

O PODER DOS
SERVIDORES
EM SUAS MÃOS

**D
S
B
Free**

Denis Augusto A. de Souza

Sumário

Agradecimentos	15
Sobre o autor.....	17
Prefácio.....	18
Como usar este livro.....	19
Capítulo 1 ■ Instalação	25
1.1 Introdução	25
1.2 Por que usar FreeBSD?	26
1.2.1 FreeBSD e outros sistemas operacionais	27
1.3 Check-list de pré-instalação.....	29
1.4 Escolhendo onde instalar o FreeBSD	32
1.5 Como o FreeBSD nomeia as partições	33
1.6 O processo de instalação	34
1.6.1 Instalação com disquetes	35
1.6.2 Planejamento da instalação	35
1.7 Introdução ao utilitário sysinstall	46
Capítulo 2 ■ Manuseio do sistema operacional.....	48
2.1 Visão geral.....	48
2.2 Sistemas Unix.....	49
2.2.1 Trabalhando com consoles	49
2.2.2 Explorando os comandos	51
2.2.3 Sticky bit (t-bit)	52
2.2.4 S bit aplicado ao proprietário de um arquivo	53
2.2.5 Trabalhando com permissões.....	54
2.2.6 Outros comandos	56
2.3 Estrutura de diretórios.....	61
2.4 Uso do ambiente shell	63
2.5 Gerenciamento de grupos e usuários	65
2.6 Agendamento de tarefas	69
2.7 Gerenciamento de processos.....	71
2.8 Uso do editor de textos Vi.....	72
2.9 Configuração de gateways e interfaces de rede.....	74
2.10 Uso de mídias removíveis	76
2.11 Uso de flags no FreeBSD	78
2.12 Gerenciador de boot do FreeBSD	79

2.13	Uso de sistemas de arquivo snapshot	80
2.14	Uso de sistemas union	81
2.15	Dicas importantes.....	82
Capítulo 3	▪ Instalação de aplicativos.....	84
3.1	Introdução	84
3.2	O que são ports?	84
3.3	O que são packages?	89
3.4	Notas gerais.....	91
Capítulo 4	▪ Ambiente X	95
4.1	Introdução	95
4.2	Entendendo o ambiente X.....	96
4.3	Gerenciador de janelas	98
4.4	Entendendo o ambiente X.....	100
4.4.1	X.Org e XFree86	101
4.4.2	Instalação do ambiente X.....	101
4.4.3	Configuração de um ambiente X.....	102
4.4.4	Gerenciadores de janelas	102
4.5	Considerações finais	104
Capítulo 5	▪ Gerenciamento e personalização.....	105
5.1	Introdução	105
5.2	Conhecendo o processo de boot do FreeBSD.....	105
5.2.1	Gerenciador de boot.....	106
5.2.2	Os primeiros dois estágios	107
5.2.3	Estágio 3	108
5.3	Otimização e gerenciamento do inetd	109
5.4	Ferramentas de gerenciamento.....	111
5.4.1	Ferramentas indicadas.....	112
5.5	Aplicação de patches	115
5.6	Compatibilidade entre FreeBSD e Linux.....	117
5.6.1	Instalação	117
5.7	Compilação do kernel do sistema operacional	122
5.7.1	Forma tradicional de compilação	126
5.7.2	Construção do kernel de um “modo novo”	126
5.7.3	Arquivo de configuração	127
5.8	Uso de quotas no sistema de arquivos	127
5.9	Ajustes para o aumento do desempenho (tuning)	129
5.9.1	Tuning de discos rígidos	130
5.9.2	Tuning kernels	133
5.9.3	Delay para controle de largura de banda	136
5.9.4	Tuning do acesso a rede.....	137
5.9.5	Adição de áreas de swap	138

