Index

We have alphabetized files under their last components. And in most cases, *only* the last component is listed. For example, to find index entries relating to the **/etc/mail/aliases** file, look under **aliases**. Our friendly vendors have forced our hand by hiding standard files in new and inventive directories on each system.

Symbols

. directory entry 129
.. directory entry 129
#! ("shebang") syntax 133
1Password 994
389 Directory Server 580, 583–584
802.2* IEEE standards *see* IEEE standards

A

A DNS records 499, 519
AA (Access Agent) 597, 599
AAAA DNS records 519
acceptance tests 958
accept command 369
`accept_redirects` parameter 401, 425
`accept` router, Exim 653
`accept_source_route` parameter 425
Access Agent (AA) 597, 599
access control 65–68
access control lists *see* ACLs
`access_db` feature, **sendmail** 623
/etc/mail/access file 623
access points, wireless 471
accounts *see* user accounts
ACLs
- DNS 534, 552
- Exim 647–650
- filesystem 140–152

Active Directory *see* Microsoft Active Directory
addresses
- *see also* IP
- *see also* IPv6
- broadcast 386
- Ethernet (aka MAC) 384
- loopback 387
- multicast 386–387

adduser command 255, 262–263
/etc/adduser.conf file 262
Adleman, Leonard 1007
/var/adm directory 126
administrative privileges *see* root account
Adobe InDesign
- crash URL, frequently used 676
- experiences with 1175

AES (Advanced Encryption Standard) 1006
AFR (Annual Failure Rate) 723
AfriNIC 392
AgileBits 994
AIDE (Advanced Intrusion Detection Environment) 990, 1062, 1063
air conditioning *see* cooling
air plenums, wiring 463
AIX 11
Akamai Technologies 690
algorithms, cryptographic 1010
`alias_database` parameter, Postfix 663
/etc/mail/aliases file 609
aliases, email 608
- *see also* email
- *see also* Exim
- *see also* Postfix
- *see also* **sendmail**
- files, as alias source 610
- files, mailing to 611
- hashed database 612
- loops 609
- mailing lists 609
- postmaster 609
- programs, mailing to 611

`alias_maps` parameter, Postfix 663
Allman, Eric 302, 612
/var/cron/{**allow**,**deny**} file 113
Almquist shell 189
Alpine Linux 8
`always_add_domain` feature, **sendmail** 623
Amazon EC2 Container Registry 936
Amazon Linux 11

- Amazon Web Services *see* AWS
- AMD 902
- American Power Conversion (APC) 1096
- American Registry for Internet Numbers (ARIN) 479
- AMP 479
- Anixter 479
- Annual Failure Rate (AFR) 723
- Ansible 841, 843, 850, 852–871, 1109
  - access options, client 869–871
  - in AWS 859
  - comments on 850
  - comparison to Salt 893–895
  - and Docker 943
  - example 853
  - groups, client 857
  - groups, dynamic 859
  - iteration 862
  - and Jinja 863
  - passwords 870
  - playbooks 864–866
  - play elements 865
  - pros and cons 895
  - recommendations, configuration base 868
  - requirements, client 855–857
  - roles 866–868
  - securing client connections 870
  - security 894
  - setup 855–857
  - state parameters 862
  - tasks 860
  - templates 863–864
  - variables 858
- **ansible.cfg** file 853
- **ansible** command 852, 857
- **/etc/ansible** directory 853
- **ansible-galaxy** command 868
- **ansible-playbook** command 843, 852, 866
- **ansible-vault** command 852, 869
- Anvin, H. Peter 155
- anycast 386, 529
- **apache2.conf** file 698
- **/var/log/apache2/*** files 297
- Apache Cassandra 946
- **apachectl** command 697
- Apache Directory Studio 579
- Apache HTTP Server 684
- Apache Software Foundation 16, 684, 946
- Apache Spark 946
- Apache Traffic Server 689
- Apache Zookeeper 946
- APC (American Power Conversion) 1096
- apex zone, DNS 522
- APIs (Application Programming interfaces) 692–694
- APM (Application Performance Monitoring) 1059–1061
- APNIC 392
- AppArmor 87–89
- **/etc/apparmor.d** directory 88
- AppDynamics 1061
- `appendfile` transport, Exim 655
- application monitoring 1059–1061
- Application Programming Interfaces (APIs) 692–694
- Appropriate Use Policy (AUP) 1132
- **apropos** command 15
- APT (Advanced Package Tool) 166–174, 167, 169–170
- **apt-cache** command 170
- **apt** command 169–170
- **/var/log/apt*** file 297
- **apt-get** command 22, 170
- **apt-mirror** command 172
- Arch Linux 8
- ARIN (American Registry for Internet Numbers) 392, 479
- ARP (Address Resolution Protocol) 378, 401–402
- ARPANET 376
- **arp** command 402
- Artifactory 936
- as a service 323
- ASHRAE temperature range 1096
- **ash** shell 189
- Assmann, Claus 638
- AT&T 1168
- attack surface 987
- AT&T UNIX System V 1169
- **auditd** daemon 299
- auditing, user access 80
- **authconfig** command 247
- **/var/log/auth.log** file 297
- `AUTH_MECHANISMS` option, **sendmail** 628
- **~/.ssh/authorized_keys** file 1020
- **/etc/auto.direct** file 814
- autofs filesystem 813
- **/etc/auto_master** file 813
- **/etc/auto.master** file 813
- automation 1109
  - code promotion 1110
  - configuration management 1109
  - machine setup 1109
  - patching 1110
  - scripts 184–242
  - upgrades 1110
- automount
  - automatic mounts 817
  - direct maps 814
  - executable maps 815
  - indirect maps 814
  - on Linux 813, 817
  - master maps 815
  - replicated filesystems 816–817
  - visibility 816
- **automountd** daemon 813
- **automount** utility 813
- autonegotiation, Ethernet 467
- **/etc/auto.net** file 815
- autonomous system (AS) 488
- `autoreply` transport, Exim 655
- **autounmountd** daemon 813
- availability 983
- availability zones, cloud 278–279
- Avatier Identity Management Suite (AIMS) 268
- AWS 26, 273, 274–275, 905
  - and Ansible 859
  - booting alternate kernel 355
  - CDN 690
  - CloudFormation 282
  - CloudWatch 323
  - CodeDeploy 960
  - console log 286
  - EBS 281, 292
  - EC2 274, 284–287
  - EC2 Container Service 947, 979
  - Elastic Beanstalk 277
  - Elastic File System (EFS) 812
  - emergency mode 63
  - event-based computing 696
  - firewall 286
  - IAM 282
  - instance store 771
  - Lambda 283
  - load balancing 686
  - NACLs 450–451
  - and NFS 795, 812
  - PaaS 695
  - pricing 292
  - quick start 283

- AWS *continued*
  - RDS 281
  - Redshift 281
  - reserved instance 291
  - security groups 286, 450–451
  - shutting down systems 60
  - single-user mode 63
  - SQS 322
  - stopping instances 287
  - subnets 449–450
  - swap space 771
  - and Terraform 452–455
  - VPC 448–449
  - VPN 449–450
- **aws** CLI tool 284–287

B

- Backblaze 723
- backing store 1081
- backup, data
  - need for 788–790
  - plan 789–790
  - and security 989
  - strategy 788–790
- bad blocks, disk 735
- `BAD_RCPT_THROTTLE` feature, **sendmail** 631
- Bairavasundaram et al. 772
- Bamboo 1109
- Barracuda 606
- **.bash_profile** file 70, 183, 194, 258
- **.bashrc** file 70, 258
- **/etc/bashrc** file 255
- **bash** shell 7, 187, 189–198
  - *see also* **sh** shell
  - command editing 190
  - environment variables 193–194
  - pipes 190–192
  - quoting 192–193
  - redirection 190–192
  - search path 70
  - variables 192–193
- Basic Input/Output System (BIOS) 32 *see also* UEFI
- **bc** command 391
- BCP (Best Current Practice) 377
- BCPL (Basic Combined Programming Language) 1167
- beer, suggested minimum 1103
- Belden Cable 479
- Bell Labs 1166
- Berkeley *see* University of California at Berkeley
- Berkeley Fast File System 764
- Berkeley Internet Name Domain system *see* BIND
- Berkeley Software Design, Inc. (BSDI) 1171
- BGP (Border Gateway Protocol) 486, 490
- **bgpd** daemon 493
- bhyve 904, 910
- BIND 525–541
  - *see also* DNS
  - *see also* **named**
  - *see also* name servers
  - ACLs 552–553
  - AXFR zone transfer 548
  - chrooted environment 551, 554
  - components 525
  - configuration examples 543–547
  - debugging 568–576
  - **delv** command 566
  - DNSSEC 557–568
  - **dnssec-keygen** command 555, 561
  - **dnssec-signzone** command 562
  - **doc** command 576
  - **drill** command 568
  - example configuration 543
  - forwarding zone 539
  - forward-only server 531
  - IXFR zone transfer 548
  - **named.conf** file 526
  - **nsupdate** program 549
  - **rndc** command 533, 540–541, 549, 574
  - **/etc/rndc.conf** file 540
  - **rndc-confgen** command 540
  - **/etc/rndc.key** file 540
  - security features 552–568
  - TSIG/TKEY 554–556
  - zone signing 562
  - zone transfers 548
- **/bin** directory 125, 126
- **~/bin** directory 183
- **/usr/bin** directory 126
- `BIN_DIRECTORY` variable, Exim 641
- BIOS (Basic Input/Output System) 32
  - *see also* UEFI
- BitBucket 962
- Black Box Corporation 479
- `blacklist_recipients` feature, **sendmail** 630
- blacklists, **sendmail** 630
- block device files 128, 130–131, 329
- block size, disk 729–730
- block storage 281
- Blowfish hashing algorithm 248, 1006
- blue/green deployment 961
- **/boot** directory 39, 125, 126
- booting
  - initial processes 93
  - logging 297, 318
  - and NFS filesystems 810
  - PXE 155
- boot loader 33
  - GRUB 35–38
  - **loader** 39–41
  - password 986
- **/var/log/boot.log** file 297
- bootstrapping
  - drive selection 32
  - failures 59–60, 60–61
  - firmware 32
  - **fsck** and 62
  - process overview 30–31
  - single-user mode 35, 38, 41, 60, 61–63
  - startup scripts 57–59
  - tasks 30
- **/boot/bootx64.efi** bootstrap 39
- **/efi/boot/bootx64.efi** bootstrap 34
- Bostic, Keith 1171
- botnets 985
- Bourne-again shell *see* **bash**
- Bourne shell 187
- Bourne, Stephen 187, 1167
- break the glass 994
- broadcast
  - domain 461
  - packets 386, 461
  - ping 407, 423, 425
  - storm 413, 466
- Bro network intrusion detection system 1000
- Brouwer, Andries E. 745
- Bryant, Bill 1015
- BSDCan conference 20
- **bsdinstall** utility 161–164
- BSD UNIX 11, 1168–1169

- **btrfs** command 785
- Btrfs filesystem 742, 756, 772–773, 783–788
  - and Docker 930
  - setup 784–786
  - shallow copies 788
  - snapshots 786–787, 787–788
  - subvolumes 786–787
  - volumes 786–787
  - vs. ZFS 783–784
- BugTraq 1035
- Bugzilla 1114
- building wiring 475
- Burgess, Mark 841
- bus errors 95
- BUS signal 95

