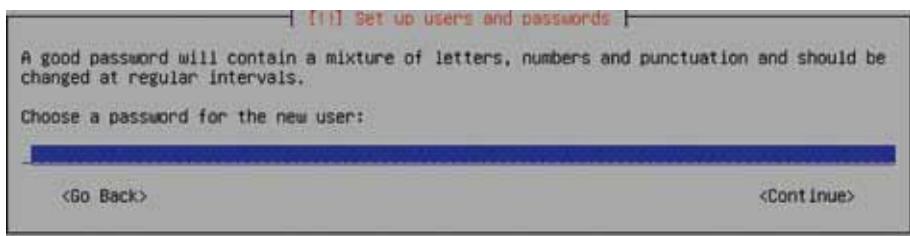


D'Imitrie Camargo (2012)

Figura 96 - Apelido do usuário

Passo 5

Em "Choose a password for the new password:", insira uma senha com no mínimo 8 caracteres, seguindo o mesmo padrão para o usuário root, e pressione ENTER.

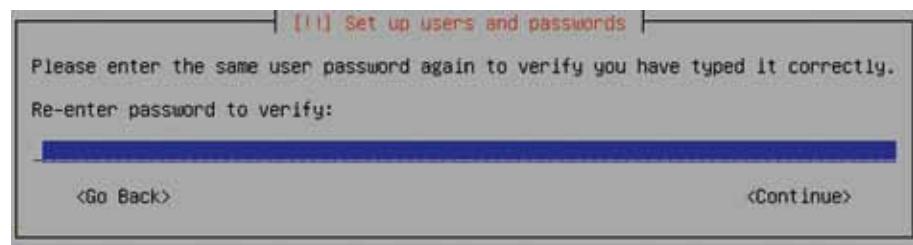


D'Imitrie Camargo (2012)

Figura 97 - Senha usuário comum

Passo 6

Em “Re-enter password to verify:” repita a senha e pressione ENTER.



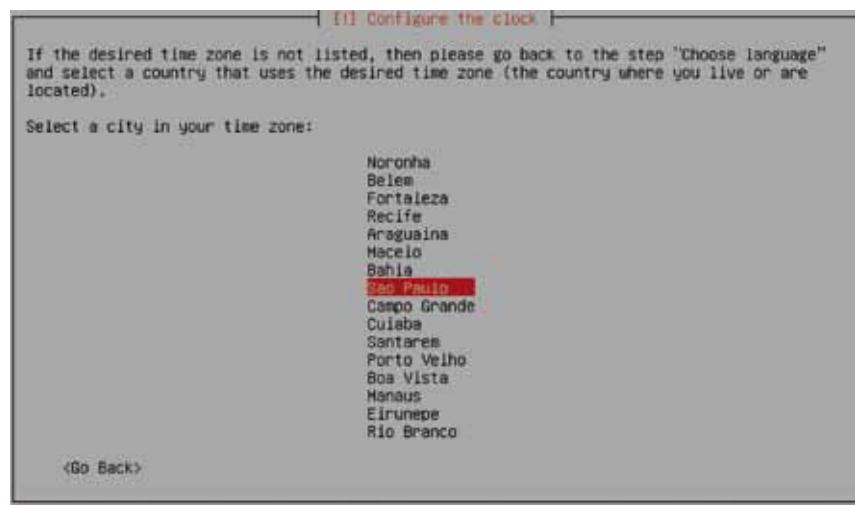
Dimitre Camargo (2012)

Figura 98 - Repetindo a senha do usuário comum

Passo 7

Fuso horário

Nesta etapa, você deve configurar o fuso horário que corresponda a alguma região. No exemplo, a região escolhida foi São Paulo.



Dimitre Camargo (2012)

Figura 99 - Fuso Horário

Após esta etapa, será feita, de forma automática, a detecção dos discos e *hardware* sem a necessidade de interferência do usuário.

DIVISÃO DO DISCO

Esta etapa é a mais importante no processo de instalação de um sistema Linux. Neste momento, deve-se partitionar o disco de maneira que ocorra uma melhor relação desempenho/segurança, garantindo a confiabilidade dos dados e a integridade do sistema.

Para a instalação de um sistema GNU/Linux, é necessário apenas uma partição Linux ativa, onde o sistema será instalado. Porém, na maioria dos casos, uma área de troca é necessária para que o sistema utilize como memória virtual. Apesar da utilização de somente duas partições ser uma prática comum em instalações GNU/Linux, o sistema Linux, como comentado em capítulos anteriores, pode conter diversas partições, de forma que determinados diretórios fiquem em partições distintas, evitando, por exemplo, que caso haja problema em alguma parte da hierarquia de diretórios, somente a partição que armazena aquela hierarquia seja afetada.

Um exemplo de esquema de particionamento será apresentado a seguir, em forma de tabela. No exemplo, a partição varia de acordo com o tamanho do disco rígido. Nesse exemplo, foi utilizado um disco de 4,3GB. A primeira partição primária a ser criada terá o tamanho de 64MB, suficiente para atender ao diretório */boot*, onde estarão residentes os arquivos responsáveis pela inicialização do sistema. As demais partições deverão ser criadas de acordo com a necessidade do sistema.

É válido você saber que antes de iniciar a divisão do disco é muito importante criar uma tabela, como a seguinte:

Tabela 5 - Partições

PARTIÇÃO	PONTO DE MONTAGEM	TAMANHO (MB)	TIPO S.A.
Primária	<i>/boot</i>	64	Ext3
Primária	<i>/</i>	3000	Ext3
Lógica	<i>/var</i>	500	Ext3
Lógica	<i>/home</i>	500	Ext3

Quando se fala em sistema de arquivos, o procedimento de particionamento e formatação dos discos é preferencialmente realizado na instalação do sistema, mas pode ser realizado por meio do comando “fdisk”, após a instalação do sistema.

A tela seguinte representa o local onde se define o método de particionamento do disco. Essa definição poderá ser de forma automática ou manual. Acompanhe, então, os seguintes passos.

Passo 1

Selecione “manual” e pressione ENTER.



Dmitri Camargo (2012)

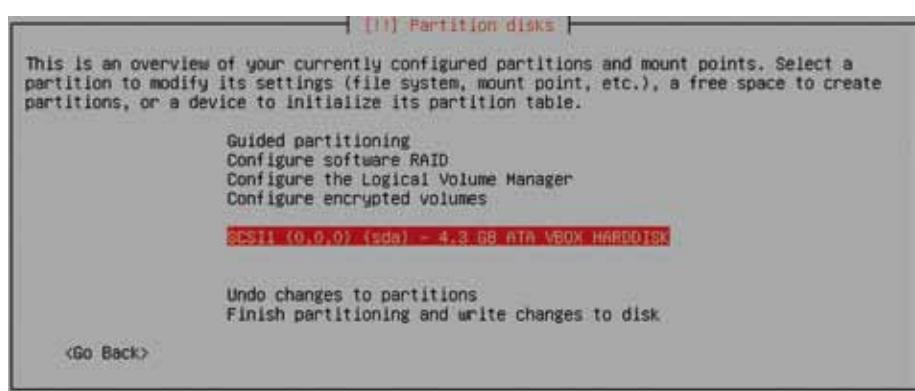
Figura 100 - Método de Particionamento

Passo 2

Nesta tela serão exibidos os(s) disco(s) disponíveis no equipamento. No caso, será exibido apenas um disco scsi sda de 4.3GB.

Selecione o disco para a instalação e pressione ENTER.

É importante você saber que sempre pode desfazer uma ação efetuada selecionando “GO BACK” (voltar).



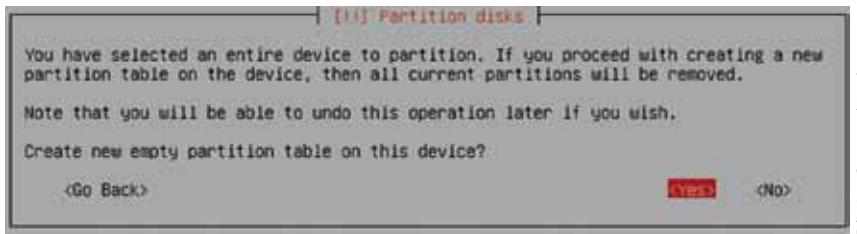
Dmitri Camargo (2012)

Figura 101 - Selecionando o Disco

Passo 3

Nesta tela, será solicitada a criação de uma nova tabela de partição vazia.

Selecione “Yes” e pressione ENTER.



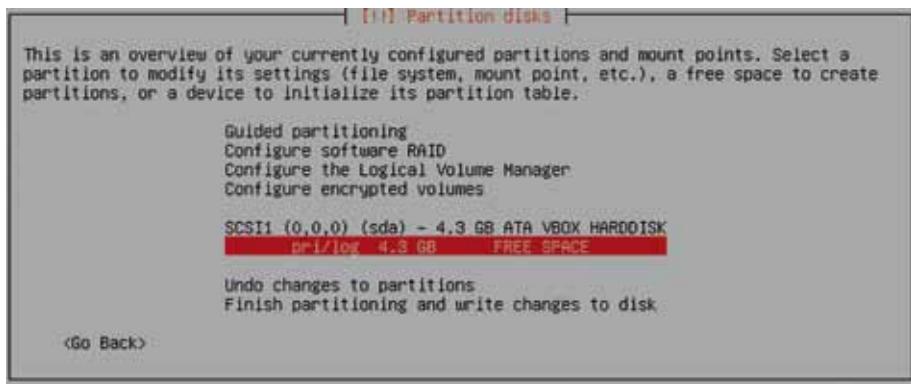
Dmitre Camargo (2012)

Figura 102 - Criar Tabela de Partição

Passo 4

Na tela seguinte, será apresentado o espaço livre no disco disponível para a instalação do sistema.

Selecione a área livre do disco “free space” e pressione ENTER.



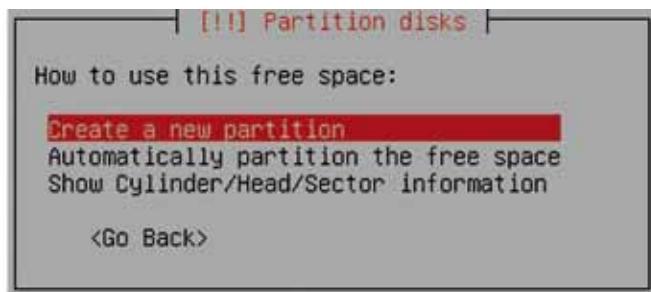
Dmitre Camargo (2012)

Figura 103 - Área Livre do Disco (free space)

Passo 5

Nesta tela, será dado o início da criação das partições no disco livre.

Selecione “Create a new partition” e pressione ENTER.



Dmitre Camargo (2012)

Figura 104 - Nova partição

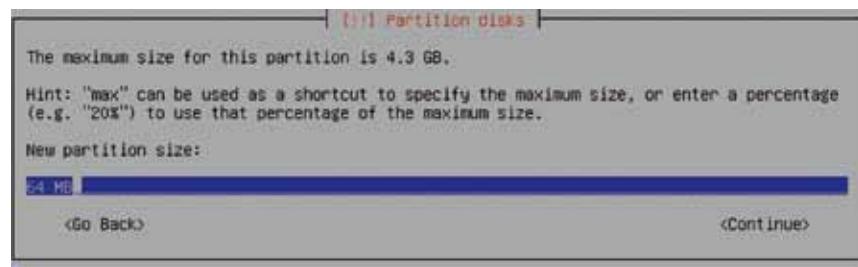
7 PONTO DE MONTAGEM

Local no sistema onde o conteúdo do dispositivo estará disponível para que você possa ler ou alterar.