Capítulo 6 ■ Segurança com FreeBSD.....	140
6.1 Visão geral.....	140
6.2 Comparações entre FreeBSD e o OpenBSD	141
6.3 Configuração do ACLs no FreeBSD.....	142
6.3.1 Uso de ACLs	143
6.4 Auditoria em ports	145
6.5 Filtro de pacotes PF	147
6.5.1 Configuração	149
6.5.2 Listas, macros e tabelas.....	149
6.5.3 Filtros de pacotes	152
6.6 Network Address Translation (NAT)	156
6.6.1 Como o NAT funciona?.....	156
6.6.2 Configuração do NAT.....	157
6.6.3 BiNAT – Mapeamento bidirecional (1 X 1)	158
6.6.4 NAT com exceções	158
6.6.5 Redirecionamento de pacotes	158
6.6.6 Balanceamento de cargas.....	159
6.6.7 Trabalhando com âncoras (Anchor).....	160
6.6.8 Verificação do status das conexões.....	162
6.6.9 Priorização de tráfego e controle de banda	162
6.6.10 Roteamento de pacotes	165
6.6.11 Logs	165
6.7 Sistema de auditoria.....	167
6.8 Trabalhando com criptografia.....	170
6.8.1 Aplicação de criptografia em partições do disco.....	172
6.8.2 Aplicação de criptografia na área de swap.....	178
6.9 Uso de VLANs.....	179
6.10 Uso de syslogd.....	182
6.11 Uso de Newsyslog	186
6.12 Hardening	188
6.12.1 Uso de flags	189
6.12.2 Remoção de banners	191
6.12.3 Remoção de programas desnecessários.....	192
6.12.4 Acessos a ambientes shell controlados	192
6.12.5 Opções de montagem	192
6.12.6 Personalização de aplicativos	193
6.12.7 Sincronismo de horas	194
6.12.8 Alteração de variáveis do kernel	194
6.13 Ambiente em chroot com jail.....	194
6.13.1 Uso de ambientes Chroot	195
6.13.2 Uso de ambientes Jail	196
6.13.3 Instalação de programas no ambiente Jail ou Chroot	200
6.13.4 Limitações, cuidados e dicas gerais.....	200
6.14 Sistema de verificações do FreeBSD.....	202

6.15	Uso de Kerberos V.....	204
6.15.1	Configuração de sshd com Kerberos	210
6.16	Uso de sudo	211
6.17	Uso de ssh	212
6.18	Destaques para a norma ISO/IEC 27002	213
6.19	Dicas diversas	214
Capítulo 7	▪ Construção de servidores	216
7.1	Visão geral	216
7.2	Visão geral do TCP/IP	216
7.3	Servidor de base de dados.....	220
7.4	Servidor web	223
7.5	Servidor de nomes (DNS)	227
7.6	Servidor de correio eletrônico (E-Mail)	229
7.7	Servidor DHCP	231
7.8	Servidor de impressão	233
7.9	Servidor de Storage iSCSI.....	235
7.10	Servidor para VPN IPSec	245
7.10.1	Uso de ipsec-tools	247
7.11	Servidor LDAP	253
7.12	Servidor de web cache	255
7.12.1	União do servidor Web Cache com Microsoft Active Directory	256
7.13	Outros servidores.....	262
Capítulo 8	▪ Troubleshooting	263
8.1	Visão geral.....	263
8.2	Ambientes wireless.....	264
8.3	Boot e compilação de kernel.....	264
8.4	Problemas com a comunicação de rede	266
8.5	Problemas com a instalação/configuração de aplicativos.....	267
8.5.1	Servidor de e-mail Sendmail	267
8.5.2	Servidor DNS	268
8.5.3	Servidor FTP	269
8.5.4	Impressoras	270
8.5.5	Compilação de ports	271
8.5.6	Problemas com sistema de arquivos (File System)	272
8.5.7	Esqueceu a senha do usuário root?	274
8.5.8	Análise de carga.....	274
8.5.9	Problemas gerais.....	279
Capítulo 9	▪ Alta disponibilidade com FreeBSD	283
9.1	Visão geral	283
9.2	Sistemas de arquivos	285
9.3	Desvendando sistemas RAID	286
9.3.1	RAID 0 (Striped Disk Arrays)	286

93.2 RAID 1 (Espelhamento)	287
93.3 RAID 3.....	287
93.4 RAID 0+1.....	288
93.5 RAID 5.....	288
93.6 RAID 6.....	289
93.7 RAID 1+0.....	290
94 Uso de RAID no FreeBSD	290
94.1 RAID 0	291
94.2 RAID 1.....	295
94.3 RAID 3.....	302
94.4 União de sistemas RAID (RAID 0+1)	305
94.5 Concatenação de discos	307
95 Uso de CARP.....	310
95.1 Funcionamento do CARP	311
95.2 Configuração do CARP.....	311
96 Heartbeat.....	318
96.1 Conclusão.....	325
97 Compartilhamento de um disco pela rede com GEOM gate	326
97.1 Cuidados	330
98 Rsync	330
99 Uso do sistema de arquivos ZFS.....	332
99.1 Uso do RAID 1.....	345
99.2 Uso de RAID-Z.....	348
99.3 Uso de áreas de swap.....	353
99.4 Uso de iSCSI	354
99.5 Conclusão	354
9.10 Uso de journaling no FreeBSD.....	355
9.11 Uso do Monit.....	357
9.12 Outras possibilidades.....	357
Capítulo 10 • Virtualização	359
10.1 Visão geral	359
10.2 Virtualização na resolução de catástrofes	362
10.2.1 Análise da segurança	363
10.3 Uso do VirtualBox.....	365
10.3.1 Pontos positivos.....	367
10.3.2 Pontos negativos.....	368
10.3.3 Reconhecimento da virtualização	368
10.3.4 Trabalhando com a versão OSE.....	369
10.4 QEMU	370
10.4.1 FreeBSD como host	370
10.4.2 FreeBSD como guest.....	373
10.4.3 Algumas observações importantes	374
10.4.4 Desempenho.....	375