C

- cables
  - 10*base* 460
  - Category* 460, 462–464
  - coating 463
  - color-coding 464
  - Ethernet 460
  - fiber 464–465
  - wiring standard, UTP 464
- CA (Certificate Authority) 1007
- cache poisoning, DNS 530
- cache, web server 686, 689
- caching-only name server 505
- Cacti 438–440
- CAIDA (Cooperative Association for Internet Data Analysis) 394
- **camcontrol** command 61, 736, 737, 738
- Canaday, Rudd 1166
- **cancel** command 369
- Canonical, Ltd. 10, 87
- canonical name (CNAME) DNS records 522
- Capistrano 842, 960
- Carbon 1048, 1052
- Card, Rémy 764
- Carrier Pigeon Internet Protocol (CPIP) 377
- CAS 267
- CBK (Common Body of Knowledge) 1031
- ccTLDs (country code Top Level Domains) 503
- CDN (Content Delivery Network) 689–690
- Center for Internet Security 744
- CentOS Linux 8, 11
- Ceph 792
- CERT 1038
- Certificate Authority (CA) 1007
- Certificate Signing Request (CSR) 1013
- **cfdisk** command 719
- CFEngine 841
- **chage** command 247, 995
- chain of trust, DNSSEC 564
- channels, wireless 471
- character device files 128, 130–131, 329
- ChatOps 1043, 1108
- chat platforms 1108
- Chatsworth Products 1092
- **chattr** command 139
- `check_client_access` option, Postfix 668
- Check Point 409
- checksum, network 382
- Chef 841, 844, 848–849, 1109 943
- **chfn** command 249
- **chgrp** command 137–138
- Children's Online Privacy Protection Act (COPPA) 1128
- **chkrootkit** command 990
- **chmod** command 136–137, 199
- **chown** command 137–138, 259
- Christiansen, Tom 188, 189
- CIA triad 983
- CI/CD (Continuous Integration and Continuous Delivery)
  - artifact 957
  - auditability 953
  - automation 952
  - blue/green deployment 961
  - build 952, 956–957
  - and containers 978–980
  - delivery 951
  - deployment 951, 959–960
  - environments 953–955
  - essential concepts 951–955
  - example 964–978
  - feature flags 955
  - integration 951, 952–953
  - pipeline 955–961, 972–978
  - release 956
  - release candidate 956
  - repository organization 968
  - and revision control 952
- CI/CD *continued*
  - stages 977
  - testing 957–959, 975–976
  - zero downtime 960–962
- CIDR (Classless Inter-Domain Routing) 379, 389, 391–392
- CIFS *see* SMB (Server Message Block)
- CIP (Critical Infrastructure Protection) 1129
- CISA (Certified Information Systems Auditor) 1032
- CIS (Center for Internet Security) 1034
- Cisco Adaptive Security Appliance 409
- Cisco IronPort 608
- Cisco routers 494–496
- Cisco Systems 480, 1008
- CISSP (Certified Information Systems Security Professional) 1031
- CJIS (Criminal Justice Information Systems) 1128
- ClamAV 990
- CLAMS acronym 1107
- C language 1167
- **cleanup** daemon 660
- **/var/spool/clientmqueue** directory 616
- **clone** system call 93
- CloudBees 961
- cloud computing 270–293
  - access to 277–278
  - automation 282
  - availability zones 278–279
  - backup, data 789–790
  - booting alternate kernels 355–356
  - cost control 291–293
  - CPU stolen cycles 1075
  - and DevOps 272
  - foundations of 270
  - fundamentals 276
  - IaaS 276
  - identity and authorization 281
  - images 280
  - instances 280
  - management layers 276
  - networking 280–281, 448–457
  - PaaS 276
  - platforms 273–276
  - public, private, and hybrid 273–274

- cloud computing *continued*
  - reasons for 271
  - regions 278–279
  - SaaS 276
  - serverless 282
  - storage 281
  - virtual private servers 279
  - web hosting 694–696
- CloudFlare 690
- CloudFront 690
- cloud hosting providers 25
- **/var/log/cloud-init.log** file 297
- CNAME DNS records 522
- `cn` LDAP attribute 582
- Coarse Wavelength Division Multiplexing (CWDM) 464
- Coax cable 460
- Cobbler 161–162, 842
- COBIT 1127, 1128
- code coverage 958
- code promotion 1110, 1118
- **collectd** command 1057
- **etc/collectd/collectd.conf** file 1058
- Common Body of Knowledge (CBK) 1031
- Common Criteria 1034
- common name, LDAP 582
- **/etc/pam.d/common-passwd** file 247
- **/compat** directory 126
- Computer Fraud and Abuse Act 1131
- concentrators *see* Ethernet: hubs
- conferences, system administration 19
- confidentiality, data 983, 1005
- **/etc/selinux/config** file 87
- configuration management
  - architecture 843–845
  - best practices 895
  - dangers of 834
  - dependency management 846–848
  - elements of 835–841
  - language comparison, platforms 845
  - overview 834
  - popular systems 841–852
  - rosetta stone 842
- **/usr/exim/configure** file 644
- `CONFIGURE_FILE` variable, Exim 641
- `confLOG_LEVEL` option, **sendmail** 639
- congestion control algorithms, TCP 417
- `conncontrol` feature, **sendmail** 631
- `ConnectionRateThrottle` option, **sendmail** 637
- `CONNECTION_RATE_THROTTLE` option, **sendmail** 628
- containers 904–905, 915–948
  - as build artifacts 979
  - capabilities 917
  - and CI/CD 978–980
  - clustering 942–948
  - control groups 917
  - core concepts 916–919
  - images 917–918, 979
  - management software 944–948
  - namespaces 917
  - networking 918
  - utility of 915–916
  - vs. virtualization 906
- Content Delivery Network (CDN) 689–690
- Continuous Integration and Delivery *see* CI/CD
- control 1096
- CONT signal 95, 96
- cooling
  - calculating load 1097–1098
  - data center 1096–1101
  - in-row 1099–1100
- COPPA (Children's Online Privacy Protection Act) 1128
- Corbato, Fernando 1166
- CoreOS Linux 8
- country code domains (ccTLDs) 503
- Courion 268
- CPAN (Comprehensive Perl Archive Network) 1055
- CPU
  - analyzing usage 1079–1081
  - stolen cycles 1075
  - utilization 1074
- **/proc/cpuinfo** file 1077
- CRAC (Computer Room Air Conditioner) 1099
- **/var/crash** directory 359
- Critical Infrastructure Protection (CIP) 1129
- **/etc/cron**.{**allow**,**deny**} file 113
- **cron** daemon 109–113, 1041
  - log file 297
- **/var/log/cron** file 297
- **crontab** command 109
- crontab file 110–113
- cryptography 1005–1016
  - Diffie-Hellman key exchange 557
  - DNSSEC 557
  - public key 1006–1007
  - symmetric key 1005–1006
- C shell 187, 189
- **.cshrc** file 258
- **csh** shell 189
- CSMA/CD protocol 460
- CSR (Certificate Signing Request) 1013
- CSRG (Computer Systems Research Group) 1169
- Cummins Onan 1093
- CUPS (Common UNIX Printing System) 361–365
  - *see also* printing
  - autoconfiguration 366
  - filters 364–365
  - instances 363
  - logging 369
  - network printing 365, 367
  - queue 362
  - restarting 369
- **cups-config** command 369
- **/etc/cups/cupsd.conf** file 363, 365
- **cupsd** daemon 362
- **cupsdisable** command 369
- **cupsenable** command 369
- **curl** command 24, 675, 679–680
- **cut** command 194
- CVS 962
- CyberArk 994
- Cybersecurity Act of 2015 1131

D

- DA (Delivery Agent) 597, 599
- **/var/log/daemon.log** file 297
- daemons 41
- DARPA (Defense Advanced Research Project Agency) 1169
- **dash** shell 189
- DataBase Administrators (DBAs) 27

data center
see also cooling
availability 1101
components 1091
cooling load 1097–1098
generators 1093
hot aisle 1098–1099
humidity 1100
in-row cooling 1099
location 1102
power 1092
rack density 1094
rack power requirements 1094–1095
racks 1092
raised floor 1092, 1099
redundant power 1093, 1101
reliability tiers 1101
security 1102
temperature range 1096
toolbox 1103
track system 1092
UPSs 1092, 1101
Datadog 1050
Data Loss Prevention (DLP) 608
DBAN (Darik's Boot and Nuke) 738
DBAs (DataBase Administrators) 27
dc LDAP attribute 582
DDoS (Distributed Denial-of-Service attack) 985
debconf utility 159
Debian/GNU Linux 8, 10
debian-installer script 159
debt, technical 1105
/var/log/debug* files 297
debugging *see* troubleshooting
default route 415, 421, 426, 483, 491
DefCon conference 20
defense in depth 987
DeHaan, Michael 161
DELAY_LA option, **sendmail** 628, 637
deleting accounts 264
Delivery Agent (DA) 597, 599
deluser command 265
delv command 509, 566
denial of service (DOS) attack 1089
DNS 508, 514, 553
email 628, 636
Dennis, Jack 1166
Deraison, Renaud 998
DES hashing algorithm 248
/etc/devd.conf file 338
devd daemon 331, 338
/dev directory 125, 126, 130, 329
development environment 954
devfs filesystem 331, 337
device drivers 328–338 344
device files 329–330
block vs. character 329
creation of 331
for disks 734–735
management of 330–338
device names, ephemeral 735
DevOps 26, 1106
see also CI/CD
automation 1109
ChatOps 1108
chat platforms 1108
CI/CD 949–980
CLAMS acronym 1107
and cloud computing 272
code promotion 1110
and configuration management 833
culture 1107
environment separation 1118
infrastructure as code 1116
lean tenet 1108
measurement 1110
philosophy, paging 1108
sharing 1110
system administrator role 1110
tenets 1107
DevOpsDays conference 20
devtmpfs filesystem 332
df command 767, 1057
dhclient command 427
/etc/dhclient.conf file 427
dhcpd.conf file 404–406
dhcpd daemon 404–406
DHCP (Dynamic Host Configuration Protocol) 156, 402–406 549
dhcrelay daemon 406
Diffie-Hellman-Merkle key exchange 1007
dig command 509–512
Digital Millennium Copyright Act (DMCA) 1131
DigitalOcean 26, 273, 275–277, 965, 970–972
booting alternate kernel 355
networking 456–457
quick start 289–291
recovery kernel 63
directories 122, 125–126
deleting 129
search bit 133
disaster recovery 1119–1122
in the cloud 278–279
list of data to keep handy 1121
planning 1120
risk assessment 1119
staffing 1121
standards 1120
threats 1119
who to put in charge 1121
/dev/disk directory 735, 770
diskpart command 745
disks
see also filesystems
addition of 718–721
bad block management 735–736
block size 729–730
comparison of HDD and SSD 722
device files 734–735
elevator algorithm 1086–1087
failure rate 723
filesystems 762–763, 763–771
formatting 735–736
hardware 721–730
hardware attachment 733–734
hardware interfaces 730–733
HDD 722–725
hot-pluggable 733
hybrid 728
logical volumes 748
LVM 747–753
management layers 740–742
monitoring with SMART 738–740
naming standards, device 734
partitions 742–747
performance 1084–1085, 1085–1086
physical volumes 748
RAID 753–762
reliability, HDD 723
reliability, SSD 727
resizing filesystems 751–753