Passo 6

Nesta tela, cria-se a primeira partição. Você está lembrado da tabela de partição que foi criada anteriormente?

Em “new partition size:”, você deve informar o tamanho da primeira partição. Selecione “continue” e pressione ENTER.



Dmitre Camargo (2012)

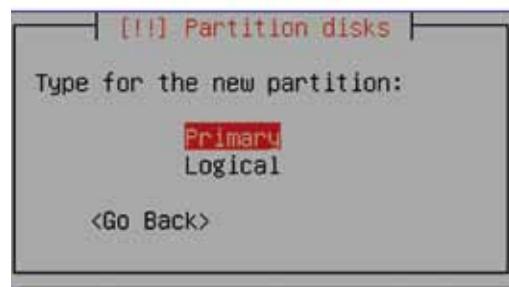
Figura 105 - Tamanho da nova partição

Passo 7

Nesta tela, deve-se informar o tipo da partição que será criada, Primária ou Lógica (estendida).

Seguindo a figura a seguir, esta partição de 64MB é primária.

Selecione “Primary” e pressione ENTER.



Dmitre Camargo (2012)

Figura 106 - Tipo da partição

Passo 8

Nesta tela, é necessário escolher em qual local a partição deverá ser criada, se no início ou no final do espaço livre do disco.

Nossa partição será criada no início do disco.

Selecione “Beginning” e pressione ENTER.

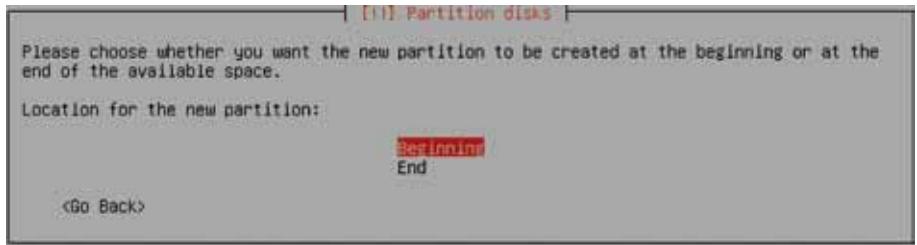


Figura 107 - Localização da Partição

Passo 9

Na tela que você verá a seguir, percebam que na opção “Use as:” está selecionado o sistema de arquivo EXT3 *Journaling file system*, que é o sistema padrão do Linux. Poderia ter sido alterado o tipo do sistema de arquivo para a instalação, bastando apenas selecionar a opção “Use as: e pressionar ENTER. Desta forma, vários sistemas de arquivos estariam a nossa disposição.

Como foi definido na tabela de partição que o sistema de arquivo para a partição de 64MB seria EXT3, não será preciso alterar.

Assim, você deverá então informar o ponto de montagem⁷ da nossa partição. Para isso, selecione “Mount point:” e pressione ENTER.

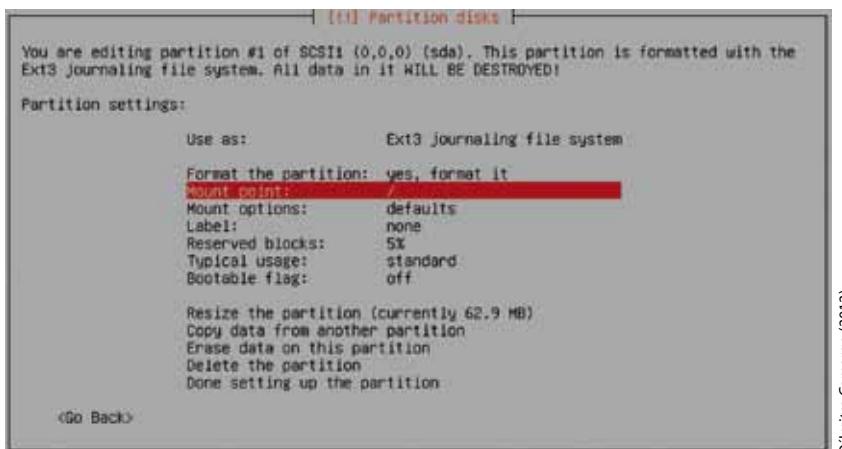


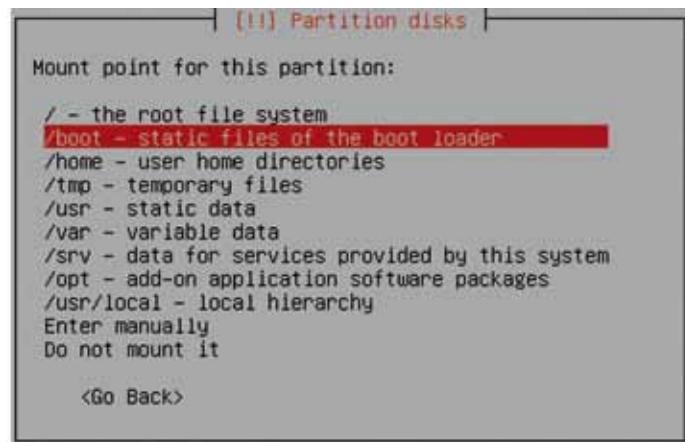
Figura 108 - Editando a partição

Passo 10

Nesta tela, serão apresentados vários pontos de montagem. Devemos escolher o que foi definido para a partição que estamos criando.

Seguindo a tabela criada, esta partição será montada no “/boot”.

Selecione “/boot – static files of the boot loader” e pressione ENTER.



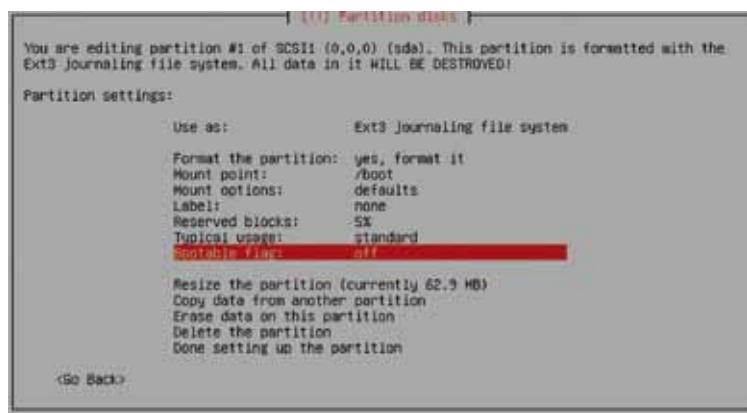
D'Imitre Camargo (2012)

Figura 109 - Ponto de montagem

Passo 11

Nesta tela, deve-se alterar o *flag* de inicialização para ‘iniciado’, fazendo com que a partição criada seja uma partição ativa de *boot*.

Selecione “Bootable flag: off” e pressione ENTER.



D'Imitre Camargo (2012)

Figura 110 - Flag de inicialização

Passo 12

Ao pressionar ENTER, o *flag* será alterado para “on”.

Nesta tela, finalize e grave as mudanças da configuração da primeira partição no disco.

Selecione “Done Setting up the partition” e pressione ENTER.



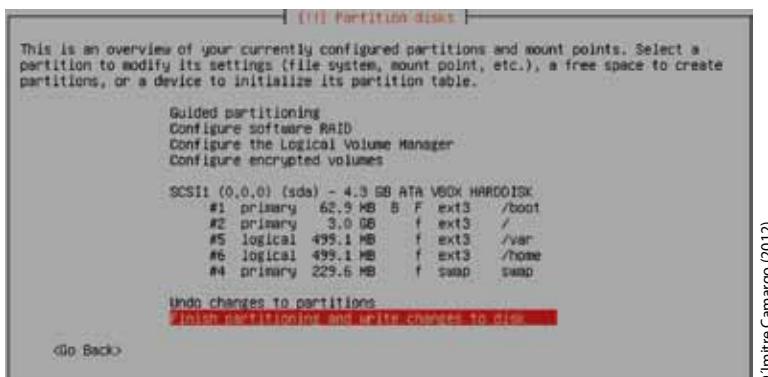
D'Imître Camargo (2012)

Figura 111 - Finalizando a primeira partição

Passo 13

Finalizada a criação desta primeira partição, você deve repetir todos os passos realizados até o momento para a criação das demais partições. Preste atenção para o ponto de montagem, o tipo do sistema de arquivo, o tamanho e o tipo da partição, pois haverá uma partição *swap*.

Ao final da configuração de todas as partições, será exibida uma tela como a seguinte, que mostrará toda a tabela de partição montada. Selecione *Finish partitioning and write to disk* e pressione ENTER para dar continuidade ao processo de instalação do sistema operacional.



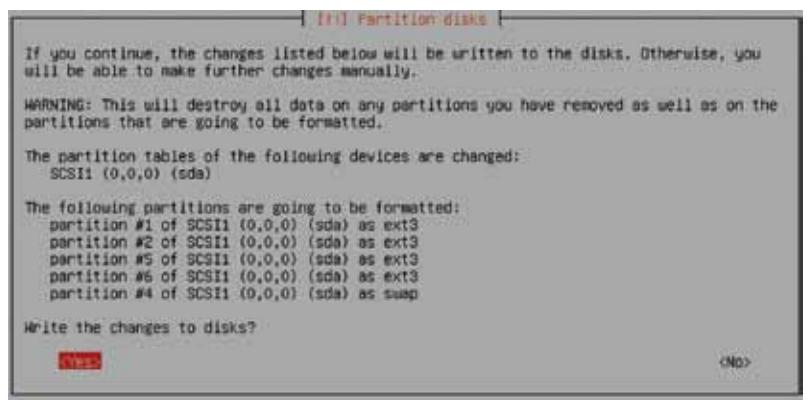
D'Imître Camargo (2012)

Figura 112 - Finalização das partições

Passo 14

É nesta tela que se confirmam todas as alterações realizadas, para dar início ao processo de finalização da instalação do sistema.

Selecione “Yes” e pressione ENTER.

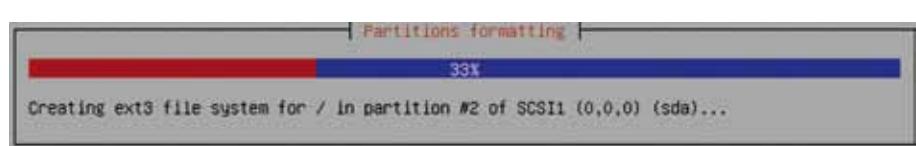


D'Imitre Camargo (2012)

Figura 113 - Gravando as alterações no disco

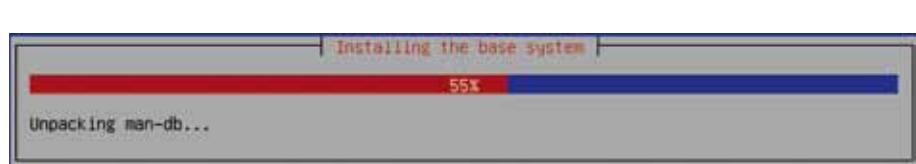
Passo 15

Após a confirmação das alterações no disco, o sistema iniciará a formatação das partições com os sistemas de arquivos solicitados e a instalação dos sistemas básicos. Não há necessidade de intervenção do usuário.