10.4.5 Pontos positivos	375
10.4.6 Pontos negativos.....	377
10.4.7 Reconhecimento da virtualização	377
10.5 Uso do Virtual Server.....	378
10.5.1 Pontos positivos.....	383
10.5.2 Pontos negativos.....	384
10.5.3 Reconhecimento da virtualização	384
10.5.4 Notas a respeito do Virtual PC.....	385
10.6 Uso do VMware.....	385
10.6.1 Estudo do VMware Workstation.....	386
10.6.2 Estudando o VMware Server	395
10.6.3 VMware no port do FreeBSD	401
10.7 Uso do GXemul.....	403
10.7.1 Instalação de uma imagem NetBSD para DECstation 5000/200.....	404
10.7.2 Debian Linux para DECstation.....	406
10.7.3 Pontos positivos.....	408
10.7.4 Pontos negativos	409
10.7.5 Reconhecimento da virtualização.....	409
10.8 Uso do Xen	409
10.8.1 Instalação do Xen	410
10.8.2 Instalação de um sistema FreeBSD Guest	413
10.8.3 Pontos positivos	417
10.8.4 Pontos negativos.....	417
10.8.5 Reconhecendo a virtualização	417
10.9 Outros ambientes	418
Capítulo 11 ■ Pentest usando FreeBSD	419
11.1 Visão geral.....	419
11.2 Tipos de penetration testing	420
11.3 Principais frameworks disponíveis	421
11.3.1 OSSTMM	421
11.3.2 ISSAF	422
11.4 Ferramentas para enumeração	423
11.4.1 DNSenum	423
11.4.2 NBTscan	424
11.4.3 Nbaudit	425
11.5 Fingerprint	426
11.6 Varreduras	429
11.6.1 Uso de conexões TCP	431
11.6.2 Uso de conexões SYN	432
11.6.3 Uso de conexões FIN	432
11.6.4 Uso de conexões ACK (ACK scan)	434
11.6.5 Uso de conexões ICMP (ping scan)	435
11.6.6 Uso de conexões UDP	435
11.6.7 Uso de conexões RPC	436

11.6.8 TCP/IP Fingerprint	436
11.6.9 OS Fingerprint	437
11.7 Análise de vulnerabilidades remotas	438
11.8 Captura de dados	440
11.8.1 TCPFlow	441
11.8.2 Ettercap	443
11.9 Exploits	448
11.10 Framework Metasploit	449
11.11 Quebra de senhas.....	458
11.11.1 John the Ripper.....	458
11.12 Considerações finais	461
Capítulo 12 ▪ Estratégias para backup	462
12.1 Visão geral	462
12.2 Backup	462
12.3 Por que e como usar backups	465
12.4 Efetuando backups com o Bacula	466
12.4.1 Arquivos de configuração.....	468
12.4.2 Criação da base de dados	470
12.4.3 Deixando o sistema seguro	471
12.4.4 Iniciando as operações	471
12.4.5 Removendo os dados de teste das tabelas do Bacula	473
12.4.6 Verificando problemas com os jobs de backup	473
12.4.7 Teste do backup.....	474
12.4.8 Notas gerais o backup.....	482
12.5 Uso do rdiff-backup	483
12.5.1 Fazendo o backup local.....	484
12.5.2 Fazendo o backup remoto.....	484
12.5.3 Fazendo a restauração local	485
12.5.4 Restauração remota.....	486
12.5.5 Remoção de arquivos antigos.....	486
12.5.6 Trabalhando com exclusões e inclusões	487
12.5.7 Desvantagens	488
12.5.8 Criação de um script.....	488
12.6 Estratégias de backup com rsync.....	488
12.6.1 Backups locais.....	490
12.6.2 Backups remotos.....	490
12.7 Como efetuar o backup com o AMANDA.....	496
12.7.1 Configuração do servidor.....	498
12.7.2 Configuração do cliente.....	504
12.7.3 Teste do backup.....	505
12.7.4 Teste da restauração.....	506
12.8 Uso dos utilitários pax, restore e dump.....	508
12.9 Conclusão	513

Apêndice A ■ ITIL aplicado ao projeto de servidores Internet.....	514
A.1 ITIL no projeto de servidores.....	514
A.1.1 O que é ITIL?	514
A.1.2 Modelo de da ITIL	518
A.1.3 Gerenciamento de nível de serviço	520
A.1.4 Gerenciamento de disponibilidade.....	522
A.1.5 Gerenciamento de Capacidade.....	526
A.1.6 Gerenciamento de Continuidade	529
A.1.7 Dificuldades com a implementação da ITIL.....	531
A.1.8 Benefícios da ITIL aplicada ao projeto de servidores	532
Referências	533
Índice remissivo	537