- disks *continued*
  - rewritability limit, SSD 726
  - scheme, partitioning 743
  - snapshots 750–751
  - speeds 722
  - tradeoffs of 721
  - types 724
  - usage 108
  - usb drive, mounting 770
  - volume groups 748
  - warranties 725
- **/proc/diskstats** file 1077
- distance-vector protocols 486
- distinguished name, LDAP 582
- Distributed Denial of Service attack (DDoS) 985
- DIX Ethernet II framing 382
- DKIM (DomainKeys Identified Mail) 607
- DKIM (DomainKeys Identified Mail) DNS records 525
- DLP (Data Loss Prevention) 608
- DMARC (Domain-based Message Authentication, Reporting, and Conformance) DNS records 525
- DMCA (Digital Millennium Copyright Act) 1131
- **dmesg** command 319, 335
- **/var/log/dmesg** file 297
- **dmidecode** command 1078
- **dmsetup** command 742
- DMZ (DeMilitarized Zone) 1029
- `dn` LDAP attribute 582
- DNS
  - *see also* BIND
  - *see also* name servers
  - *see also* resource records, DNS
  - *see also* zones, DNS
  - apex zone 522
  - architecture 499
  - Berkeley Internet Name Domain (BIND) daemon 525–541
  - bogus TLD 543
  - cache poisoning 530
  - caching 508–509
  - and CDNs 690
  - cloud-based 500
  - configuration 415–416
  - database 512
  - debugging 509–510
  - **delv** command 509
  - dynamic updates 549
  - EDNS0 protocol 532
- DNS *continued*
  - efficiency 508–509
  - forward zones 502
  - in-addr.arpa zone 502, 520
  - ip6.arpa 521
  - IPv6 support 519, 521
  - key rollover, DNSSEC 565
  - KSKs (key-signing keys) 566–570
  - lame delegations 575
  - lookups 500
  - **named.conf** file 526
  - `nameserver` directive 501
  - name server market share 500
  - name servers 504
  - name server types 504
  - namespace 502
  - negative caching 508
  - `NOERROR` status 510
  - **/etc/nsswitch.conf** file 501
  - `NXDOMAIN` status 510, 570
  - open resolvers 553
  - primary objective 498
  - private addresses, queries from 541
  - query 499
  - record types 515
  - recursive servers 530
  - registering a domain name 503
  - **/etc/resolv.conf** file 500
  - resolver configuration 500
  - resource records *see* resource records, DNS
  - reverse mapping 502, 506, 520
  - root server hints 539
  - root servers 505, 506, 539
  - round robin 508–509
  - second-level domain name 503
  - security 551
  - `SERVFAIL` status 510, 568, 572, 575
  - service providers 500
  - splattercast 529
  - split DNS 541
  - subdomains 503
  - TTL (time to live) 508
  - UDP packet size 532
  - ZSK (Zone-Signing Keys) 566–570
- DNSKEY DNS records 558
- `dnslookup` driver, Exim 653
- Dnsmasq 156
- DNSSEC 525, 557–568
- **dnssec-keygen** command 561
- **dnssec-signzone** command 562
- **doc** command 576
- Docker 905, 915, 919–937
  - architecture 919–921
  - base images 933
  - bridge network 928–929
  - client setup 921
  - debugging 942–944
  - **Dockerfile** 933, 933–934, 941
  - docker group 921
  - Docker Hub 922
  - filesystem 918–919
  - image building 932–936
  - installation 921
  - interactive shell 923
  - logging 938
  - logs 925
  - namespaces 928–929
  - networking 927–930
  - options 930–932
  - overlays, network 930
  - registries 936–937
  - repository, images 922–926
  - rules of thumb 937
  - running containers 924
  - security 939–941
  - storage drivers 930
  - subcommands 920
  - Swarm 947
  - and **systemd** 932
  - TLS 940
  - volume containers 927
  - volumes 926–927
- **.dockercfg** file 936
- **docker** command 919–921, 922–926
- **dockerd** daemon 919, 930–932
- **/var/lib/docker** directory 919
- `DOCKER_HOST` environment variable 922
- Docker Hub 936
- Docker, Inc. 919, 936
- **/var/run/docker.sock** socket 932
- Docker Swarm 960, 979
- documentation 14–16
  - BCPs 377
  - FYIs 377
  - local 1115
  - man pages 14–16
  - package-specific 16
  - RFCs 17, 377
  - standards 1116
  - STDs 377
  - system-specific 16

DomainKeys Identified Mail
  see DKIM
`DOMAIN` macro, **sendmail** 621
"do not fragment" flag 383
`DontBlameSendmail` option, **sendmail** 632
`DONT_BLAME_SENDMAIL` option, **sendmail** 628
dot files 259
`DOUBLE_BOUNCE_ADDRESS` option, **sendmail** 628
Double Choco Latte 1114
double colon notation 395
dpkg command 164, 166–167
/var/log/dpkg.log file 297
dpkg-query command 22
DR *see* disaster recovery
drill command 509–511, 568
drivers *see* device drivers
Drone 979
Dropbear 1027
DS DNS records 558
dtrace command 1058
dtrace tool 1057
du command 1057
dumpon command 359
Duo 991

E

echo command 201
`EDITOR` environment variable 193
editors, text 7
effective GID 67
effective UID 67
efibootmgr command 34
EFI (Extensible Firmware Interface) 746
EFI System Partition (ESP) 33
EGID (Effective GID) 92
Eich, Brendan 187
EIGRP (Enhanced Interior Gateway Routing Protocol) 486, 490
Elastic 322
Elastic Beanstalk 695
Elastic Load Balancer (ELB) 686
Elasticsearch 321, 1110
Electronic Communications Privacy Act 1131
Electronic Frontier Foundation 1008
elevator algorithm 1086–1087
ELK (Elasticsearch, Logstash, Kibana) stack 321–322, 1110
.emacs file 258
email
  see also aliases, email
  see also Exim
  see also MX DNS records
  see also Postfix
  see also **sendmail**
  access agents 599
  aliases 608
  architecture 597–600
  body 600–602
  bounces 610
  components 597–600
  configuration 612–613
  delivery agents 599
  encryption 607
  envelope 600
  forgery 606
  headers 600–602
  loops 610
  Maildir format 599
  mailer-daemon 610
  Mail Submission Agent (MSA) 598
  marketshare 612
  mbox format 599
  message structure 600–603
  MX records 521–522, 623, 626, 653
  postmaster 609
  privacy 607–608
  spam *see* spam
  transport agents 598–599
  User Agents (UA) 597
Email Privacy Act 1131
EMC Ionix (Infra) 1114
emergency.target target 50
encryption *see* cryptography
environmental monitoring 1100
environment separation 1118
environment variables 193–194
ephemeral storage 281
equipment racks 1092
escrow, password 993–995
ESMTP protocol 599, 603
ESP (EFI System Partition) 33
/etc directory 125, 126
Ethernet 381, 460–469
  addressing 384–385
  autonegotiation 412, 422, 426, 467
  broadcast domain 461
Ethernet *continued*
  broadcast storms 466
  cable characteristics 463
  collisions 460
  congestion 478
  CSMA/CD protocol 460
  framing 382
  hubs 465
  jumbo frames 468
  loops 466
  MTU 383, 469
  OUIs 384
  packet types 461
  power over (PoE) 468
  Routers 467
  signaling 460
  speeds 460–461
  standards 460
  switches 465
  topology 461
  trunking 467
  VLANs 466
ethtool command 421
Etsy 1052
EUID (Effective UID) 92
event logging 989
example systems 9–11
exec system call 93
execute bit 133
exicyclog command 643
exigrep command 643
exilog command 643
Exim 612, 640–658
  see also email
  access control lists (ACLs) 647–650
  aliases file 654
  authentication 651
  blacklists 649
  command-line flags 642
  configuration 643–655
  configuration variables 641
  content scanning 648
  debugging 658
  .forward file 655
  global options 645–647
  installation of 640
  lists 646
  logging 657–658
  macros 647
  options 645
  panic log 657
  `retry` configuration file section 656

Exim *continued*
 rewrite configuration file section 657
 routers 652–655
 security 642
 transports 655–656
 utilities 642
 virus protection 648
exim_checkaccess command 643
exim command 642
exim_dbmbuild command 643
exim_dumpdb command 643
exim_fixdb command 643
exim_lock command 643
eximon command 643
eximstats command 643
exim_tidydb command 643
EXIM_USER variable, Exim 641
exinext command 643
exipick command 643
exiqgrep command 643
exiqsumm command 643
exiwhat command 643
expect language 7
export command 193
exportfs command 802
/etc/exports file 797, 802
exports, NFS 796
EXPOSED_USER macro, **sendmail** 625
ext4 filesytem 763–771

F

FaaS (Functions as a Service) 282
Fabric 842, 960
Fabry, Robert 1168
Fail2Ban 1004
/var/log/faillog file 297
Family Educational Rights and Privacy Act (FERPA) 1128
FAST_SPLIT option, **sendmail** 628
FAT (File Allocation Table) 33
fcntl systems call 797
fdisk command 61, 719, 745
FEATURE macro, **sendmail** 622
Federal Information Security Management Act (FISMA) 1128
Fedora Linux 8, 10
Feigenbaum, Barry 819
FERPA (Family Educational Rights and Privacy Act) 1128
Ferraiolo, David 85
fetch command 24
fiber, optical
 color-coding 464
 multimode 464
 single-mode 464
 standards 464
 types 464
Fielding, Roy 693
file attributes 132–140
 ACLs 81
 change time 134
 changing 136–137
 color-coding 135
 of device files 135
 displaying with **ls** 134–136
 encoding 136
 execute bit 133
 flags 139
 group permission 133
 inode number 135, 764
 linux bonus 139
 mnemonic syntax 136
 NFS 148
 owner permission 133
 permission bits 132–133
 setuid/setgid bits 68, 133
 sticky bit 134
file command 126
file descriptors 190
File Integrity Monitoring (FIM) 1061
filenames
 control characters in 128
 globbing 128
 length limitation of 122
 pathnames 122
 pattern matching 13
 spaces in 202
files
 see also device files
 see also directories
 see also file attributes
 see also filenames
 access control of 66–67
 block device 128, 130–131
 character device 128, 130–131
 default permissions 138–139
 deleting 128, 129, 133
 directory 128, 129
 hard link 129–130
 link count 135
 local domain socket 128, 131
files *continued*
 modes *see* file attributes
 named pipe 128, 131
 regular 128, 129
 renaming 133
 revision control 235–240
 symbolic link 128
 types of 126–132
file sharing 791–818, 819–829
Filesystem Hierarchy Standard 126
filesystems 762–763, 763–771, 772–773
 see also partitions, disk
 ACLs 81, 140–152
 automatic mounting 768–770, 812–818
 Btrfs 783–788
 checking and repairing 62
 components of 121
 copy-on-write 772
 error detection 772
 ext4 763–771
 inodes 764
 journaling 763
 lazy unmounting 123
 lost+**found** directory 767
 mounting 122–124, 767
 NFS 796
 organization of 125–126
 pathnames 122
 performance 773
 polymorphism 765
 processes using 124
 relation to other layers 740–742
 replicated 816–817
 resizing 751–758
 root 36, 38, 41, 125
 SMB 825–826
 superblock 764
 terminology 764–765
 UFS 763–771
 union 917–919
 unmounting 122–124
 XFS 763–771
 ZFS 772–773, 773–783
filesystem UID 67
file transfer, secure 1027
FIM (File Integrity Monitoring) 1061
find command 137, 200
fio command 1085

firewalls 1027–1030
  packet-filtering 1028
  safety of 1029
  service filtering 1028
  stateful inspection 1029
firmware, system 32
FISMA (Federal Information Security Management Act) 1032, 1128
flock system call 797
Fluke 474, 480
Fluke meter 1097, 1099
Fontana, Richard 774
fork system call 93
formatting, disk 735
.forward file 609
`FORWARD` chain, **iptables** 444
forwarder, DNS 504–505
.forward file 634
forward zone, DNS 502
Fowler, Martin 949
Fox, Brian 187
FQDNs (Fully Qualified Domain Names) 502
frame, network 381
FreeBSD 11
  and Active Directory 587–589
  adding users 262–263
  and Kerberos 587–589
  anti-virus 990
  autonegotiation 426
  boot messages 353–355
  building, kernel 345
  configuration, kernel 344–346
  default route 426
  device management 337–339
  disk addition recipe 720–721
  firewall 445–448, 991, 1028
  fstab file 768
  idle timeout 253
  installation 161–164
  jails 905
  kernel panics 359
  loadable modules, kernel 348
  location of kernel source 345
  logging 302–318
  logical volume management 753
  log rotation 321
  NAT 445–448
  network hardware 426
  networking 425–427
  network parameters 427
  paging statistics 1083
FreeBSD *continued*
  parameters, kernel 344–345
  partitioning, disk 747
  printing 360–371
  /proc filesystem 105
  removing users 262–263
  router, use as a 482
  security of 982
  shadow passwords 252–254
  software management 175–178
  tracing 1058
  versions, kernel 328
  virtualization 910
  VPN 1030
freebsd-update command 176
free command 1057
Free Software Foundation (FSF) 1134
fsck command 123, 763, 765, 766
FSF (Free Software Foundation) 1134
/etc/fstab file 61, 123, 720, 721, 766, 812
  on FreeBSD 768
  on Linux 769
fully qualified domain names (FQDNs) 502
Functions as a Service (FaaS) 282
fuser command 124, 989, 1085
FYI (For Your Information) 377