D'Imitre Camargo (2012)

Figura 114 - Formatando as partições



D'Imitre Camargo (2012)

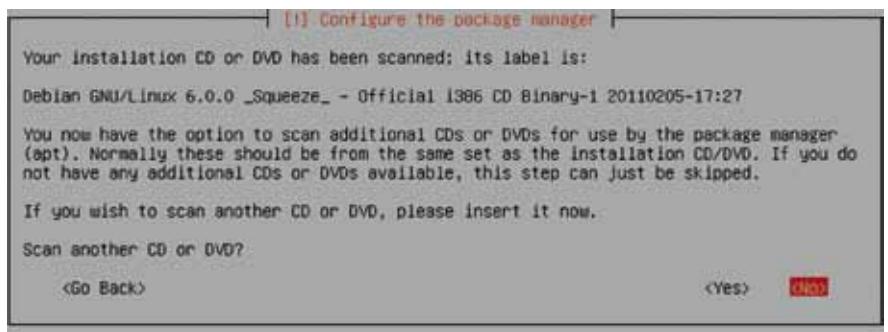
Figura 115 - Instalando sistema básico

Aguarde a finalização.

Passo 16

CONFIGURAÇÃO DO GERENCIADOR DE PACOTES

Nesta etapa será configurado o gerenciador de pacotes do Linux. Caso exista mais de uma mídia com arquivos de instalação do Debian Squeeze, selecione a opção *Yes* para catalogar novas mídias, do contrário, selecione a opção “*No*”. Em seguida, selecione “*No*” e pressione ENTER.



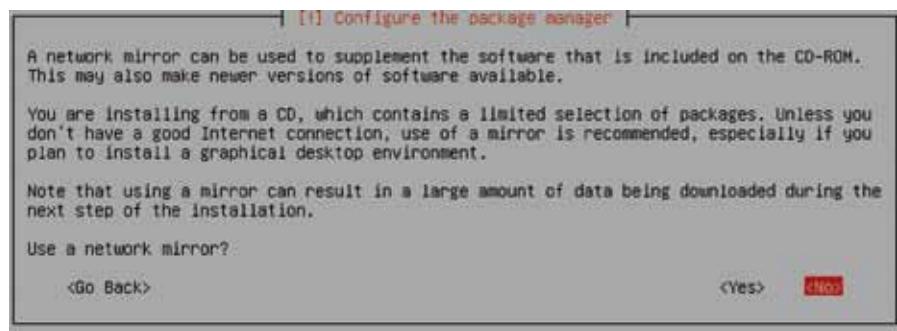
D'Imitre Camargo (2012)

Figura 116 - Gerenciador de Pacotes I

Passo 17

Nesta tela, configura-se o servidor repositório dos pacotes do Linux. Se a máquina a ser instalada possuir acesso à internet, escolha a opção *Yes* para que seja configurada em servidor de repositório de acordo com a localização geográfica do sistema, do contrário, selecionar *No*. É possível selecionar “no”, pois esta função é configurada após a instalação do sistema.

Seleciona “*No*” e pressione ENTER.



D'Imitre Camargo (2012)

Figura 117 - Gerenciador de Pacotes II

Passo 18

Pressione ENTER na opção “no”, e o gerenciador de pacotes irá tentar configurar a lista de repositórios e não conseguirá. Assim, surgirá uma tela com erro.

Note o comentário informando, que a configuração dos repositórios pode ser realizada por meio do arquivo “sources.list”, que está localizado no local “/etc/apt/”.

Selecione “continue” e pressione ENTER.

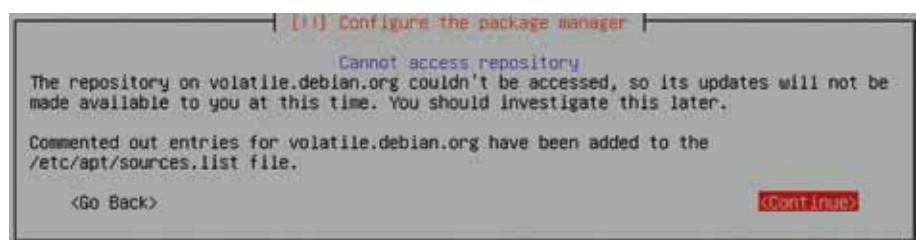


Figura 118 - Erro do gerenciador de pacotes

Passo 19

Nesta etapa, o processo de instalação iniciará a seleção dos *softwares* a serem instalados. Neste primeiro momento, a intervenção do usuário não é necessária.

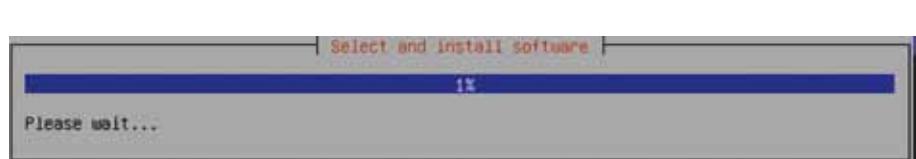


Figura 119 - Seleção de software

Dmitre Camargo (2012)

Passo 20

Nesta tela será perguntado se você deseja participar da pesquisa de utilização de pacotes (requer acesso a Internet). Nesse caso, independe se você selecionar a opção *Yes* ou *No*, pois não há necessidade de participar.

Selecione “No” e pressione ENTER.

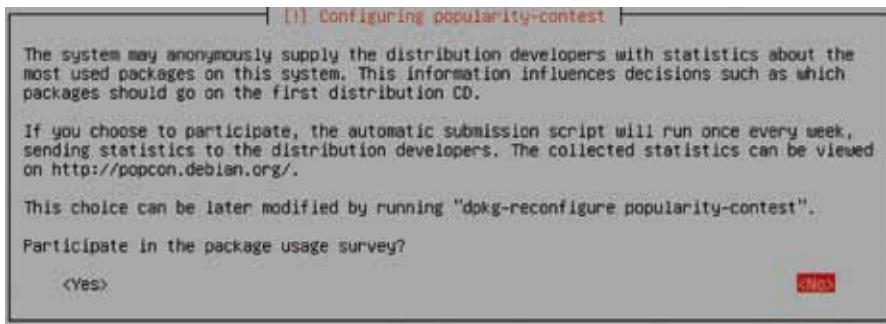


Figura 120 - Pesquisa de Participação

D'Imitre Camargo (2012)

Passo 21

Nesta tela será solicitada a escolha de quais os programas serão instalados, e a escolha dependerá da funcionalidade do equipamento. Para selecionar algum programa, pressione a barra de espaço do teclado em cima do programa.

Todos os programas mencionados na lista podem ser instalados após o término da instalação. Instale apenas o “Standard system utilities”, lembrando que em servidores Linux não se instala o Graphical Desktop.

Selecione “Standard system utilities” e pressione ENTER



Figura 121 - Seleção de software

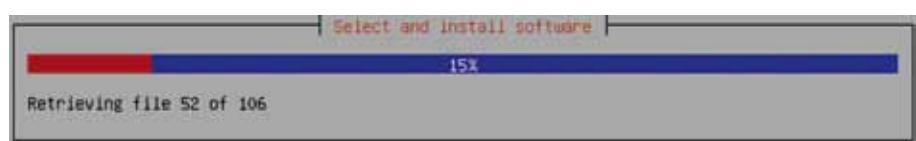
D'Imitre Camargo (2012)

Passo 22

Após a seleção dos softwares, o sistema iniciará a instalação dos mesmos. Não há necessidade de interferência do usuário.

⁸ GRUB

Grub: ou Grand Unified Bootloader é definido como sendo um carregador de vários sistemas operacionais. É muito utilizado quando o equipamento possui *dual-boot*, ou seja, Windows e Linux, onde o usuário pode escolher qual sistema irá carregar.



D'Imitre Camargo (2012)

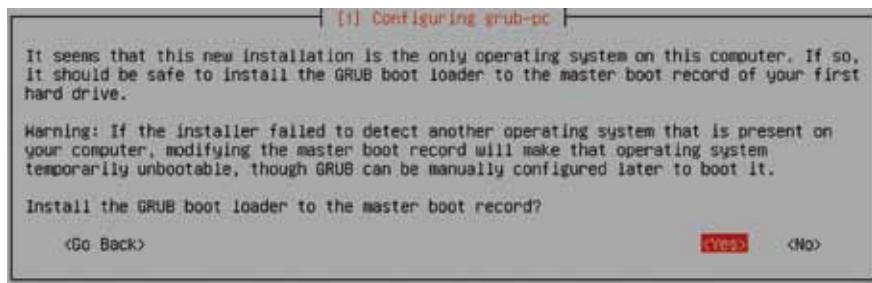
Figura 122 - Instalando software.

Aguarde a finalização.

Passo 23

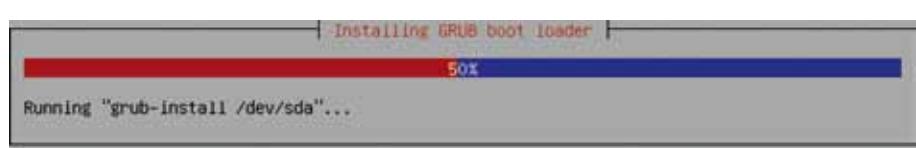
Nesta tela *Install the GRUB⁸ boot loader on a hard disk*, selecionar a opção Yes para que seja instalado o gerenciador de boot, possibilitando a carga no sistema operacional no boot do equipamento.

Selecionar “Yes” e pressione ENTER.



D'Imitre Camargo (2012)

Figura 123 - Instalação do Grub



D'Imitre Camargo (2012)

Figura 124 - Instalando o Grub

Passo 24

Finalizando a instalação

Esta é a etapa final de instalação do sistema. Remover a mídia do *drive* de CD-ROM e selecionar a opção *Continue*, possibilitando o *reset* do equipamento e a carga do sistema operacional.

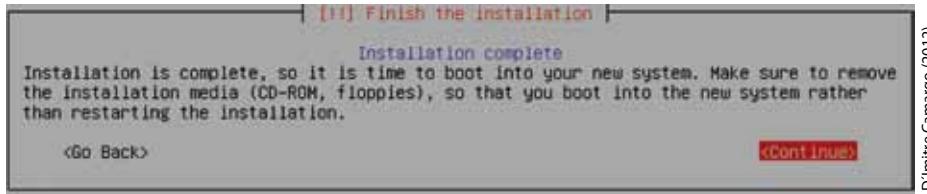


Figura 125 - Finalizando a instalação

D'imitre Camargo (2012)



Figura 126 - Completando a instalação

D'imitre Camargo (2012)

Passo 25

Após o *reset*, o sistema será iniciado pela primeira vez. Na tela abaixo, está sendo mostrada a tela do Grub que está dando carga ao sistema operacional instalado. Se, por ventura, esta máquina estivesse com outros sistemas operacionais instalados, estes seriam mostrados nesta tela.