G

gcloud cli tool 288–289
.gconf file 258
.gconfpath file 258
GCP (Google Cloud Platform) 26, 273, 275
  App Engine 277
  BigQuery 281
  booting alternate kernel 355
  Cloud Functions 283
  networking 455–456
  pricing 292
  quick start 288–289
GECOS field 245, 249, 1167
gem command 230
General Electric 1166
generators, standby 1093
generic top-level domains (gTLDs) 503
geom command 720
GeoTrust 1007
getent command 590
getfacl command 142–152
getpwnam() library call 244
getpwuid() library call 244
getty process 244
GIAC (Global Information Assurance Certification) 1032
gibi- prefix 13
GIDs *see* group IDs
giga- prefix 13
Git 952, 962, 1116
git command 236
.gitconfig file 258
GitHub repository 24, 235, 239–241, 962, 965
GitLab 235, 239–241, 962
Gi unit 13
GLBA (Gramm-Leach-Bliley Act) 1129
globbing 13, 128, 209
GlusterFS 792
go command 969
Go language 692, 966
Google 723, 756, 944
Google App Engine 695
Google Authenticator 991
Google Cloud Platform *see* GCP
Google Compute Engine (GCE)
  booting failures 64
  serial console 64
Google Container Registry 936
Google Deployment Manager 960
Google Gmail 596
Google G Suite 606
Google Wifi 472
gpart command 37, 720, 747, 769
gparted command 719, 746, 758
gpasswd command 254
gpg command 1015
GPG encryption 607
GPT (GUID Partition Table) 33, 719, 746, 770
Grafana 1048, 1049–1050, 1110
Gramm-Leach-Bliley Act (GLBA) 259, 1129
graphical.target target 50
Graphite 1047–1048, 1048, 1049–1050, 1052, 1110
Gravitational 1027
Graylog 322
`greet_pause` feature, **sendmail** 631
grep command 197–198

groupadd command 255
groupdel command 255
/etc/group file 66–67, 254–255, 579, 590
group IDs 92, 92–93, 245, 249
    see also groups
    mapping names to 67
    pseudo-groups 79–80
    real, effective, and saved 67
groupmod command 255
group permission bits 133
groups
    see also **/etc/group** file
    see also group IDs
    adding 255
    docker 921
    GID 254
    GIDs (group IDs) 67
    passwords 254
    vs. RBAC 85
growfs command 752
GRUB boot loader 34, 35–38
    boot password 986
    command line 37
    commands 38
    options 38
    single-user mode 62
grub.cfg config file 36, 358
grub-mkconfig utility 36
/efi/ubuntu/grubx64.efi bootstrap 34
/etc/gshadow file 254
gTLDs (Generic Top-Level Domains) 503
GUID (globally unique identifier) 33
GUID Partition Table (GPT) 33
GVinum 753

H

h2i command 675
H2O HTTP server 684
halt command 59
halting the system 59
haproxy.cfg file 710
HAProxy load balancer 710–713
    configuration of 710–711
    health checks 711
    statistics 712
    sticky sessions 712–713
    TLS terminaton 713–714
Hard Disk Drive (HDD) 722–725
hard links 129–130
hash, cryptographic 1009–1011
HashiCorp 282, 452, 911, 913, 965
Hazel, Philip 612, 640
HDD (Hard Disk Drive) 722–725
hdparm command 737, 738
head command 196
header, packet 381
Health Insurance Portability and Accountability Act *see* HIPAA (Health Insurance Portability and Accountability Act)
HEAT 1114
Hein, Trent R. 1171
Heroku 277, 695, 960
HGST 725
HIDS (Host-based Intrusion Detection System) 1062
hier man page 126
HIPAA (Health Insurance Portability and Accountability Act) 259, 1032, 1129
HipChat 1108
history
    of Linux 1171–1172
    of Sun Microsystems (now Oracle America) 1169
    of system administrators 1169–1170
    of UNIX 1166–1168
Hitachi 725
/home directory 126
home directory, user 250, 744
`home_mailbox` option, Postfix 665
host command 509
hosting recommendations 25
hostname 385, 411–412
    fully qualified 502
hostname command 411
/etc/hostname file 419
/etc/hosts file 385, 411
hot aisle cooling 1098–1099
HP-UX 11
htop command 102
htpasswd command 701
.htpasswd file 701
httpd.conf file 698
/var/log/httpd/* file 297
httpd server 684, 696–704
    applications server modules 702
    authentication, basic 701
    configuration 698–699
    log file 297
httpd server *continued*
    logging 703
    multi-processing modules 697
    TLS configuration 702
    virtual hosts 699
HTTP protocol 674–682
    authentication, basic 676, 701
    headers 678
    keep-alive 680–681
    load balancers 684
    over TLS 681
    port 697
    request methods 677
    responses 677
    security of 676
    servers 683–684
    SNI (Server Name Indication) 682
    versions of 675
HTTPS protocol 676, 681
    port 697
hubs, Ethernet 465
humidity 1100
HUP signal 95, 96, 304, 320
HVAC *see* cooling
HVM (Hardware Virtual Machine 902
hybrid cloud 274
hypervisors 901–904

I

IaaS (Infrastructure as a Service) 276
IAM (Identity and Access Management) 268–269, 282
IANA (Internet Assigned Numbers Authority) 503
IBM SoftLayer 273, 905
IBM T. J. Watson Research Center 612, 658
ICANN (Internet Corporation for Assigned Names and Numbers) 376, 392, 479, 503
Icinga 1043, 1046–1047, 1110
`icmp_echo_ignore_broadcasts` parameter 424, 425
ICMP (Internet Control Message Protocol) 378
    redirects 401–403, 407
id command 800
~/.ssh/id_ecdsa.pub file 1020
identity management *see* IAM

idle timeout, FreeBSD 253
IDS (Intrusion Detection System) 1062
IEC units 13
IEEE 802.2 framing 382
IEEE standards
  802.1Q 467
  802.1x 470, 475
  802.3 460
  802.3ab 460
  802.3af 468
  802.3an 460
  802.3ba 460
  802.3bs 460
  802.3bt 468
  802.3u 460
  802.11ac 469
  802.11b 473
  802.11g 469
  802.11n 469
IETF (Internet Engineering Task Force) 376
ifconfig command 387, 412, 425–426, 470, 1079
ifdown command 417, 419, 421
ifup command 417, 419, 421
IGF (Internet Governance Forum) 376
IMAP protocol 604
IMAPS protocol 604, 608
in-addr.arpa DNS records 520
in-addr.arpa zone 502
incident handling 1037–1038, 1122
/usr/include directory 126
InfluxDB 1049
Information Systems Audit and Control Association (ISACA) 1128
Information Technology Infrastructure Library (ITIL) 1130
Infrastructure as a Service (IaaS) 276
infrastructure as code 911, 952, 1116
init process 30–31, 41–43, 57, 93
  bootstrapping and 42
  flavors of 42
  modes 41
  run levels 43, 50
  startup scripts 57
  vs. **systemd** 43
init scripts 31
Innotek GmbH 911
inode file attribute 135, 764
`INPUT` chain, **iptables** 444
in-row cooling 1099
(IN)SECURE magazine 1036
integration tests 958
integrity, data 983, 1005
Intel 902
/etc/network/interfaces file 419
interfaces, network *see* networks
International Computer Science Institute (ICSI) 1001
International Organization for Standardization (ISO) 462
Internet
  documentation 376–379
  governance of 376
  history 375–378
  registries 392, 503
  standards 376–379
Internet Assigned Numbers Authority (IANA) 503
Internet Corporation for Assigned Names and Numbers (ICANN) 479, 503
Internet of Things (IoT) 1173
Internet Printing Protocol (IPP) 361
Internet protocol *see* IP
Internet Systems Consortium (ISC) 16, 525
INT signal 95, 96
ioctl system call 330
iostat command 1057, 1084–1085
IoT (Internet of Things) 1173
IP 375–458
  see also routing
  address assignment 411–412
  address classes 387–388
  addresses 385, 387–398
  allocation, address 392
  anycast 386
  ARP 401–402
  broadcast 386, 426
  broadcast ping 407, 423
  broadcast storm 413
  CIDR 391–392
  configuration 410–416, 418
  configuring 425–426
  debugging 428–436
  default route 415, 421, 426
  DHCP 402–406
  directed broadcast 407
  encapsulation 381–382
  faster than light (FTL) 377
IP *continued*
  firewalls 408–409
  forwarding 406
  fragmentation 383
  IPv4 vs. IPv6 379–381
  layers 378
  masquerading *see* NAT
  MTU 383
  multicast 386
  netmask 413, 426
  packet size 382–384
  packet sniffers 434–437
  packet structure 381–382
  ports 385–386
  private addresses 392–394
  privileged ports 386
  reassembly 383
  redirects 407
  routing 398–401
  security 406–410
  services 386
  source routing 407
  spoofing 408
  stack 378
  subnetting 388–389
  time-to-live field (TTL) 431
  transmission via avian carriers 377
  unicast 386
  uRFP 408
  VPN 409–411
TCP/IP *see* IP
ip6.arpa zone 521
ipcalc tool 390
ip command 387, 399, 402, 412, 414, 418, 483, 1079
iperf tool 437–438
/etc/ipf/ipf.conf file 445
IPFilter 445–448
`ip_forward` parameter 425
ipfw command 991, 1028
IPP (Internet Printing Protocol) 361
IPsec protocol 409, 1030
iptables command 440–445, 991, 1028
IPv4 *see* IP
/proc/sys/net/ipv4 directory 422
IPv6 394–399, 402–406
  see also IP
  addressing 394–399
  address notation 395–396
  automatic host numbering 397
  debugging 428–436

- IPv6 *continued*
  - DNS support 519, 521
  - double colon 395
  - fragmentation 383
  - link-local unicast 485
  - MTU 383
  - Neighbor Discovery (ND) 398, 401–402
  - penetration of 379
  - prefixes 396–397
  - scenic routing for 377
  - SLAAC 397
  - tunneling 398
  - vs. IPv4 379–381
- **/proc/sys/net/ipv6** directory 422
- (ISC)2 International Information Systems Security Certification Consortium 1031
- ISO 27001:2013 standard 1123, 1129
- ISO 27002:2013 standard 1129
- ISOC (Internet Society) 376
- ISO (International Organization for Standardization) 462
- ISP (Internet Service Provider) 376, 392
- IT Governance Institute (ITGI) 1128
- ITIL (Information Technology Infrastructure Library) 1127, 1130
- **iwconfig** command 470
- **iwlist** command 470

J

- Jacobson, Van 435
- Java language 691
- JavaScript 186, 187
- JavaScript Object Notation (JSON) 692, 850–852
- Jenkins 961–964, 1109
  - build agents 963
  - build context 962
  - build master 963
  - build trigger 962
  - and code repositories 962
  - concepts 962–963
  - distributed builds 963
  - and Docker 961
  - **Jenkinsfile** file 964, 968, 975
  - job 962
  - Pipeline 963–965, 968–970
  - project 962
- Jenkins Enterprise 961
- **Jenkinsfile** file 964, 968, 975
- Jinja 845, 851, 862, 863, 864, 876, 878, 879, 880
- Jira 1114
- Jodies, Krischan 390
- John the Ripper 1000
- Jolitz, Bill 1171
- JOSSO 267
- **journalctl** command 56–57, 298, 319, 335
- **/etc/systemd/journald.conf** file 57, 300
- **journald** process 43, 56
- journaling, filesystem 763
- Joy, Bill 187, 1169
- **jq** command 693
- JSON (JavaScript Object Notation) 692, 850–852
- jumbo frames, Ethernet 468
- Juniper Networks 480

K

- k8s *see* Kubernetes
- Kali Linux 8
- Kaminsky, Dan 530
- Karels, Mike 1171
- **.kde/** directory 258
- **kdestroy** command 588
- [**kdump**] process 41
- KeePass 994
- Kerberos 81, 267, 579, 586–589, 1015–1016
  - and Active Directory 587–589
  - and NFS 798
  - and NTP 588
- kernel
  - arguments 31
  - booting 348
  - booting alternate in cloud 355–356
  - building, FreeBSD 345–346
  - building, Linux 341–343
  - errors 356–359
  - functions of 325–326
  - initialization of 41
  - loadable modules 346–348
  - loading 31
  - location of 125
  - options 38
  - panics 356–359
  - selection of 36, 40
- kernel *continued*
  - single-user mode 35
  - source location, FreeBSD 345
  - source location, Linux 342
  - tuning, FreeBSD 344–345
  - tuning, Linux 339–341
  - version numbers 327–328
- **/boot/kernel** directory 348
- **/var/log/kern.log** file 297
- **kgdb** command 359
- Kibana 321, 1110
- kibi- prefix 13
- Kickstart 156
- **killall** command 97
- Kill A Watt meter 1097
- **kill** command 97, 1089
- KILL signal 95, 96
- kilo- prefix 13
- **kinit** command 588
- Ki unit 13
- **kldload** command 348
- **kldstat** command 348
- **kldunload** command 348
- **klist** command 588
- **/dev/kmsg** device 299
- **knife** command 844
- **~/.ssh/known_hosts** file 1017
- Kolstad, Rob 1171
- Korn shell 189
- **/etc/krb5.conf** file 587–589
- Krebs, Brian 986
- **ks.cfg** file 156–159
- **ksh** shell 189
- **kubectl** tool 945
- Kubernetes 283, 944–946, 960, 979
- Kuhn, Rick 85
- kVA unit conversion 1094–1095
- KVM 904, 908–910
  - guest installation 909–910
- kW unit conversion 1094–1095

L

- LACNIC 392
- Lambda 696
- lame delegations, DNS 575
- LAN (Local Area Network) 460–469
- Large Installation System Administration (LISA) conference 1171
- **last** command 298

/var/log/lastlog file 297, 298
layer 3 switches 467
LDAP 267, 580–586
 alternatives to 594
 attributes 581
 coverting **passwd** and **group** file 585–586
 data structure 581–582
 use with Exim 651
 LDIF 582
 querying 584–585
 uses for 580–581
 use with **sendmail** 624
/etc/openldap/ldap.conf file 583
LDAP_DEFAULT_SPEC option, **sendmail** 628
LDAP (Lightweight Directory Access Protocol) 579
`ldap_routing` feature, **sendmail** 624
ldapsearch command 584
LDIF (LDAP Data Interchange Format) 582
League of Professional System Administrators (LOPSA) 1134
least privilege, principle of 987
LEDE 472
Lerdorf, Rasmus 187
Let's Encrypt 1008
/lib64 directory 125
/lib directory 125, 126
/usr/lib directory 126
libpcap format 435
Librato 1050
licenses, software 1133
Lightweight Directory Access Protocol *see* LDAP
limits command 1090
link layer 381
links
 hard 129–130
 symbolic 128, 131–132
link-state protocols 487
lint tool 697
Linux
 account attributes 250–252
 and Active Directory 587
 adding users 261–262
 anti-virus 990
 as a firewall 409, 440–448
 autonegotiation 422
 boot messages 349–353
 building, kernel 341–343
 bulk account creation 263–264
Linux *continued*
 configuration, kernel 339–344
 default route 421
 device driver, adding 344
 device management 331–337
 device mapper 742
 disk addition recipe 719–720
 distributions 8
 errors, kernel 356–358
 filesystem, creating 766
 firewall 991, 1028
 fstab file 769
 history of 1171–1172
 iptables 440
 and Kerberos 587
 loadable modules, kernel 346–348
 location of kernel source 342
 logging 295, 299–302
 logical volume management 748
 log rotation 319–321
 LXC 905
 NAT 444–445
 network configuration 418
 network hardware 421–422
 networking 417–425
 NetworkManager 417
 network tuning 422–424
 parameters, kernel 339–341
 partitioning, disk 746
 PAT 444–445
 performance checkup 1077–1088
 pluggable congestion control algorithms 417
 printing 360–371
 profiling, performance 1087–1090
 RAID 756, 758–764
 reasons to choose 1071
 router, use as a 482
 scheduler, I/O 1086–1087
 security-enhanced 83, 85
 security of 982
 shadow passwords 250–252
 stateful firewall 445–448
 swap space 771
 TCP/IP options 422–424
 tracing 1058
 versions, kernel 327–328
 vga modes 358
 virtualization 905–910
 and viruses 989
Linux *continued*
 VPN 1030
 and ZFS 774
LinuxCon conference 20
LinuxFest Northwest 1134
Linux Foundation 905, 1008, 1134
Linux installation
 see also system administration
 automating with **debian-installer** 159–160
 automating with Kickstart 156–159
 CentOS 156
 Debian 159
 netbooting with Cobbler 161
 preseeding 159–162
 Red Hat 156
 Ubuntu 159
 via PXE 154–155
Linux Mint 8
Linux package management 164–166
 APT 169–170
 high-level management systems 166–174
 repositories 167–169
 RHN 169
Lions, John 1169
LISA conference 20
LLC (Link Layer Control) layer 382
lmtp daemon 660
LMTP (Local Mail Transfer Protocol) 660
ln command 129, 131
loadable modules
 in FreeBSD 348
 in Linux 346–348
/proc/loadavg device 1056
load balancing
 architecture 685
 in AWS 686
 equalization 685
 with HAProxy 710
 http 684
 with NGINX 708
 partitioning 685
 round robin 508, 685
 and security 686
 servers 1073
loader bootstrap 39–40
 commands 40
 configuration 40

- **/boot/loader.conf** configuration file 40
- **/boot/defaults/loader.conf** file 348
- Local Area Network (LAN) 460–469
- **local** daemon 660, 664
- **/usr/local** directory 125, 126
- **/etc/mail/local-host-names** file 622
- `local_interfaces` option, Exim 646
- localization, software 178–181
  - guidelines 178–179
  - limiting active releases 180
  - organization 179
  - testing 180–181
  - update structure 179–180
- Local Mail Transfer Protocol (LMTP) 660
- **locate** command 21
- **lockd** daemon 798
- **lockf** system call 797
- locking accounts 265–266
- **/var/log** directory 126, 297
- **/var/spool/exim/log** directory 657
- `log_file_path` option, Exim 657
- **logger** command 318
- logging 294–324
  - *see also* syslog
  - architecture 296
  - at scale 321–323
  - boot-time 318
  - Docker 925, 938
  - for **sudo** 73
  - growth 298
  - **httpd** 703
  - kernel 318
  - locations 296–299
  - management 294–295, 319–321, 321–323
  - policies 323–324
  - rotation of files 319–321
- Loggly 323
- logical volume management 748
  - *see also* Btrfs filesystem
  - *see also* LVM
  - *see also* ZFS filesystem
- **login** command 244, 591
- **.login_conf** file 258
- **/etc/login.conf** file 246, 252–254
- **logind** process 43
- **/etc/pam.d/login** file 592
- **.login** file 258
- logins *see* user accounts
- login shell, user 250
- log monitoring 1059
- logos, example system 9–10
- **/etc/logrotate.conf** file 321
- **logrotate** utility 296, 319, 319–321
- `log_selector` option, Exim 658
- **/dev/log** socket 299
- Logstash 321, 1110
- **logwatch** tool 1060
- loopback address 387
- LOPSA (League of Professional System Administrators) 1134
- **lost+found** directory 767
- **lpadmin** command 369
- **lpc** command 369
- **lp** command 361, 369
- **lpinfo** command 369
- **lpmove** command 369
- **lpoption** command 369
- **lpoptions** command 368
- **lppasswd** command 369
- **lpq** command 361, 369
- **lpr** command 361, 362, 369
- **lprm** command 362, 369
- **lpstat** command 362, 369
- **lsattr** command 139
- **lsblk** command 719, 734
- **ls** command 134–136
- LSM (Linux Security Modules) 83
- **lsmod** command 346
- **lsof** command 124, 988, 1057, 1085
- **lsusb** command 335
- **lvchange** command 748, 749, 752
- **lvcreate** command 748, 750, 751
- **lvdisplay** command 748
- LVM (logical volume management) 747–753
  - architecture 748
  - configuration phases 749–753
  - relation to other layers 740–742
  - snapshots 750–751
  - vs. RAID 747
- **lvresize** command 748, 752
- LWN (Linux Weekly News) 1036
- LXC 917
- Lynis audit tool 999

M

- **m4** command 613, 617–618
- MAC (Mandatory Access Control) 84–85
- MAC (Media Access Control) address 384
- MAC (Media Access Control) layer 382
- **/bin/mail** command 598
- mail *see* email
- `mailbox_command` option, Postfix 665
- `mailbox_transport` option, Postfix 665
- Maildir format, email 599
- Maildrop 599
- **/var/spool/postfix/maildrop** directory 660
- `MAILER` macro, **sendmail** 622
- **/var/log/mail*** files 297
- `MAIL_HUB` macro, **sendmail** 626
- **mailq** command 638, 642, 671
- `mail_spool_directory` option, Postfix 665
- Mail Submission Agent (MSA) 597, 598
- Mail Transport Agent (MTA) 597, 598
- Mail User Agent (MUA) 597
- **main.cf** file, Postfix 661
- major numbers, device 329
- **make** command 957, 962
- **makemap** command 621
- **makewhatis** command 15
- malware 605–607, 984
- **man** command 15
- Mandatory Access Control (MAC) 84–85
- **mandb** command 15
- **/usr/share/man** directory 126
- man pages 14–16
  - sections 14
  - updating keywords db 15
- `MANPATH` environment variable 16
- Mantis 1114
- `manualroute` driver, Exim 653
- **/dev/mapper** device 742
- Marathon 946, 979
- Mascheck, Sven 133
- `MASQUERADE_AS` macro, **sendmail** 625
- Master Boot Record (MBR) 33
- MasterCard 1033
- **master.cf** file, postfix 661
- **/etc/salt/master** file 872