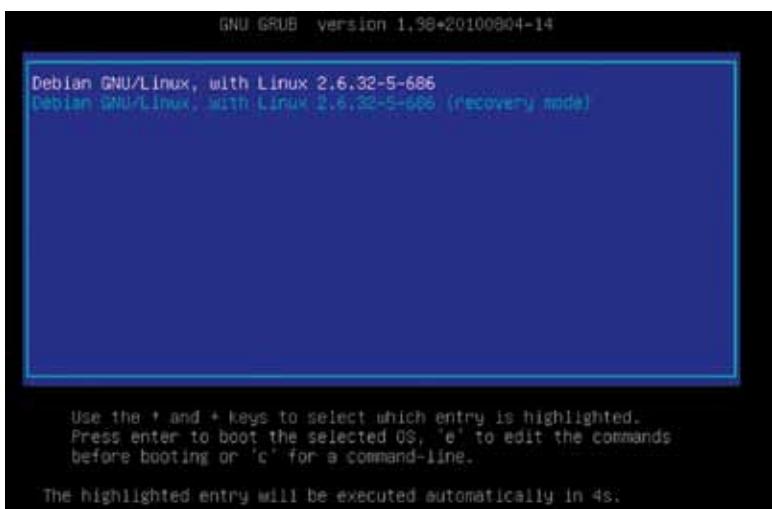


Figura 127 - Grub

D'imitre Camargo (2012)

Passo 26

Após a carga do sistema operacional, esta será a tela de acesso ao Linux. Note que é solicitado um *login*, que é o usuário criado na instalação do sistema.

```
done,
Mounting local filesystems...done.
Activating swapfile swap...done.
Cleaning up temporary files...
Configuring network interfaces...done.
Starting portmap daemon...
Starting NFS common utilities: statd.
Cleaning up temporary files...
Setting console screen modes.
Skipping font and keymap setup (handled by console-setup).
Setting up console font and keymap...done.
Setting kernel variables ...done.
INIT: Entering runlevel: 2
Using makefile-style concurrent boot in runlevel 2.
Starting NFS common utilities: statd.
Starting portmap daemon...Already running..
Starting enhanced syslogd: rsyslogd.
Starting ACPI services...
Starting deferred execution scheduler: atd.
Starting periodic command scheduler: cron.
Starting MTA: exim4.

Debian GNU/Linux 6.0 debian tty1
debian login: _
```

Dmitre Camargo (2012)

Figura 128 - Tela de *login* do Linux

Como informado no começo desse passo a passo, nesta instalação foi utilizado o sistema operacional Linux Debian Squeeze. As configurações aqui realizadas foram as mais básicas.

12.3 INSTALAÇÃO DE SISTEMA OPERACIONAL DE ARQUITETURA FECHADA

Esta arquitetura é definida como 'proprietária', ou seja, seu código possui um dono. Portanto, para sua utilização deverá ser adquirida uma licença para o seu uso. É possível usá-lo por meio da compra de licença, mas não se pode fazer qualquer alteração em código. Um exemplo é o sistema operacional da Microsoft Windows.



**FIQUE
ALERTA**

Jamais instale qualquer produto de arquitetura fechada sem a licença para uso. Do contrário, você poderá ser incluído no artigo 184 do Código Penal. Pirataria é crime!

12.3.1 PROCEDIMENTOS INICIAIS

A instalação dos sistemas de arquitetura fechada (Windows) é mais simples que os sistemas de arquitetura aberta (Linux), mas o procedimento para os dois são os mesmos. Antes de começar a instalação do sistema Windows, você deve ter em mãos as seguintes informações:

- a) se o equipamento que for instalar o Windows possuir algum sistema operacional ativo, faça o *backup*;
- b) *drives* como por exemplo: placa de vídeo, rede, etc., podem ser necessários;
- c) CD ou pen-drive contendo a imagem da distribuição escolhida;
- d) se o equipamento faz parte de uma rede tenha em mãos: (o nome da máquina, o número do IP, a máscara de rede, o *gateway*, o DNS e o domínio).

O processo de configuração do SETUP para inicialização, por meio do CD-ROM, é o mesmo apresentado na instalação do sistema Linux. No entanto, a instalação do Windows 2008 Server deve ser a partir de uma unidade de CD-ROM que leia DVD.

Passo 1

Iniciando instalação

Feitas as configurações no SETUP, coloque o DVD do Windows 2008 na unidade de CD-ROM do equipamento e ligue para que seja iniciada a instalação a partir do CD-ROM.

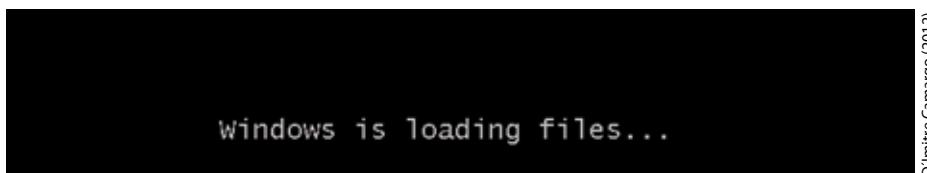


Figura 129 - Início da Instalação

Passo 2

Configuração de idioma

Nesta tela, configure da seguinte forma:

- a) *language to install*: vamos setar com *English*;
- b) *time and currency format*: setar para o formato de tempo e hora do Brasil;
- c) *keyboard or input method*: setar o teclado para o que nos convém.

Pressione o botão NEXT.



D'Imitre Camargo (2012)

Figura 130 - Configuração de idioma

Passo 3

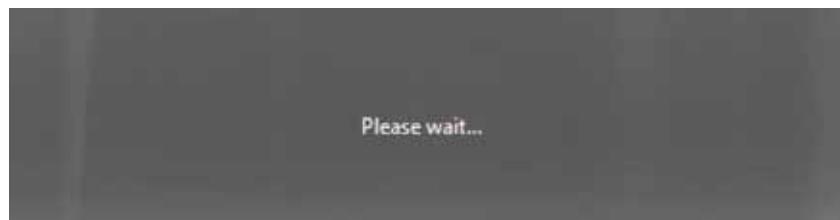
Nesta próxima tela, será iniciada a instalação do sistema operacional.

Pressione INSTALL NOW.



D'Imitre Camargo (2012)

Figura 131 - Iniciando a instalação



D'Imitre Camargo (2012)

Figura 132 - Tela de aguarde

Passo 4

Nesta tela seguinte, você irá selecionar o tipo de sistema operacional que deseja instalar. No exemplo, será instalado o Windows 2008 Standard.

Pressione NEXT.

Operating System	Architecture	Date Modified
Windows Server 2008 Standard (Full Installation)	X86	1/19/2008
Windows Server 2008 Enterprise (Full Installation)	X86	1/19/2008
Windows Server 2008 Datacenter (Full Installation)	X86	1/19/2008
Windows Server 2008 Standard (Server Core Installation)	X86	1/19/2008
Windows Server 2008 Enterprise (Server Core Installation)	X86	1/19/2008
Windows Server 2008 Datacenter (Server Core Installation)	X86	1/19/2008

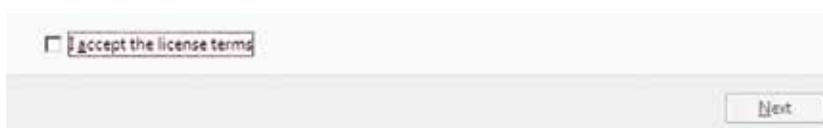
D'Imitre Camargo (2012)

Figura 133 - Escolha do sistema

Passo 5

Nesta tela, você deve aceitar os termos da licença. Selezionando a caixa “Eu aceito os termos da licença”.

Pressione NEXT.



D'Imitre Camargo (2012)

Figura 134 - Licença

Passo 6

Nesta tela de escolha do tipo da instalação, escolha “Custom Advanced”, basta clicar em cima de *Custom Advanced*, que o sistema segue.



D'Imitre Camargo (2012)

Figura 135 - Tipo da instalação

Passo 7

Nesta tela, escolha onde deseja instalar o Windows 2008.

Se quiser instalar na partição selecionada, pressione NEXT.

Se quiser dividir o disco em partições, clicar em *Drive Options (Advanced)*. Como exemplo, selecione *Drive Options (Advanced)*, para dividir o disco.

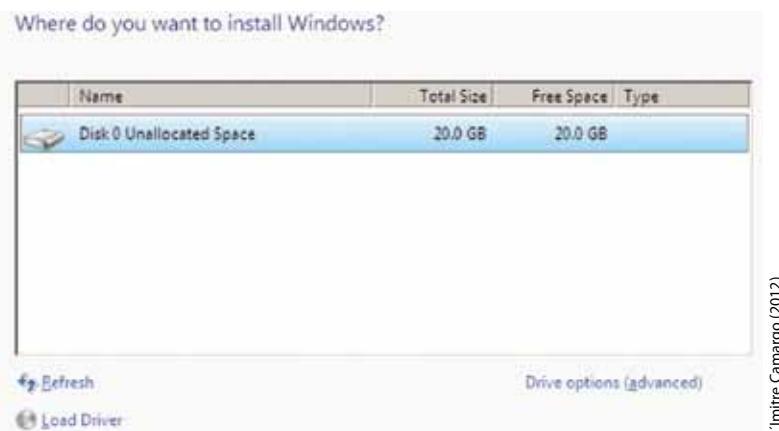


Figura 136 - Local para instalação

Passo 8

Nesta tela, selecione NEW para criar uma nova tabela de partição.



Figura 137 - Local de instalação 1

Passo 9

Selecionado o NEW, surgirá uma opção para determinar o tamanho da partição. Já vem selecionado o tamanho máximo livre no disco.



Figura 138 - Tamanho partição

Passo 10

Alterar para 10Gb e aplicar. Após, clicar em APPLY.

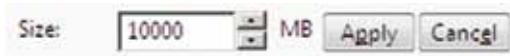


Figura 139 - Partição dividida

D'Imitre Camargo (2012)

Passo 11

Após pressionar APPLY, aparecerá uma tela, como a que você verá a seguir, informando que o disco está dividido em duas partições, de 10GB cada.

Name	Total Size	Free Space	Type
Disk 0 Partition 1	9.8 GB	9.8 GB	Primary
Disk 0 Unallocated Space	10.2 GB	10.2 GB	

Figura 140 - Disco particionado

D'Imitre Camargo (2012)

Passo 12

Selecione a partição que você instalar o sistema e pressione NEXT. No exemplo, foi escolhida a partição primária. O sistema dará início à instalação na primeira partição de 10GB.



Figura 141 - Instalando o Windows

Aguarde o andamento da instalação.



Figura 142 - Andamento da Instalação

Passo 13

O sistema será reiniciado automaticamente, sem a intervenção do usuário.

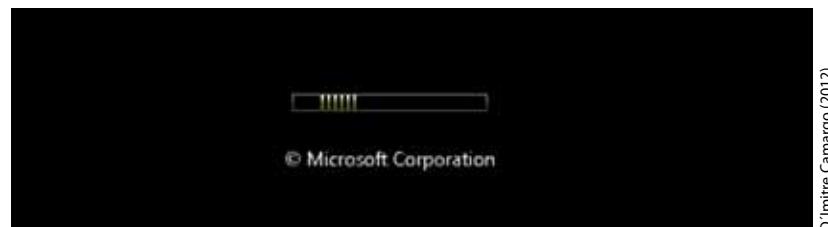


Figura 143 - Tela de reset

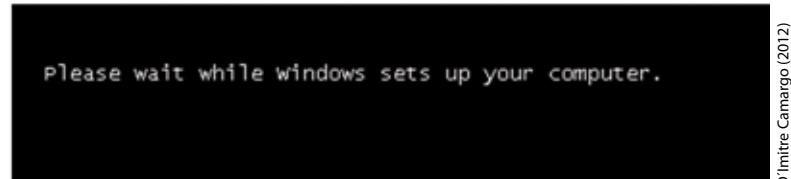


Figura 144 - Tela de retorno do Windows

O sistema retorna, completando a instalação.