/etc/master.passwd file 68, 245, 252, 995
Matsumoto, Yukihiro "Matz" 187, 223
MatterMost 1108
MaxDaemonChildren option, **sendmail** 637
MAX_DAEMON_CHILDREN option, **sendmail** 628
MaxMessageSize option, **sendmail** 637
MAX_MESSAGE_SIZE option, **sendmail** 628
MAX_MIME_HEADER_LENGTH option, **sendmail** 628
MAX_RCPTS_PER_MESSAGE feature, **sendmail** 631
MAX_RCPTS_PER_MESSAGE option, **sendmail** 628
mbox format, email 599
MBR (Master Boot Record) 33, 745
McAfee SaaS Email Protection 606
McCarthy, John 270, 1166
MCI_CACHE_SIZE option, **sendmail** 628
MCI_CACHE_TIMEOUT option, **sendmail** 628
McIlroy, Doug 1167
McKusick, Kirk 764, 1171
MD5 hashing algorithm 246, 1011
mdadm command 758
mdadm.conf file 760–761
md RAID system 756
/proc/mdstat file 759
Mean Time Between Failures (MTBF) 723
mebi- prefix 13
/media directory 126
mega- prefix 13
memcached daemon 281
/proc/meminfo file 1077
memory
  management 1081–1082
  paging 1081
  usage, analyzing 1082
Mercurial 962
Mesos 283, 946, 979
/var/log/messages file 297
Metasploit 999
Metcalfe, Bob 460
MFA (MultiFactor Authentication) 991
mfsBSD project 162
MIB (Management Information Base) 1064
microscripts 183–184
Microsoft Active Directory 579, 580
  as a nameserver 500
  and FreeBSD 587–589
  and Linux 587–589
Microsoft Azure 273
Microsoft Office 365 596
mii-tool command 421
Miller, Todd 70
MIN_FREE_BLOCKS option, **sendmail** 628
/etc/salt/minion file 874
minor numbers, device 329
MIN_QUEUE_AGE option, **sendmail** 628
Mirai botnet 986
MIT 270, 579, 1166
Mi unit 13
mkdir command 129
mkfs.btrfs command 784
mkfs command 719, 765, 766
mkisofs command 162
mknod command 130, 331
mkswap command 771
/mnt directory 126
Moby project 919
mod_cache caching module, **httpd** 689
modified EUI-64 algorithm 397
mod_passenger module, **httpd** 702
mod_perl module, **httpd** 702
mod_php module, **httpd** 702
modprobe command 347, 445
/etc/modprobe.conf file 347
mod_proxy_fcgi module, **httpd** 702
/boot/modules directory 348
/lib/modules directory 346
mod_wsgi module, **httpd** 702
Monitorama conference 20
monitoring 1040–1069
  application 1059–1061
  burn-out 1068
  charting platforms 1049–1050
  command output, harvesting 1054–1056
  commercial platforms 1050–1051
  culture 1044–1045
monitoring *continued*
  dashboards 1044
  data collection 1051–1055
  data types 1042
  environmental 1100
  events 1042
  graphing 1047–1049
  historical data 1043
  historic trends 1042
  instrumentation 1042
  intrusion detection 1062–1064
  log 1059
  network 1055–1056
  noise 1068
  notifications 1043–1044
  overview 1041–1044
  platforms 1045–1051
  push notifications 1042
  and quality of life 1045
  real-time metrics 1042
  real-time platforms 1046–1047
  run books 1068
  security 1061–1063
  SNMP 1063–1067
  systems 1056–1059
  temperature 1100
  time-series platforms 1047–1049
  tips and tricks 1068
  what to monitor 1044–1045
Monitus 1050
Mosh 1027
mount command 123–124, 765, 767, 768, 807, 825
mountd daemon 802
mounting, filesystem 767
mount.ntfs command 123
mount_smbfs command 123
Mozilla Foundation 1008
MPLS (Multiprotocol Label Switching) 381
mpstat command 1057, 1075, 1080
/var/spool/mqueue directory 616
MSA (Mail Submission Agent) 597, 598
/var/spool/exim/msglog file 658
MSSP (Managed Security Service Provider) 1061
MTA (Mail Transport Agent) 597, 598
MTBF (Mean Time Between Failures) 723
mtree command 1062

- **mtr** tool 434
- MTU (Maximum Transfer Unit) 382–384, 1031
- MUA (mail user agent) 597
- multicast, IP 386, 461
- multicast routing 490
- Multics 1166
- MultiFactor Authentication (MFA) 991
- multimode fiber 460, 464
- Multiple-Input, Multiple-Output (MIMO) wireless 472
- multiuser mode 41, 43
- **multi-user.target** target 49, 50
- Munin 1049, 1060
- **munin-node** command 1060
- **munin-node.conf** file 1060
- Murdock, Ian 10
- MX DNS records 521–522
- `my_local_delivery` clause, Exim 656
- `my_remote_delivery` clause, Exim 656

N

- Nagios 1043, 1046–1047
- **named**
  - *see also* BIND
  - *see also* DNS
  - *see also* name servers
  - `$INCLUDE` directive 513
  - `$ORIGIN` directive 513, 538
  - `$TTL` directive 512, 513
  - `acl` statement 534, 552–553
  - `allow-query-cache` clause 532
  - `allow-query` clause 532, 552
  - `allow-transfer` clause 532, 552
  - `allow-update` clause 532
  - `also-notify` statement 529
  - `avoid-v4-udp-ports` clause 530
  - `avoid-v6-udp-ports` clause 530
  - `blackhole` clause 532, 552
  - `channel` clause 569
  - `clients-per-query` option 533
  - `controls` statement for **rndc** 540
  - `datasize` option 533
  - debug levels 573
  - `directory` statement 528
  - `dnssec-enable` option 532
  - `dnssec-must-be-secure` option 532
  - `dnssec-validation` option 532
  - dynamic updates 549
  - `edns-udp-size` option 532
  - error messages 572
  - `files` option 533
  - `forwarders` clause 531
  - `forward` option 531
  - freeze 574
  - `hostname` statement 529
  - `include` statement 527
  - `key-directory` statement 529
  - `key` (TSIG) statement 534
  - `lame-ttl` option 533
  - localhost zone 543
  - logging 568–572
  - `logging` clause 536, 569
  - log messages 572
  - `masters` statement 535
  - `max-acache-size` option 533
  - `max-cache-size` option 530, 533
  - `max-cache-ttl` option 533
  - `max-clients-per-query` option 533
  - `max-journal-size` option 533
  - `max-ncache-ttl` option 533
  - `max-udp-size` option 532
  - `notify` statement 529
  - `options` statement 528
  - performance tuning 533–534
  - `query-source` clause 530
  - `query-source-v6` clause 530
  - `recursion` option 530
  - `recursive-clients` option 530
  - reload 574
  - **root.cache** file 539
  - `search` directive 501
  - `server-id` statement 529
  - `server` statement 535
  - slave servers, configuring 538
  - split DNS 541
  - `statistics-channel` statement 536
  - `tcp-clients` option 533
  - `update-policy` clause 551
  - `use-v4-udp-ports` clause 530
  - `use-v6-udp-ports` clause 530
  - `version` statement 529
  - `view` statement 542
  - zones, configuring 536
  - `zone` statement 536
  - `zone-statistics` option 533
  - zone transfer permissions 532
  - zone transfers 548
- **named.conf** file 526
- named pipes 128, 131
- name servers
  - *see also* BIND
  - *see also* DNS
  - *see also* **named**
  - authoritative 504, 505
  - caching 504
  - caching-only 505
  - delegation 506
  - forwarder 504
  - master 504
  - nonauthoritative 504
  - nonrecursive 504, 505
  - primary 504
  - recursive 504, 505
  - root servers 505
  - secondary 504
  - slave 504
  - stub 504
  - switch file 501
- Name Service Switch (NSS) 590
- namespaces, Linux 82
- namespaces, process 91
- **nano** command 7
- Napierała, Edward Tomasz 813
- National Security Agency (NSA) 83, 85
- NAT (Network Address Translation) 379, 392–394, 444–445, 445–448
- **nc** command 1054
- ND (Neighbor Discovery protocol) 398, 401–402
- negative caching, DNS 508
- Neighbor Discovery protocol (ND) 398, 401–402
- Nemeth, Evi xl–xli, 1170
- NERC CIP 1032
- NERC (North American Electric Reliability Corporation 1129
- Nessus vulnerability scanner 998–1004
- **netcat** command 675
- **net** command 589
- Netlink sockets 330
- Net-SNMP package 1065

netstat command 399, 415, 482, 988, 1074
net-tools package 482
network administrators 27
network booting 154–155
networkd process 43
/etc/sysconfig/network file 420
Network File System *see* NFS
networking
  broadcast storm 413
  congestion control algorithms 417
  default route 426
  and Docker 927–930
  packet sniffers 434–437
  troubleshooting 428–436
  tuning 422–424
Network Intrusion Detection System (NIDS) 1000–1003, 1062
NetworkManager 417
network monitoring 1055–1056
network operations center (NOC) 27
networks
  see also Ethernet
  see also IP
  see also IPv6
  see also routing
  see also TCP/IP
  see also wireless networks
  architecture 477
  congestion 478
  design issues 476
  documentation 478
  expansion 477
  firewalls 1027–1030
  maintenance 478
  management 478
  packet contents 382
  port scanning 996–998
  software-defined (SDN) 473
  subnetting 388–389
  success factors 460
  wireless 469–473
network-scripts directory 56
Network Time Protocol (NTP) 295, 1132
Neumann, Peter 1167
newaliases command 612, 642, 663
Newark Electronics 479
newfs command 720, 765, 766
newgrp command 254
New Relic 1061
newsyslog utility 321
newusers command 263
NFS 791–818
  ACLs 147–152
  approach 794–801
  automatic mounting 812–818
  and AWS 795, 812
  client-side 807–810
  dedicated servers 812
  drawbacks of 794
  exports 796
  hard vs. soft mounts 809
  history of 794–795
  identity mapping 799–800, 810–811
  and Kerberos 798
  on Linux 802–804
  locking, file 797–798
  mounting at boot time 810
  mount options 809
  nobody account 800
  on FreeBSD 804–806
  performance 793, 801, 812
  ports 799, 810
  protocol versions 794–795
  pseudo-filesystem 797
  remote procedure calls 795
  root access 800
  RPC 795
  security 793–794, 798–799, 810
  server-side 801–807
  statefulness 792, 796
  statistics 811–812
  transport protocols 795
  vs. SMB 792, 821
nfsd daemon 802, 806–810
nfsstat command 811
nfsuserd daemon 811
nginx.conf file 706
nginx daemon 705
NGINX HTTP server 684, 704–709
  configuration 705–708
  installation of 704
  load balancing 708
  master process 704
  signals 705
  TLS 708
  virtual hosts 705
  worker process 704
nice command 102–103
niceness, process 93
NIDS (Network Intrusion Detection System) 1000–1003, 1062
NIS (Network Information Service) 594
NIST SP 800 series standards 1033
  800-34 1120, 1130
  800-53 1130
NLnet Labs DNSSEC tools 566
nmap port scanner 996–998
nmbd daemon 820–821
nobody account 79, 800
NOC (network operations center) 27
Node.js 691, 1052
No Electronic Theft Act 1131
nohup command 96
/var/run/nologin file 253
/bin/nologin shell 78
non-repudiation 1005
North American Electric Reliability Corporation (NERC) 1129
NoSQL database 946
NSA (National Security Agency) 981, 982
NS DNS records 518
NSEC3 DNS records 558
NSEC DNS records 558
nslookup command 509
NSS (Name Service Switch) 590
nsswitch.conf file 244, 245, 501, 579, 586, 590, 614, 823
ntpd daemon 587, 881
NTP (Network Time Protocol) 295
/dev/null file 330

O

`objectClass` LDAP attribute 582
object stores 281
office wiring 475
OID (Object Identifier), SNMP 1064
`o` LDAP attribute 582
OM1 fiber 464
OM2 fiber 464
OM3 fiber 464
OpenLDAP 580
open resolvers, DNS 553
OpenSolaris 773
OpenSSH 1019–1020
openssl selection 1012–1014

- OpenStack 273, 274, 283
- openSUSE Linux 8
- OpenVPN 409
- Open Web Application Security Project (OWASP) 992
- OpenWrt 8, 472
- **/opt** directory 126
- optical fiber 464
- **/etc/network/options** file 419
- Oracle 911
- Oracle Identity Management 268
- Oracle Linux 8
- Oracle VirtualBox 904
- O'Reilly Media 1170
- O'Reilly series (books) 17
- O'Reilly, Tim 1170
- organizational unit, LDAP 582
- orphaned processes 94
- OS1 fiber 464
- OSCON conference 20
- **ospf6d** daemon 493
- **ospfd** daemon 493
- OSPF (Open Shortest Path First) protocol 487, 489
- OSSEC (Open Source SECurity) 990, 1060, 1062, 1063
- OSS mailing list 1035
- OSTicket 1114
- `OSTYPE` macro, **sendmail** 621
- OTRS 1114
- OUI (Organizationally Unique Identifier) 384
- `ou` LDAP attribute 582
- out-of-memory killer 1082
- oven, easy-bake 468
- OWASP (Open Web Application Security Project) 992, 1034
- owner permission bits 133
- ownership, file 137–138