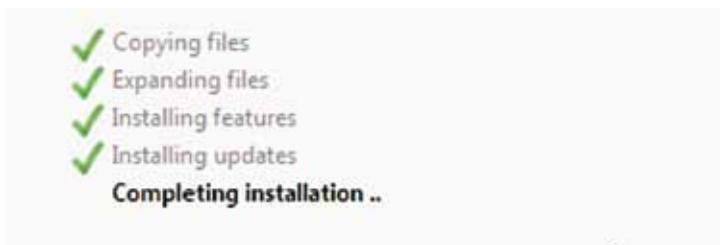


Figura 145 - Completando a instalação

Aguarde a finalização da instalação.

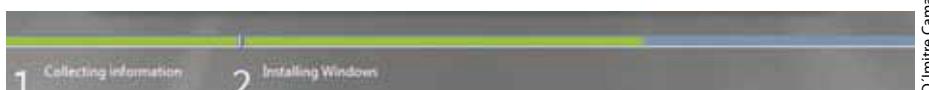


Figura 146 - Andamento da instalação

Passo 14

Após a finalização, o sistema será reiniciado novamente e surgirá uma tela semelhante a que você verá a seguir, informando que a senha do usuário administrador deverá ser trocada (em Inglês).



Figura 147 - Mensagem de senha

Passo 15

Na próxima tela será solicitada a criação de uma nova senha para o usuário administrator. Insira uma senha forte e repita. Em seguida, pressione SETA.



D'Imitře Camargo (2012)

Figura 148 - Criando a senha do administrator

Passo 16

Logo a seguir, você será notificado que a senha do usuário administrator foi alterada com sucesso. Pressione OK.

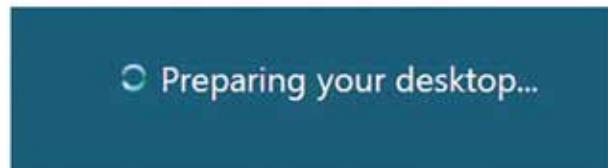


D'Imitře Camargo (2012)

Figura 149 - Confirmação de alteração de senha

Passo 17

Após o OK, o sistema irá configurar a Área de Trabalho para o administrator.



D'Imitře Camargo (2012)

Figura 150 - Preparando o desktop

Passo 18

Após estes procedimentos, o sistema operacional Windows está instalado e pronto para seu funcionamento. Até o momento este sistema não possui funcionalidade alguma de um servidor de rede. O Windows 2008 Server sempre inicializa com a tela de tarefas de configuração inicial aberta (*Initial Configuration Tasks*). É possível remover esta tela da inicialização selecionando a caixa “do not show this window at logon” e também carregar a tela SERVER MANAGER.

Por meio da guia ROLES que foram instalados todos os serviços disponíveis no Windows, como por exemplo: DHCP, DNS, Servidor WEB, dentre outros.



Figura 151 - Server manager

D'Imitre Camargo (2012)

Para promover este servidor para ser um servidor de domínio, que irá criar contas de usuário, grupos e contas de computadores, você deve executar o comando “DCPROMO”, o qual irá promovê-lo a um ACTIVE DIRECTORY.

Muitas das tarefas de gerenciamento do Windows 2008 estão na guia “administrative tools”.

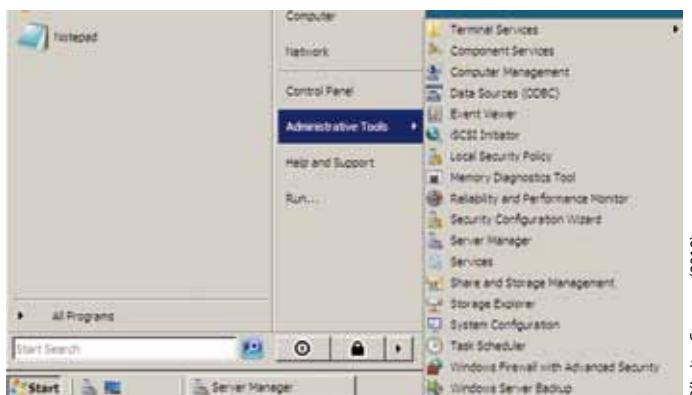


Figura 152 - Administrative Tools

D'Imitre Camargo (2012)

Instalar um sistema operacional é uma tarefa bastante simples, porém alguns cuidados deverão ser tomados no momento da escolha do disco ou partição na qual será instalado o sistema, pois a maioria de servidores possui mais de um disco rígido ou mais de uma partição. Para servidores novos, ou seja, que irão receber o sistema operacional pela primeira vez, estes cuidados podem ser desprezados.

Acompanhe o Casos e Relatos a seguir, pois exemplifica muito bem essa situação.



CASOS E RELATOS

Escolha do disco

Uma determinada empresa da grande Florianópolis estava realizando a troca de sistema operacional de seu servidor de arquivos. Este, por sua vez, possuía dois discos que não estavam espelhados, um para sistema e outro para dados.

No momento da instalação do sistema, o técnico escolheu o disco errado para a instalação, e este foi formatado para receber o novo sistema, removendo todos os dados da empresa. Problemas deste tipo acontecem com frequência, por isso, é sempre bom verificar qual disco possui o sistema instalado e se existe redundância de disco.



RECAPITULANDO

Neste capítulo você estudou o sistema operacional de rede e os diversos tipos existentes, bem como os requisitos necessários para uma atualização ou instalação de um sistema operacional. Pôde saber o que se trata de uma arquitetura aberta e sua instalação, aprendendo a configurar o BIOS para inicialização, através do CD-ROM. Além disso, conheceu uma arquitetura fechada e o passo a passo de sua instalação, bem como, promover um servidor Windows a servidor de domínio.

Anotações:

Trabalhando com Sistemas de Redundância, Virtuais e Lógicos

13



No último capítulo do seu livro didático, serão apresentados os fatos que darão início à virtualização de servidores. Você verá como funciona a virtualização e saberá quais os tipos existentes. Terá a oportunidade de conhecer também as formas de redundância de disco, os tipos de proteção dos dados e, para finalizar, veremos o que são volumes lógicos e como administrar os volumes.

Ao final deste capítulo, você terá subsídios para:

- a) virtualizar um servidor;
- b) compreender o que é uma máquina virtual;
- c) compreender os tipos de redundância de disco;
- d) criar e administrar um volume lógico.

Nessa última etapa do seu aprendizado, aproveite para fazer um apontamento dos conceitos que você considera mais relevantes. Faça um resumo desses assuntos e coloque em prática todas as etapas do passo a passo, pois desta forma, você estará reforçando todo o conteúdo adquirido neste material didático.

13.1 VIRTUALIZAÇÃO DE SISTEMAS OPERACIONAIS

Você já ouviu falar em virtualização? É uma técnica utilizada para instalar vários sistemas operacionais em apenas um equipamento. Um sistema virtualizado é aquele que possui as mesmas características de uma máquina física. Virtualizar sistemas operacionais vem se tornando uma prática muito comum nos setores de tecnologia da informação. O que na década de 60 era apenas uma especulação, hoje é uma realidade.

Conheça, a seguir, algumas das vantagens da virtualização:

- a) redução de custo;
- b) diminuição do espaço físico;
- c) consumo de energia (alimentação de servidores e refrigeração);
- d) recuperação de servidores em tempo reduzido;
- e) segurança para os dados e para o sistema operacional.

Agora, conheça algumas das desvantagens:

- a) quantidade de espaço no disco rígido;
- b) quantidade de memória.

13.1.1 A ORIGEM DA VIRTUALIZAÇÃO

A virtualização teve sua origem com a IBM, na década de 60, que na época avaliava o conceito de sistemas de compartilhamento de tempo ou TSS (*Time Sharing System*). Por parte da IBM havia a necessidade de realizar avaliações e testes no TSS que, por sua vez, necessitava de mais equipamentos para resultados mais precisos.

Na ocasião, os equipamentos *mainframe* tinham um custo muito alto, e foi por meio desta necessidade que a IBM teve a idéia de dividir um único equipamento em partes, onde cada parte desta divisão seria responsável por suas ações de gerenciamento.

O sistema TSS não obteve um resultado satisfatório, por ser sistema pesado e que consumia muitos recursos do equipamento. Diante disto, no início da década de 70, a IBM cria e desenvolve um novo sistema, chamado de CP/CMS, que mais tarde passou a ser chamado de VM/370. Mas foi a partir de 1998, após a fundação da empresa VMWARE, que esta tecnologia surgiu para o meio corporativo.

**FIQUE
ALERTA**

A manutenção dos servidores responsáveis pela camada de virtualização deve ser contínua, para evitar alguma perda de informação.

13.1.2 O FUNCIONAMENTO DA VIRTUALIZAÇÃO

Para que o processo de virtualização funcione, existe a necessidade de um *software* que proporcione a camada de virtualização, chamado de Hipervisor ou Monitor de Máquina Virtual (VMM). O hipervisor é a camada de *software* entre o *hardware* e o sistema operacional. No mercado, você irá encontrar dois tipos: por Software, os que são instalados sobre um Sistema Operacional, como VMware Server, Microsoft Virtual Server, Citrix XenServer e outros. E por *Hardware*, que possuem Kernel próprio, instalados diretamente no *hardware*, como alguns aplicativos do tipo VMware Server, Microsoft Virtual Server, Citrix XenServer e outros.

Conheça a seguir algumas funções do monitor de máquina virtual.

- a) Realizar a alteração de execução do SO convidado, de privilegiado para não privilegiado, e vice e versa.
- b) Simular e separar o uso da CPU para as máquinas virtuais.
- c) Administrar o uso de memória e discos disponibilizados para a máquina virtual.
- d) Intermediar as chamadas de sistema e controlar acesso a outros dispositivos.

**SAIBA
MAIS**

Ao acessar o site <<http://www.vmware.com/br/>>, você irá encontrar as mais diversas informações sobre virtualização total e paravirtualização, além de conhecer outros produtos para virtualização.

13.1.3 MÁQUINA VIRTUAL

No mundo da virtualização, o termo mais utilizado é 'máquina virtual' (*Virtual Machine* - VM), mas o que de fato isto significa? VM nada mais é que uma máquina criada por meio de *software*, ou seja, ela não existe fisicamente, mas possui todas as funcionalidades de uma máquina física: sistema operacional, aplicações, dis-

positivos como *drive* de disquete, CDROM e USB também estão presentes. O que existe é apenas um arquivo, que pode ser manipulado.

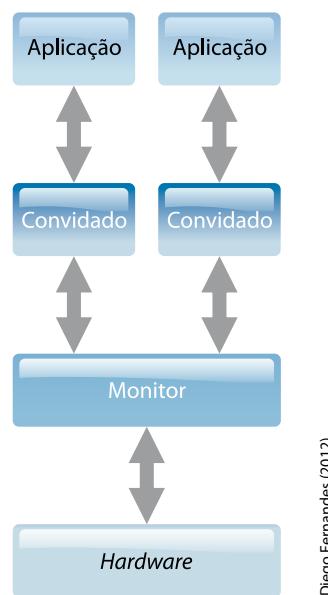
Quando você cria uma máquina virtual, estará possibilitando que vários sistemas operacionais trabalhem separadamente com o mesmo equipamento. Uma máquina virtual é igual a um equipamento físico: possui BIOS, processo de *boot* e dispositivos, mas todos esses dispositivos não existem fisicamente, são virtuais.

TIPOS DE MÁQUINAS VIRTUAIS

De acordo com Silva (2007), as máquinas virtuais estão divididas em dois grupos: a máquina virtual tipo 1 e a máquina virtual tipo 2. Conheça, a seguir, as características de cada uma delas.

MÁQUINA VIRTUAL TIPO 1

Neste tipo de sistema, o monitor é implementado entre o *hardware* e os sistemas convidados, também conhecidos de sistemas *guest* ou *guest systems*.



Diego Fernandes (2012)

Figura 153 - Máquinas Virtuais Tipo 1
Fonte: Adaptado de Silva (2007)

O monitor VMM possui controle sobre o *hardware* e monta um ambiente de máquinas virtuais, dando a cada máquina virtual um comportamento semelhante a uma máquina física, em que é possível executar sobre esses ambientes, sistemas diferentes e isolados.



**VOCÊ
SABIA?**

Que é possível gravar sua máquina virtual em um pen-drive e acessá-la em qualquer lugar, em qualquer computador? No entanto, este computador deverá possuir um *software* de virtualização.

MÁQUINAS VIRTUAIS TIPO 2

Neste sistema, o monitor é implementado como um processo de um sistema operacional real, denominado de "sistema anfitrião" (*host system*).

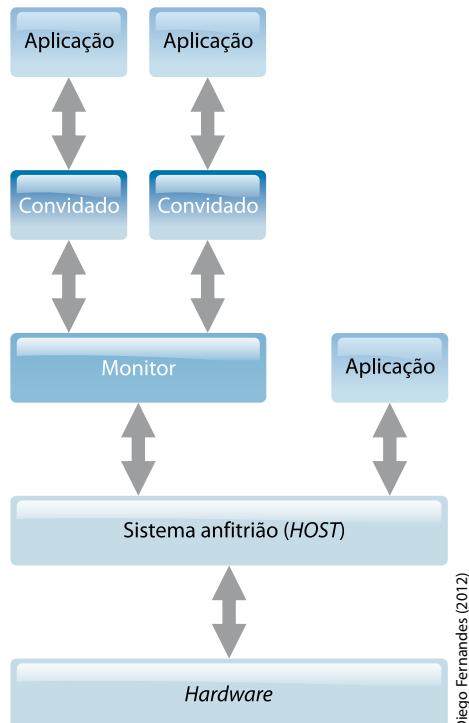


Figura 154 - Máquinas Virtuais do Tipo 2
Fonte: Adaptado de Silva (2007)

Nesse caso, o monitor VMM é executado sobre o sistema operacional anfitrião, como um processo, o monitor simula as operações que o sistema anfitrião controlaria.

13.1.4 TIPOS DE VIRTUALIZAÇÃO

São as maneiras de interpretação da camada virtual e o *hardware* do equipamento. Existem dois tipos de virtualização: a virtualização total e a paravirtualização. Conheça, a seguir, as características de cada tipo.

VIRTUALIZAÇÃO TOTAL

Neste tipo de virtualização, o monitor da máquina virtual fornece uma réplica virtual de toda a arquitetura necessária ao sistema operacional visitante. Dessa forma, o sistema visitante é executado sem modificações sobre o VMM, o que causa alguns inconvenientes, como a sobrecarga.

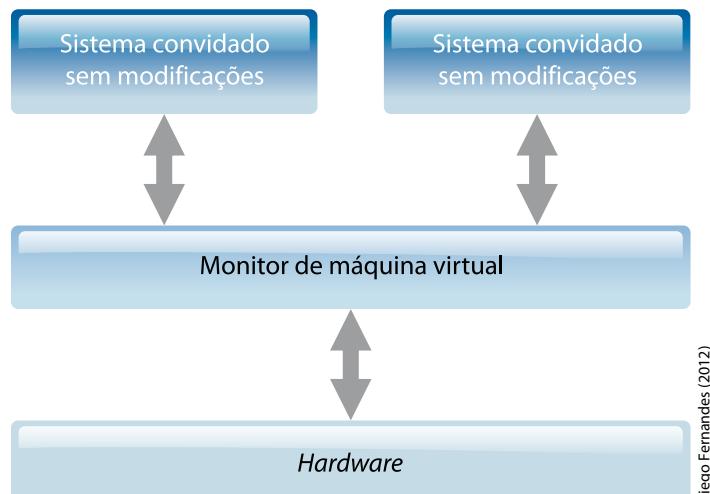


Figura 155 - Virtualização Total
Fonte: Adaptado de Silva (2007)

PARAVIRTUALIZAÇÃO

Neste modelo de virtualização, o sistema operacional é modificado para chamar o monitor da máquina virtual sempre que executar uma instrução que possa alterar o estado do sistema (uma instrução sensível). Essa função acaba com a necessidade de o VMM testar instrução por instrução, como acontece na virtualização total, o que representa um ganho significativo de desempenho. Outro ponto positivo da paravirtualização é que os dispositivos de *hardware* são acessados por *drives* da própria máquina virtual, não sendo necessário o uso de *drives* genéricos.

Embora a paravirtualização apresente um ganho de desempenho significativo frente à virtualização total, essa disparidade tem sido superada devido à presença

de instruções de virtualização nos processadores Intel e AMD, que favorecem a virtualização total.

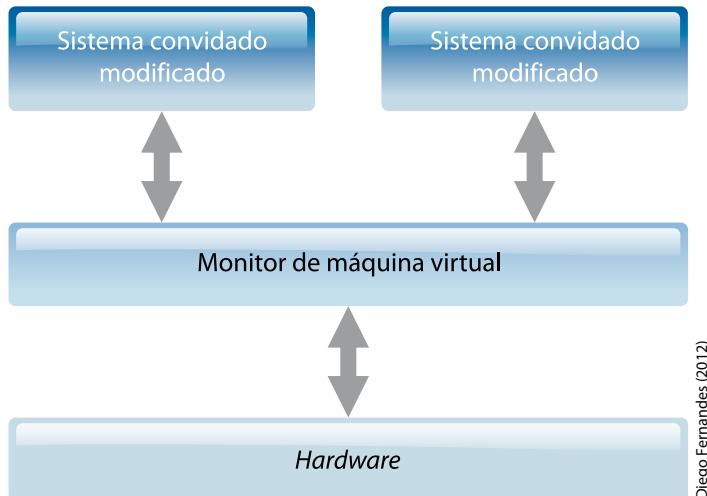


Figura 156 - Paravirtualização
Fonte: Adaptado de Silva (2007)

Diego Fernandes (2012)

13.2 RAID – REDUNDANT ARRAY OF INDEPENDENT DISKS

Este sistema é um arranjo redundante de discos independentes, o que faz este sistema ser rápido e confiável. O *RAID* funciona com dois conceitos. No primeiro conceito, ocorre a divisão dos dados (*data striping*), que aumenta o desempenho dos equipamentos. Neste conceito, os dados que estão sendo armazenados no disco são separados em diversos pedaços e armazenados em discos separados. Esse processo ocorre de forma simultânea.

Já no segundo conceito, ocorre o espelhamento dos discos. Toda a informação armazenada em um disco é automaticamente gravada num segundo disco, aumentando a segurança das informações. Em caso de falha no primeiro disco, o segundo (que é uma réplica do primeiro) entra em funcionamento para substituição do disco com falha.

O sistema *RAID* pode ser implementado de duas formas: por *software* - quando implementado por meio do sistema operacional, seja Linux ou Windows - ou por *hardware*, quando implementado por meio de placas controladoras *RAID*.

Em momentos de falhas de disco, é necessário ter muita atenção na hora da troca dos discos. Para entender melhor esta afirmação, acompanhe a situação seguinte.

¹ REDUNDÂNCIA

É a garantia de funcionamento de um sistema, mesmo ocorrendo uma falha.



CASOS E RELATOS

Espelho inverso

Um servidor com discos espelhados de uma empresa, e com cerca de 200Gb de informações armazenadas, certo dia falhou num determinado disco do servidor e a área de tecnologia da empresa foi acionada. Esta possuía um disco de mesmo tamanho em estoque, então foi feita a troca e a inicialização do espelhamento.

Passado o período do espelhamento, foi verificado que as informações não estavam atualizadas e foi constatado que o técnico havia usado um disco com informações de outro setor. O que aconteceu foi que o técnico realizou o espelho do disco de forma inversa, substituindo as informações. Portanto, é necessário ter bastante atenção. Use sempre discos formatados e não cometa o erro de inverter o espelho, pois o espelho faz cópia do disco vazio para o cheio.

13.2.1 NÍVEIS DE RAID

Os níveis de RAID são as formas de implementação do sistema de redundância de discos que estão divididas em cinco níveis, os quais serão apresentados a seguir.

RAID-LINEAR	Neste nível, ocorre o agrupamento dos discos, formando um grande disco virtual. Os pedaços do disco são postos em ordem sequencial e somente irão para o segundo disco quando o primeiro estiver cheio. Este nível não possui redundância ¹ . Se um disco falhar, o sistema será comprometido e sua confiabilidade será mínima.
RAID-0	Este nível também é conhecido como “striping”. Nele, os dados são mapeados para aumentar o desempenho. No momento em que os dados são armazenados no conjunto, são fatiados e escritos em paralelo nos discos. Não possui redundância e seu custo é baixo.

RAID-1	<p>Este nível também é conhecido por espelhamento. Pode ser utilizado com dois discos ou mais, desde que todos possuam o mesmo tamanho. Se ocorrer dos discos possuírem tamanhos diferentes, o RAID-1 deverá ser realizado do menor para o maior.</p> <p>Neste nível é realizada uma cópia fiel do primeiro para o segundo disco, mas se o disco possuir mais de uma partição, poderá ser realizado o espelho de apenas uma das partições importantes ou necessárias. Possui redundância e é bastante utilizado por sua praticidade.</p>	
RAID-4	<p>Este nível é pouco utilizado. É utilizado com três ou mais discos. Trata-se de um disco para armazenamento da paridade, como forma de proteção dos dados, enquanto os dados são salvos nos demais discos. Apesar de este nível utilizar um disco só para paridade, o tamanho total do armazenamento será calculado com a fórmula $(N-1)*S$, sendo N igual ao número de discos e S o tamanho do menor disco. Quando ocorre uma falha em apenas um disco, é utilizada a paridade para reconstrução dos dados, mas se a falha for nos dois discos, os dados serão perdidos.</p>	
RAID-5	<p>Este nível é semelhante ao RAID-4, mudando apenas a forma de armazenamento da paridade, que é distribuída em todo o conjunto dos discos. Este nível é bastante utilizado.</p>	

Quadro 21 - Níveis de RAID


**SAIBA
MAIS**

Quer saber mais sobre a redundância de disco, seus níveis e a comparação entre os níveis? Então acesse o site <<http://www.dimap.ufrn.br/~aguilar/Manuais/Servidor/raid-niveis.html>>, e você terá muitas informações sobre implementação e pré-requisitos para a instalação de redundância.

13.2.2 CRIAÇÃO DE ARRAY DE DISCOS

O sistema *RAID*, que será apresentado como exemplo, está baseado na ferramenta “mdadm” utilizada para criação de *RAID*. Existem outros pacotes, como o “raidtools” e “mkraaid” que também são utilizados para a criação de redundância de discos.

Este modelo de *array* de discos está baseado em partições lógicas já configuradas no sistema. Veja a seguir!