P

- PaaS (Platform as a Service) 276, 695
- package management 21–23, 162–176
- packages *see* software packages
- Packer 911–913, 965, 970–972
- **packer** command 913
- packet encapsulation 381–382
- packet filtering 991
- packet-filtering firewalls 1028
- packet forwarding 482–485
- packets
  - broadcast 461
  - multicast 461
  - unicast 461
- packet sniffers 434–437
- Padl Software 585
- [**pagedaemon**] process 41
- page size 90
- page table 1081
- PAM (Pluggable Authentication Modules) 80–81, 266, 590–593
- panic, kernel 356
- Papertrail 323
- paravirtualization 902
- **parted** command 719, 735, 746
- partitions, disk 742–747
  - *see also* filesystems
  - relation to other layers 740–742
  - scheme 743
- `PARTLABEL` option 770
- `PARTUUID` option 770
- passphrase 993
- **passwd** command 68, 251, 257
- **/etc/passwd** file 67, 244, 245–250, 579, 590, 995, 996
- passwords 992–996
  - aging 995
  - alternatives to 78
  - break the glass 994
  - change interval 993
  - changing 68
  - cracking 1000
  - escrow 993–995
  - expiration 250, 252
  - hashes 245, 246–248
  - management 994
  - obsolescence of 991
  - root 78
  - strength 247, 993
  - vaults 993–995
- `PATH` environment variable 199
- path MTU discovery 383
- pathnames 122
- `PATH` shell variable 70
- PAT (Port Address Translation) 393, 444
- payload, packet 381
- PCI DSS (Payment Card Industry Data Security Standard) 1033, 1129
- PCIe (Peripheral Component Interconnect Express) interface 730
- PCRE (Perl-Compatible Regular Expression) 659
- Peek, Mark 282
- penetration testing, application 992–993, 999
- **perf** command 1087
- `perf_events` interface 1087
- performance 1070–1090
  - *see also* performance analysis tools
  - analysis methdology 1076–1077
  - BIND 533
  - common issues 1073–1074
  - CPU 1074
  - disk 1084–1085
  - disk bandwidth 1075
  - kernel variables 1071
  - memory 1075, 1081–1082
  - network 1075
  - NFS 793, 801, 812
  - **nice** command 102–103
  - philosophy, tuning 1071–1072
  - resources that affect 1074
  - troubleshooting 1088–1090
  - tuning rules 1072
- performance analysis tools
  - **fio** command 1085
  - **iostat** command 1084
  - **mpstat** command 1075, 1080
  - **perf** command 1087
  - **ps** command 1081, 1089
  - **sar** command 1086
  - **top** command 1075, 1089
  - **uptime** command 1089
  - **vmstat** command 1075, 1079, 1083
- performance tests 958
- periodic processes 109–119
- Perl 186, 187
- permission bits, file 132–133
- `permit_mynetworks` option, Postfix 668
- PGP (Pretty Good Privacy) 607, 1014
- **pgrep** command 101
- philosophy, IT management 1105, 1106
- phishing 984, 1131
- PHP language 186, 187, 692
- phpLDAPadmin 579
- physical volumes 748
- **pickup** daemon 660
- **pidof** command 101

PID (Process ID) 91
/srv/pillar directory 872
ping6 command 429–431, 1055
ping command 429–431, 1055
Pingdom 1050
pip command 230, 853
pipe daemon 661
pkg command 22, 23, 176
pkill command 97
PKI (Public Key Infrastructure) 1007
Platform as a Service (PaaS) 276, 695
Pluggable Authentication Modules *see* PAM
policy 1122–1125
  appropriate use 1132
  best practices 1124
  enforcement 1132
  standards 1123
POP3S protocol 608
portmap daemon 799, 997
portmaster command 178
portsnap utility 177
postalias command 661
postcat command 661
postconf command 661, 663
Postel, Jon xli
Postel's Law xli
Postfix 612, 658–671
  see also email
  access control 667–669
  aliases file 660
  architecture 659
  configuration 661–669
  debugging 670–671
  encryption 670
  .forward file 665
  lookup tables 663–664
  null client configuration 662
  programs 659
  queues 660
  receiving mail 659
  security 661
  sending mail 660
  soft-bouncing 671
  utilities 661
  virtual domains 665–666
postfix command 661
postmap command 661
POSTROUTING chain, **iptables** 445
postsuper command 661
power factor 1095
poweroff.target target 50
Power over Ethernet (PoE) 468
power requirements
  blade servers 1094
  network equipment 1094
  storage equipment 1094
PowerShell Desired State Configuration 842
PPID (Parent PID) 91
Pratt, Ian 906
PREROUTING chain, **iptables** 444
preseed.cfg file 159
Pretty Good Privacy (PGP) encryption 607
preventative maintenance 1093
printenv command 193
PRINTER environment variable 363
printf command 201
printing 360–371
  see also CUPS
  architecture 360–361
  debugging 369–371
  Internet Printing Protocol (IPP) 361
  network printers 367
  service shutoff 368
privacy 1131
  and **sendmail** 635–636
PRIVACY_FLAGS option, **sendmail** 628
privacy legislation, E.U. 1129
PrivacyOption variable, **sendmail** 636
private addresses 392–394
private cloud 274
privileged ports 386, 997, 1028
/proc directory 126
procedures 1122–1125
processes 90–119
  components of 90–93
  control terminal 93
  EGID 92
  EUID 92
  GID 92
  init *see* **init** process
  life cycle 93–98
  monitoring of 98–101, 101–102
  namespaces 91
  niceness 93, 102–103
  nice value 1089
  open files 124
  orphaned 94
  ownership 67
processes *continued*
  periodic 109–119
  PID 91
  PPID 91
  priorities 103
  runaway 107–109, 1090
  spontaneous 41
  starting and stopping 93–98
  states 97–109
  tracing 105–107
  UID 92
  uninterruptible 98
  zombie 98
/proc filesystem 104–105, 124, 333, 339, 770, 1077
procfs filesystem 105, 339
procmail command 599
production environment 954
/etc/profile.d directory 259
/etc/profile file 255, 259
.profile file 194, 258
Prometheus 1048
proxy cache, web server 688
proxy, HTTP 683–684
ps command 98–101, 124, 1081, 1089
pseudo-accounts 78–80
pseudo-devices 330
pseudo-groups 78–80
pseudo-random number generators 1011
PTR DNS records 520
public cloud 274
public key authentication 1019
Public Key Infrastructure (PKI) 1007
PUE (Power Usage Effectiveness) 1095
Puppet 841, 844, 849–850, 1109
  and Docker 943
Purdue 1170
pvchange command 748
pvck command 748
pvcreate command 748, 749
pvdisplay command 748
PVH (ParaVirtualized Hardware) 903
PVHVM (ParaVirtualized HVM) 903
pw command 255, 257, 265, 995
pwconv utility 252
PXELINUX 156
PXE (Preboot eXecution Environment) 154–155

- Python language 7, 187, 215–222, 691
  - best practices 230–231
  - command-line arguments 220–221
  - data types 218–220
  - dictionaries 218–220
  - files 218–220
  - indentation 217–218
  - input validation 220–221
  - lists 218–220
  - loops 221–222
  - numbers 218–220
  - package management 229–230
  - strings 218–220
  - tuples 218–220
  - variables 218–220
  - versions 215–216
  - virtual environments 232
  - vs. Ruby 223

Q

- QCon conference 20
- QEMU PC emulator 903
- **qmgr** daemon 660
- **qshape** command 671
- quad A DNS records 519
- Quagga 493
- quay.io 936
- `QUEUE_LA` option, **sendmail** 628, 637
- QUIT signal 95, 96

R

- RabbitMQ 322
- rack density 1094
- rack power 1093–1094
- racks, equipment 1092
- Rackspace 273
- RAID (Redundant Array of Inexpensive Disks) 741, 753–762, 1073
  - disk failure recovery 756
  - levels 754–756
  - RAID 5 drawbacks 757–758
  - RAID 5 write hole 753, 758
  - scrubbing 758
  - software vs. hardware 753
  - vs. LVM 747
- RAID-Z *see* ZFS filesystem
- Rails web development platform 223
- RainerScript 312
- Rake 960
- RancherOS Linux 8
- **/dev/random** device 1012
- random number generation 1011
- ransomware 981–982
- Rapid7 999
- `ratecontrol` feature, **sendmail** 631
- RBAC (Role-Based Access Control) 85, 259
- **/etc/defaults/rc.conf** file 58
- **/etc/rc.conf** file 426
- **/etc/rc.d** directory 57
- **/etc/rc.d/rc.local** script 55
- **/etc/rc** script 57
- real GID 67
- **realm** command 587
- **realmd** daemon 587
- real UID 67
- **reboot** command 59
- reboot procedures 59
- **reboot.target** target 50
- `recipient_delimiter` option, Postfix 665
- Red Flag Rule 1130
- Red Hat Enterprise Linux
  - *see* RHEL
- Red Hat, Inc. 10
- Red Hat Network (RHN) 167, 169
- `redirect` driver, Exim 654
- `redirect` feature, **sendmail** 623
- Redis 281
- Redundant Array of Inexpensive Disks *see* RAID (Redundant Array of Inexpensive Disks)
- Reed, Darren 445
- `REFUSE_LA` option, **sendmail** 628, 637
- regexes *see* regular expressions
- regions, cloud 278–279
- regular expressions 209
  - captures 213
  - examples of 211–213
  - failure modes 213
  - literal characters 210
  - matching process 210
- re:Invent conference 20
- **reject** command 369
- `reject_unauth_destination` option, Postfix 668
- `RELAY_DOMAIN` feature, **sendmail** 630
- **/etc/mail/relay-domains** file 629
- `relay_entire_domain` feature, **sendmail** 630
- `relay_hosts_only` feature, **sendmail** 630
- **etc/postfix/relaying_access** file 669
- release 956
- release candidate 956
- Remedy 1114
- removing accounts 264
- rendezvous addresses, multicast 490
- **renice** command 102–103, 1089
- rescue mode 60
- **rescue.target** target 50, 61
- **resize2fs** command 752
- resizing, filesystem 751–758
- **/etc/resolv.conf** file 415, 500
- resource records, DNS 499, 506–507, 513–525
  - A 519
  - AAAA 519
  - CNAME 522
  - DKIM 525
  - DMARC 525
  - DNSKEY 558
  - DS 558
  - MX 521
  - NS 518
  - NSEC 558
  - NSEC3 558
  - PTR 520
  - quad A 519
  - RRSIG 558
  - SOA 516
  - special characters in 514
  - SPF 525
  - SRV 523
  - TXT 524
  - types 515
- REST (Representational State Transfer) 693
- **/etc/postfix/restricted_recipients** file 669
- reverse proxy, web server 688
- reverse zone, DNS 502
- revision control 235–240, 952
- RFC1918 addresses 392–394, 541
- RFC (Request for Comments) 17, 377
- RHEL 8, 10
- RHN (Red Hat Network) 167, 169
- Richards, Martin 1167

ripd daemon 493
RIPE DNSSEC tools 567
RIPE NCC 392
ripngd daemon 493
RIPng (Routing Information Protocol, next generation) 486, 488
RIP (Routing Information Protocol) 486, 488
risk assessment 1119, 1130
Ritchie, Dennis 1167
Rivest, Ron 1007
RJ-45 wiring standard 464
rm command 128
rmdir command 129
rmuser command 262–263, 265
rndc command 540–541, 549
/etc/rndc.conf file 540
rndc-confgen command 540
/etc/rndc.key file 540
Role-Based Access Control (RBAC) 85, 259
root account 248
  see also RBAC
  best practices 69
  disabling 78
  management of 69
  user ID 67
root.cache file 539
/root directory 126
root filesystem 36, 38, 743
rootkits 990
root server hints, DNS 539
root servers, DNS 506, 539
root shell 41
rotation, log file 319–321
round robin DNS 508–509
route command 414
routed daemon 492
routing, network 398–401, 481–496
  adding 414
  Cisco routers 494–496
  configuration 414–415
  cost metrics 487
  daemons 485–488, 492–494
  default 415, 421, 426
  default routes 483, 491
  deleting 414
  distance-vector 486
  link-state 487
  multicast 490
  next hop 482
  protocols 485–488
routing, network *continued*
  redirects 401–403, 485
  static 400, 485, 490
  strategy 490–492
  table 484
  tables 399–401
RPC 795
rpc.idmapd daemon 811
rpm command 21, 164
RRDtool 1058
RRSIG DNS records 558
RSA conference 20
RSA public key cryptosystem 1007
rsync command 594
/etc/rsyslog.conf file 304
rsyslog.conf file 314–317
rsyslogd daemon 303
  architecture 304
  configuration 305–314, 314–317
  legacy configuration options 312
  message properties 313
  versions 304
RT: Request Tracker 1114
Ruby language 7, 187, 223–229, 691
  as a filter 229
  best practices 230–231
  blocks 225–227
  environment management 232–235
  hashes 227
  installation of 223
  package management 229–230
  regular expressions 227–229
  symbols 227
  vs. Python 223
runaway processes 107–109
/run directory 126
/var/run directory 126
run levels, **init** 43, 50
rvm environment manager 232–235