Instalação do pacote “mdadm”

```
# apt-get install mdadm
```

Comando para verificação de sincronização dos discos

```
# while [ 1 ]; do clear; cat /proc/mdstat > /dev/tty2; sleep 1; done;
```

Criar partições de mesmo tamanho com o comando “fdisk”, exemplo /dev/hda7 e /dev/hda8.

```
# fdisk /dev/hda
```

Criando o *array* de discos com as duas partições criadas

```
# mdadm --create --verbose /dev/md0 --level=1 --raid-devices=2 /dev/hda7 /dev/hda8
```

Passo 1

Após a execução do comando anterior, alterne a janela de terminal para “tty2” com alt+F2 e execute o comando de verificação de sincronização.

```
# while [ 1 ]; do clear; cat /proc/mdstat > /dev/tty2; sleep 1; done;
```

Caso no sistema não existam os dispositivos de *array* em /dev, ou seja, os dispositivos md0, md1,..md15, então estes deverão ser criados manualmente, conforme segue:

- copiar o MAKDEV do diretório /dev para o diretório /tmp: # cp /dev/MAK-**DEV** /tmp;
- executar o comando: /tmp/MAK**DEV** md;
- recortar os arquivos md* localizados no /tmp para o diretório /dev: # mv /tmp/ma* /dev.

Passo 2

Dispositivos de *array* criados. É hora de editar o arquivo de configuração do RAID mdadm.

```
# nano /etc/mdadm/mdadm.conf
DEVICE /dev/hda7      dev/hda8
ARRAY  /dev/md0      devices=/dev/hda7, /dev/hda8
Criar o sistema de arquivo EXT3 no dispositivo /dev/md0
# mkfs -j /dev/md0
```

Criar um novo ponto de montagem em /mnt para o dispositivo **md0**

mkdir /mnt/array

Montar o dispositivo de *array* no ponto de montagem criado **/mnt/array**

mount -t ext3 /dev/md0 /mnt/array

Passo 3

Adicione a linha de comando abaixo, no arquivo /etc/fstab, para que o dispositivo de *array* seja montado automaticamente.

```
# nano /etc/fstab  
/dev/md0      /mnt/array      ext3      defaults0      2
```

Verificando os dispositivos:

mdadm -E /dev/hda7

mdadm -E /dev/hda8

Verificar detalhes dos dispositivos:

mdadm --detail --scan

mdadm --detail /dev/md0

Simulando falhas:

mdadm /dev/md0 --fail /dev/hda7

mdadm --detail /dev/md0

Removendo dispositivo com falha, exemplo /dev/hda7:

mdadm /dev/md0 --remove /dev/hda7

mdadm --detail /dev/md0

Voltando o dispositivo /dev/hda7 ou outro dispositivo:

mdadm /dev/md0 --add /dev/hda7

mdadm --detail /dev/md0

Parar o *array* de discos:

mdadm -S /dev/md0

Inicia o *array* de discos:

mdadm -As /dev/md0

O RAID pode ser implementado por *hardware*, na forma de controladores especiais de disco, ou por *software*, como módulo do kernel do Linux. (FERREIRA, 2003).

² KERNEL

É o coração ou núcleo de qualquer sistema operacional. É ele que interage entre as aplicações e os hardwares.

13.3 LVM – LOGICAL VOLUME MANAGER

É um gerenciador de disco que utiliza uma camada para gerenciamento de volumes lógicos adicionada entre a parte física do equipamento e a interface I/O no kernel⁵ do Linux, para a junção de vários discos, permitindo uma visão lógica dos discos. As partições lógicas criadas sobre o LVM podem ter seu espaço aumentado ou diminuído quando este não tiver mais espaço. A qualquer momento você pode adicionar novos discos ao volume, seja por falta de espaço ou simplesmente para ter mais espaço, isso tudo sem a necessidade de migrar informações do disco cheio para o novo, bastando apenas o redimensionamento das partições novas.

As camadas de gerenciamento de disco estão divididas em *physical volumes*, *physical extensions* e *volume group*. Conheça cada camada a seguir.

Physical volumes (PV):

Ou volumes físicos, são os discos agrupados em forma de *RAID*.

Physical extensions (PE):

Ou extensões físicas, são as divisões dos volumes físicos.

Volume group (vg):

Ou grupo de volumes, é a união de vários volumes físicos.

13.3.1 LOGICAL VOLUMES (LV)

Ou volumes lógicos são as divisões dos volumes físicos, ou seja, são as chamadas partições que podem ser formatadas e montadas. As extensões físicas são as acessadas pelo usuário.

Na criação de LVM não é permitido utilizar as partições "/" e "/boot", pois o LVM, para montar os volumes lógicos, necessita de módulos do kernel, e nestas duas partições o kernel não estaria acessível.

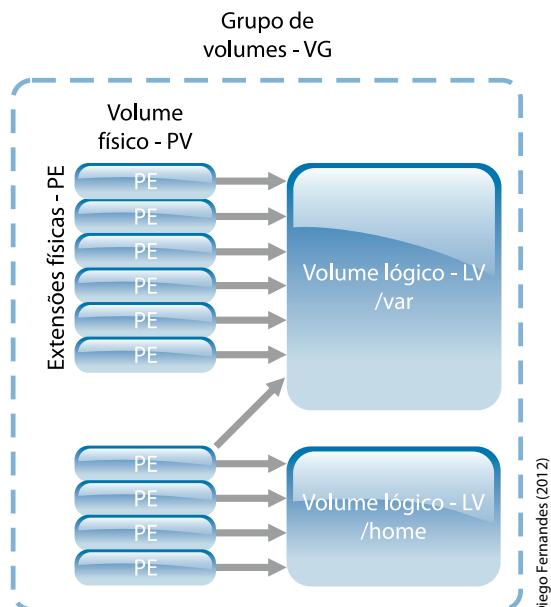


Figura 157 - Grupo de Volumes
Fonte: Adaptado do autor

Diego Fernandes (2012)

13.3.2 GERENCIANDO OS VOLUMES LÓGICOS

Por meio do gerenciamento, é possível criar, remover, alterar e realizar outras tantas configurações que se fazem necessárias para a administração dos volumes lógicos. Serão detalhados os comandos mais utilizados. Veja a seguir!

CRIANDO VOLUME FÍSICO

Os comandos e opções a seguir são os mais utilizados para gerenciamento de volumes físicos. Para todos os comandos mencionados, utilizando a opção “-h”, dará suporte ao comando.

Esses comandos são:

Pvcreate

Utilizado para criar volume físico.

Uso:

```
# pvcreate <opções> <partição>
```

Opções:

- f Força a criação.

Exemplo: #pvcreate -f /dev/sda5

Pvdisplay

Utilizado para visualizar configuração dos volumes criados.

Uso:

```
# pvdisplay <opções> <partição>
```

Opções:

-v Exibe mapeamento das extensões físicas e lógicas e volumes lógicos.

Exemplo: # pvdisplay /dev/sda5

Pvscan

Utilizado para procurar volumes físicos.

Uso:

```
# pvscan <opções>
```

Opções:

-v exibe as informações dos volumes e atividade do pvscan.

Exemplo: # pvscan -v

CRIANDO GRUPOS DE VOLUME

Os comandos e opções a seguir são os mais utilizados para gerenciamento dos grupos de volumes. Para todos os comandos mencionados, utilizando a opção “-h”, dará suporte ao comando.

Esses comandos são:

Vgcreate

Utilizado para criar grupo de volume.

Uso:

```
# vgcreate <opções> <grupo de volume> <partição>
<partição>
```

Opções:

- A <y/n> autobackup sim ou não;
- v informações do vgcreate.

Exemplo: # vgcreate -A y senai /dev/sda5 /dev/sda6

Vgremove

Utilizado para remover grupo de volume.

Uso:

vgremove <opções> <grupo de volume>

Opções:

- v informações do vgremove.

Exemplo: # vgremove senai

Vgextend

Utilizado para expandir o grupo de volumes.

Uso:

vgextend <opções> <grupo de volume> <partição>
<partição>

Opções:

- A <y/n> autobackup sim ou não;
- v informações do vgextend.

Exemplo: # vgextend senai /dev/sda5 /dev/sda6

Vgreduce

Utilizado para diminuir o tamanho do grupo de volume.

Uso:

vgreduce <opções> <grupo de volume> <partição>

Opções:

- A <y/n> autobackup sim ou não;

-v informações do vgreduce.

Exemplo: # vgreduce -A y senai /dev/sda5 /dev/sda6

Vgchange

Utilizado para alterar funções do grupo de volume.

Uso:

vgchange <opções> <grupo de volume>

Opções:

-a <y/n> ativa grupo, sim ou não;

-A <y/n> autobackup, sim ou não;

-v informações do vgchange.

Exemplo: # vgchange -a y senai

Vgrenname

Utilizado para alterar o nome de volume antigo.

Uso:

vgrename <opções> <localização volume antigo>
<localização volume novo>

Opções:

-A <y/n> autobackup sim ou não;

-v informações do vgrename.

Exemplo: # vgrename -A y /dev/senai /dev/ctai

Vgdisplay

Utilizado para relatar informações do grupo de volume.

Uso:

#vgdisplay <opções> <grupo de volume>

Opções:

-v informações do vgdisplay.

Exemplo: # vgdisplay ctai

Vgscan

Utilizado para procurar grupos de volumes nos discos, criando os arquivos "/etc/lvmtab e /etc/lvmtab.d".

Uso:

vgscan <opções>

Opções:

-v informa atividades do vgscan.

Exemplo: # vgscan -v

CRIANDO VOLUMES LÓGICOS

Os comandos e opções a seguir são os mais utilizados para gerenciamento dos volumes lógicos. Para todos os comandos mencionados, utilizando a opção "-h" dará suporte ao comando.

Esses comando são:

lvcreate

Utilizado para criar volume lógico.

Uso:

lvcreate <opções> <opções> <volume lógico>

Opções:

-A <y/n> autobackup, sim ou não;

-v informações do lvcreate;

-L <tM> tamanho do volume a ser criado em <tamanhoMegabytes>;

-n adiciona nome para o volume.

Exemplo: # lvcreate -A y -L 1024M -n volsenai ctai

lvremove

Utilizado para remover volume lógico.

Uso:

```
# lvremove <opções> <localização volume lógico>
```

Opções:

- A <y/n> autobackup, sim ou não;
- v informações do lvremove;
- f remove forçado.

Exemplo: # lvremove -A y -f /dev/ctai/volsenai

lvextend

Utilizado para expandir o volume lógico.

Uso:

```
# lvextend <opções> <localização volume lógico>
```

Opções:

- A <y/n> autobackup, sim ou não;
- v informações do lvextend;
- L <+tM> tamanho do volume a ser criado em <tamanhoMegabytes>.

Exemplo: # lvextend -A y -L +1024M /dev/ctai/volsenai

lvreduce

Utilizado para diminuir o tamanho do volume lógico.

Uso:

```
# lvreduce <opções> <localização volume lógico>
```

Opções:

- A <y/n> autobackup, sim ou não;
- v informações do lvreduce;

-L <-tM> tamanho do volume a ser diminuído em <tamanhoMegabytes>.

Exemplo: # lvextend -A y -L 1024M /dev/ctai/volsenai

lvchange

Utilizado para alterar funções do volume lógico.

Uso:

```
# lvchange <opções> <localização volume lógico>
```

Opções:

- a <y/n> ativa volume lógico. sim ou não;
- A <y/n> autobackup, sim ou não;
- v informações do lvchange.

Exemplo: # vgchange -a y /dev/ctai/volsenai

lvrename

Utilizado para alterar nome de volume antigo.

Uso:

```
# lvrename <opções> <localização volume antigo> <localização volume novo>
```

Opções:

- A <y/n> autobackup, sim ou não;
- v informações do lvrename.

Exemplo: # lvrename -A y /dev/ctai/volsenai /dev/ctai/volsenai2

lvdisplay

Utilizado para relatar informações do volume lógico.

Uso:

```
# lvdisplay <opções> <localização volume lógico>
```

Opções:

-v informações de extensões lógicas em volumes físicos em extensões físicas.

Exemplo: # lvdisplay -v /dev/ctai/volsenai2

lvscan

Utilizado para procurar volumes lógicos.

Uso:

lvscan <opções>

Opções:

-v informa atividades do lvscan.

Exemplo: # lvscan -v

**RECAPITULANDO**

Neste último capítulo do livro, você aprendeu o que é virtualização e seus tipos, o que é máquina virtual, paravirtualização e virtualização total. Você pôde aprender também o que é uma redundância de disco e como realizar um *array* de discos no Linux. Por fim, conheceu um gerenciador de volume lógico, além de ter a oportunidade de aprender a criar e administrar um volume lógico, um volume físico e a procurar um volume existente no disco.

Anotações:

REFERÊNCIAS

- BUENO, Henrique. **Virtualização - Um Pouco de História.** 2009. Disponível em: <<http://hbueno.wordpress.com/2009/04/29/virtualizacao-um-pouco-de-historia/>>. Acesso em: 15 out. 2011.
- DICIONÁRIO BABYLON. **Barramento PCI.** Disponível em: <<http://dicionario.babylon.com/barramento%20pci/>>. Acesso em: 10 de out. 2011.
- FEBRABAN. **Em 2007 os bancos investiram R\$ 7,0 bilhões em segurança física.** Disponível em: <http://www.febraban.org.br/p5a_52gt34++5cv8_4466+ff145afbb52ffrtg33fe36455li5411pp+e/sitefebraban/2007%20bancos%20investiram.pdf>. Acesso em: 12 de fev. 2012.
- FERREIRA, Rubem E. **Linux:** Guia do Administrador do Sistema. São Paulo: Novatec, 2003. 510 p.
- MACHADO, Francis Berenger; MAIA, Luiz Paulo. **Arquitetura de sistemas operacionais.** 2. ed. Rio de Janeiro: LTC, 1997.
- MATOS, Diogo Menezes Ferrazani. **Virtualização total e paravirtualização.** 2008. Disponível em: <http://www.gta.ufrj.br/grad/08_1/virtual/Virtualizaototalepara-virtualizao.html>. Acesso em: 12 de out. 2011.
- OLIVEIRA, Rômulo Silva; CARISSIMI, Alexandre da Silva; TOSCANI, Simão Sirineo. **Sistemas Operacionais.** Porto Alegre: Sagra-Luzzato, 2001.
- PRITCHARD, Steven. **Certificação Linux LPI – Nível 1: Exames 101 e 102.** 2. ed. rev. Rio de Janeiro: Alta Books, 2007. 486 p.
- RED HAT ENTERPRISE LINUX 3. **Guia de Administração do Sistema.** 2003. Disponível em: <http://web.mit.edu/rhel-doc/3/rhel-sag-pt_br-3/s1-raid-levels.html>. Acesso em: 12 out. 2011.
- RIBEIRO, Uirá. **Certificação Linux.** 2. ed. rev. aum. Belo Horizonte: DK Editora, 2009. 517 p.
- RODRIGUES, Thiago Costa. **Introdução ao VMWare (virtualização).** 2006. Disponível em: <http://www.oficinadanet.com.br/artigo/95/introducao_ao_vmware_virtualizacao>. Acesso em: 10 out. 2011.
- SANTOS, Fábio da Silva. **GNU/Linux Módulo 1 – Introdução,** Diretoria de Transferência Tecnológica, Centro de Computação – UNICAMP. São Paulo: UNICAMP, [20—]
- SAVIS. **Datacenters - Powering Complex Managed Hosting and IT Infrastructure Solutions.** Disponível em: <<http://datacentergallery.savvis.net/>>. Acesso em: 10 de dez. 2011.
- SILVA, Rodrigo Ferreira da. **Virtualização de Sistemas Operacionais.** 2007. Disponível em: <<http://www.lncc.br/~borges/doc/Virtualizacao%20de%20Sistemas%20Operacionais.TCC.pdf>>. Acesso em: 12 de out. 2011.
- STALLINGS, Willian. **Arquitetura e Organização de Computadores.** 8. ed. São Paulo: Pearson Editora, 2010.
- TANENBAUM, Andrew S. **Sistemas Operacionais Modernos.** 3. ed. São Paulo: Pearson Editora, 2010.

TIBET, Chuck V. **Linux Administração e Suporte**. São Paulo: Novatec, 2001. 379 p.

TRADE INFORMÁTICA. **Leitor Biométrico da Geometria da Mão para Controle de Acesso**.

Disponível em: <<http://www.trade.com.br/site/produtos/produtos.asp?Produto=130&Categoria=2&SubCategoria=2>>. Acesso em: 12 de fev. 2012.

TORVALDS, Linus et al. **Linux kernel v. 2.6.28.8**: include/linux/ext2_fs.h. The Linux Kernel Archives. 2009. Disponível em: <<http://www.kernel.org/pub/linux/kernel/v2.6/>>. Acesso em 12 de fev. 2012.

WIKIPÉDIA. **Barramento PCI**. Disponível em: <http://pt.wikipedia.org/wiki/Barramento_pci>.

Acesso em: 10 de fev. 2012.

MINICURRÍCULO DOS AUTORES

Luiz Antonio Silva de Paula é licenciado em Física pela Universidade Federal de Santa Catarina (2001), com Especialização em Desenvolvimento de *Software* para a WEB pela Univali (2004). Possui experiência na área de Ciência da Computação, com ênfase em Software Básico, nos sistemas operacionais GNU/Linux Debian e Windows 200x, XP e OpenSolaris, tendo trabalhado na área de Redes de computadores (LAN e WAN), gerência de redes e configuração de roteadores e *switchs* CISCO. Atua na prospecção e desenvolvimento de solução em *software* livre para integração de ambientes proprietários com os projetos Open Ldap e Samba, tendo também ministrado treinamento interno em Administração GNU/Linux e outros treinamentos em rede, Internet e *hardware* de computadores. Atuou como professor, ministrando a disciplina "Tecnologias da Informação" no Instituto de Ensino Superior da Grande Florianópolis - IES-FASC, nos cursos de Administração e Contabilidade.

Atualmente, é analista Sênior de TI da Caixa Econômica Federal, atuando no segmento de desenvolvimento descentralizado de *software*, nas disciplinas de Gerência de Requisitos, Gerência de Configuração, Ambiente, Arquitetura e outras atividades do processo de desenvolvimento. Também é professor do SENAI/SC, nas disciplinas de Administração de Sistemas Operacionais, Programação de *Scripts*, Sistemas Operacionais e Segurança da Informação.

Mauro César Matias é tecnólogo em Redes de Computadores (2007), pela Faculdade Estácio de Sá. Possui especialização em Redes Corporativas, Gerência de Segurança e Convergência pela Unisul (2009), Certificado CCNA - *Cisco Certified Network Associate* pelo Senai/CTAI, em (2003) e Certificado FCP - *Furukawa Certified Professional*, pelo Senac/SC, em (2006). Também possui experiência na área de Tecnologia em Redes, com ênfase em *Software* de redes para servidores com sistemas operacionais GNU/Linux Debian e Windows 200x e XP. Trabalha na área de administração dos servidores bancários/escritório com sistemas operacionais Windows Server 2003 e servidores *asterisk*, com sistemas operacionais GNU/Linux Debian da Caixa Econômica Federal.

Atua no desenvolvimento de *scripts*, tendo ministrado treinamento interno em Administração Windows Server 2003, XP, Sistemas Caixa Econômica Federal. Atualmente, é analista de Suporte de TI da Caixa Econômica Federal, atuando no segmento de administração de servidores e *scripts*.

Também é professor do curso superior de redes de computadores no SENAI/Florianopolis, nas disciplinas de Cabeamento Estruturado e Novas Tecnologias, e professor do curso Técnico em Manutenção de Computadores do SENAI/São José, nas disciplinas de Sistemas Operacionais II e Infraestrutura da Internet.

Possui a certificação GIAC Computer and Network Security Awareness - Stay Sharp Program do SANS Institute.

ÍNDICE

B

Barramento PCI 22, 260
Bios 6, 86, 87, 196, 197, 198, 199, 234, 240

C

Clock 21, 22, 59

D

Dispositivo 6, 38, 45, 48, 49, 50, 51, 52, 55, 62, 67, 68, 69, 72, 73, 86, 96, 109, 110, 114, 115, 121, 122, 123, 124, 127, 133, 134, 135, 138, 139, 141, 142, 144, 145, 148, 150, 152, 153, 154, 155, 156, 157, 158, 175, 183, 184, 186, 187, 188, 189, 198, 203, 239, 240, 242, 246, 247
DNS 7, 196, 204, 206, 225, 233
Domain Name 206, 207

F

FastEthernet 36, 37, 38

G

Gateway 7, 196, 204, 205, 206, 225
GigaBitEthernet 36, 37, 38
Grub 7, 8, 222, 223

H

Hot-Swap 144

J

Journaling 142, 143, 144, 182, 215

K

Kernel 122, 124, 126, 128, 152, 182, 239, 248, 260

M

Máscara de Rede 7, 196, 204, 205, 225

P

Período de Graça 188, 189

Ponto de Montagem 7, 154, 156, 211, 215, 216, 217, 247

S

SAS 38, 39, 49, 52

SATA 38, 39, 49, 51, 141, 144, 145, 146, 149

SCSI 38, 39, 52, 141, 144, 145, 146, 212

Service Pack 194

Smartphone 20, 33, 40, 58

T

Tablets 20, 23

SENAI - DN
UNIDADE DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA – UNIEP

Rolando Vargas Vallejos
Gerente Executivo

Felipe Esteves Morgado
Gerente Executivo Adjunto

Diana Neri
Coordenação Geral do Desenvolvimento dos Livros

SENAI - DEPARTAMENTO REGIONAL DE SANTA CATARINA

Simone Moraes Raszl
Coordenação do Desenvolvimento dos Livros no Departamento Regional

Beth Schirmer
Coordenação do Núcleo de Desenvolvimento

Caroline Batista Nunes Silva
Juliano Anderson Pacheco
Coordenação do Projeto

Gisele Umbelino
Coordenação de Desenvolvimento de Recursos Didáticos

Luiz Antonio Silva de Paula
Mauro Cesar Matias
Elaboração

Juliano Anderson Pacheco
Revisão Técnica

Adriana Ferreira dos Santos
Design Educacional

D'imitre Camargo Martins
Diego Fernandes
Julia Pelachini Farias
Luiz Eduardo Meneghel
Ilustrações, Tratamento de Imagens

Felipe da Silva Machado
Diagramação

Juliana Vieira de Lima
Revisão e Fechamento de Arquivos

Luciana Effting Takiuchi - CRB-14/937
Bibliotecária - Ficha Catalográfica

DNA Tecnologia Ltda.
Sidiane Kayser dos Santos Schwinzer
Revisão Ortográfica e Gramatical

DNA Tecnologia Ltda.
Sidiane Kayser dos Santos Schwinzer
Normalização

i-Comunicação
Projeto Gráfico

SENAI

*Iniciativa da CNI - Confederação
Nacional da Indústria*

ISBN 978-85-7519-484-3



9 788575 194843 >