S

SaaS (Software as a Service) 276
Safari Books Online 17
Safe Harbor 1129
SAGE-AU 1134
SailPoint IdentityIQ 268
Salt 841, 844, 850, 871–893, 1109
  comments on 850
  comparison to Ansible 893–895
  debugging 892
  dependencies 880–882
  and Docker 943
  documentation 892–893
  environments 888
  formulas 887–888
  functions 882–883
  globbing 876
  highstates 886–887
  installation of 871–873
  and Jinja 878–880
  matching, minion 876–877
  parameters 883–885
  pillars 872
  ports, network 873
  pros and cons 896
  security 873, 894
  setup, minions 873
  .sls files 874
  state binding, minions 886
  state IDs 880–882
  states 872, 877–878
  variables, minions 874–876
salt command 874
/srv/salt directory 872
salt-key command 874
salt-master daemon 872, 873, 874
salt-minion daemon 873
Salt Open 871
SaltStack 871
Samba 820–829
  see also SMB (Server Message Block)
  and AD 820, 822–823
  browsing shares 826
  character sets 829
  configuring shares 823–827
  debugging 827–829
  group permissions 824–825
  installation of 821
  local authentication 822
  logging 828
  mounting shares 825–826
  security 826–827
/var/log/samba/* file 297
SAML (Security Assertion Markup Language) 578
SANS (SysAdmin, Audit, Network, Security) Institute 1035, 1134, 1171

Sarbanes-Oxley Act (SOX) 259, 1032, 1127, 1130
sar command 1057, 1072, 1086
SAS (Serial Attached SCSI) interface 731–732
  formatting, disk 736
SATA (serial ATA) interface 730
  formatting, disk 736
  secure erase 737
Satellite Server 167
savecore command 359
saved GID 67
saved UID 67
/sbin directory 125, 126
/usr/sbin directory 126
SCALE conference 20
Schneier, Bruce 993, 1006, 1035
Schroeder, Bianca 727
scientific method 1076
scp command 1016, 1027
scripting 182–242
  see also **bash**
  see also Perl
  see also Python language
  automation 184–185
  choosing a language 186–187
  error messages, useful 188
  languages 7
  microscripts 183–184
  philosophy 183–188
  style 188
SCSI (Small Computer System Interface) 731–732
SDN (Software-Defined Networking) 473
search path 21
second-level domain name 503
SecOps 1061
Secret Server 994
/var/log/secure file 297
Secure Hash Algorithm (SHA-1, SHA-2, SHA-3) 1010
Secure Sockets Layer (SSL) 681, 1009
security
  see also cryptography
  access control 65–68
  aging, password 995
  and Ansible 870, 894
  architecture 1028
  attack response 1004
  attack surface 987
  auditing 999

security *continued*
  authentication, public key 1019–1020
  and automation 987
  AWS 450–455
  and backups 989
  basic measures 987–992
  Blowfish hash 248
  boot loader 986
  botnets 985
  broadcast ping 425
  buffer overflows 984
  certifications 1031–1034
  chain of trust, DNSSEC 564
  CIA triad 983
  configuration errors 986–987
  credit card data 1129
  of credit cards *see* PCI DSS (Payment Card Industry Data Security Standard)
  data loss prevention (DLP) 608
  DDoS 985
  defense in depth 987
  deleting accounts 264
  demoting data 955
  DES hash 248
  disk erasure 737–738
  DMZ 1029
  DNS 551–568
  DNSSEC 557–568
  and Docker 921, 939–941
  elements of 983
  encryption 1009, 1019–1020
  event logging 989
  of Exim 642
  file integrity monitoring 1061
  file transfer, secure 1027
  firewall, Linux or UNIX as a 440–448
  firewalls 1027–1030
  group logins 996
  handling attacks 1037–1038
  hash, cryptographic 1009–1011
  home directory permissions 259
  and HTTP 676
  ICMP redirects 425
  incident handling 1037–1038
  incident hotline 1038
  insider abuse 986
  intrusion detection 1000–1004, 1062–1064

security *continued*
  IoT 985, 1174
  IP forwarding 425
  and IP networking 406–410
  IPsec 1030
  Kerberos 81
  least privilege 987
  and load balancing 686
  locking accounts 78, 265–266
  malware 984
  MD5 hash 246
  monitoring 1061–1063
  multifactor authentication 991
  NFS 793–794, 798–799, 810
  of open source software 1012
  open vs. closed operating systems 985
  packet filtering 991
  passphrase 993
  password cracking 1000
  password expiration 250, 252
  password hashes 245, 246–248
  passwords 992–996
  passwords, obsolescence of 991
  password strength 247, 993
  patching schedule 988
  penetration testing 992, 999
  phishing 984, 1131
  port scanning 996–998
  of Postfix 661
  power tools 996–1004
  privileged ports 386, 997, 1028
  and random numbers 1011
  removing accounts 264
  root account 248, 996
  root account, disabling 78
  rootkits 990
  and Salt 873, 894
  and Samba 826–827
  of search paths 70
  self-assessments 991
  SELinux 83, 85
  of **sendmail** 632–638
  SHA-512 hash 246
  shell, secure (ssh) 1016–1027
  and SNMP 1065
  social engineering 983–984
  source routing 425
  sources of compromise 983–987
  sources of information on 1034–1036
  spear phishing 984

security *continued*
- standards 1031–1034, 1123
- **sudo** command 70
- of syslog messages 317
- system accounts, non-root 78–80
- of TCP/IP 482, 485
- TrustedBSD 83
- unnecessary services 988
- updates, software 987
- vigilance 991–992
- viruses 989–990
- VPN 409–411, 1030
- vs. convenience 982
- vulnerabilities, software 984–985
- vulnerability scanning 998–999
- of wireless networks 473
- worms 989–990

Security Assertion Markup Language (SAML) 578
SecurityFocus 1035
security incidents 1122
SecuritySpace 612
Seeley, Donn 1171
segmentation violation 95
segment, TCP 381
SEGV signal 95
Selenium 958
/etc/selinux directory 87
SELinux (Security-Enhanced Linux) 83, 85
Sender ID 606
Sender Policy Framework (SPF) 601, 606
sendmail 612, 613–640
- *see also* aliases, email
- *see also* email
- *see also* spam
- blacklists 630
- and **chroot** 636
- command line flags 615
- configuration 617–624
- daemon mode 615
- databases 620–621
- directory locations 614
- and LDAP 624
- load average limit 628
- logging 639–640
- **m4** and 613–614
- masquerading 625–626
- open relay 628, 629
- permissions 634–635

sendmail *continued*
- privacy 628, 635–636
- queue monitoring 638
- queue processing 615
- queues 616
- rate and connection limits 628
- sample configuration 619
- security 632–638
- and the service switch file 614
- starting 615
- testing and debugging 638–640

sendmail.cf file 616, 617
Sensu 1047
Server Fault 19
serverless, cloud 282
server mode 41
ServiceDesk 1114
Service Level Agreement (SLA) 1125–1127
ServiceNow 1114
/etc/services file 386, 1028
setfacl command 142–152
setgid bit 249
setgid execution 68
setrlimit system call 1090
setuid execution 68, 92
setuid/setgid bits 68–69, 133
sfdisk command 719
sftp command 1016, 1027
sftp-server command 1016
sg_format command 736
SHA-1, SHA-2, SHA-3 (Secure Hash Algorithm) 1010
SHA-512 hashing algorithm 246
/etc/shadow file 68, 245, 250–252, 995
shadow passwords 251–252, 252–254
Shamir, Adi 1007
Shapiro, Greg 638
/usr/share directory 126
shares, NFS 796
sharing a filesystem *see* NFS
shell, root 41
shell scripting 189–198
Shibboleth 267
showmount command 807
shred command 737
sh shell 186
- *see also* **bash**
- arithmetic 209–210
- command-line arguments 203–205

sh shell *continued*
- comparison operators 205
- control flow 205–206
- execution of 198–199
- file evaluation 206
- functions 203–205
- globbing 13, 209
- I/O 201–202
- loops 207–208
- scripting 198–209

shutdown command 59, 61
shutdown procedures 59
Shuttleworth, Mark 10
Siemon 479, 480
SignalFx 1050
signals 94–96
- BUS 95
- caught, blocked, or ignored 95
- CONT 95, 96
- HUP 95, 96
- INT 95, 96
- KILL 95, 96
- list of important 95
- QUIT 95, 96
- SEGV 95
- sending 97
- STOP 95, 96
- TERM 95, 96
- tracing 105–107
- TSTP 95, 96
- USR1 95
- USR2 95
- WINCH 95

Silicon Graphics, Inc. 764
Simple Mail Transport Protocol *see* SMTP
single-mode fiber 464
single-user mode 38, 41, 60, 61–63
- cloud instances 62–63
- FreeBSD 62
- Linux 61–63
- remounting the root filesystem 61

Site Reliability Engineer (SRE) 27
/etc/skel directory 258, 261
SLAAC (StateLess Address Auto-Configuration) 397
Slack 1108
Slackware Linux 8
/etc/openldap/slapd.conf file 583
slapd daemon 583
SLA (Service Level Agreement) 1125–1127

slices *see* partitions, disk
slurpd daemon 583
smartctl command 739
smartd daemon 739
`SMART_HOST` macro **sendmail** 626
SMART (self-monitoring, analysis, and reporting technology) 738–740
/usr/local/etc/smb4.conf file 821
smbclient command 826
/etc/samba/smb.conf file 821
smbd daemon 820–821
smbpasswd command 822
SMB (Server Message Block) 819–829
  history of 819–820
  vs. NFS 792, 821
smbstatus command 827
S/MIME email encryption 607
SmokePing 437
smrsh command 634
SMS notifications 1043
SMTP 603
  authentication 604
  commands 603
  debugging 604
  error codes 604
  status messages 604
smtpd daemon 659
`smtpd_recipient_restrictions` option, Postfix 669, 670
smtpd_*_restrictions options, Postfix 668
`smtpd_sasl_auth_enable` option, Postfix 670
smtpd_tls_* options, Postfix 670
`smtp` transport, Exim 656
smurf attacks 407, 424
snapshots, volume 750–751
SNI (Server Name Indication) 682
snmpd.conf file 1066
snmpd daemon 1064, 1065–1069
snmpdelta command 1066
snmpdf command 1066
/etc/snmp directory 1066
snmpget command 1066
snmpgetnext command 1066
snmpset command 1066
SNMP (Simple Network Management Protocol) 1056, 1063–1067
  agents 1064
  community string 1065
SNMP *continued*
  graphing 439–440
  MIB 1064
  organization 1064
  protocol operations 1065
  traps 1065
snmptable command 1066
snmptranslate command 1066
snmptrap command 1066
snmpwalk command 1066
Snort network intrusion detection system 1001
Snowden, Edward 981
SOAP (Simple Object Access Protocol) 693
SOA (Start of Authority) DNS records 516
social coding 239–241
sockets, local domain 128, 131
socket system call 131
`soft_bounce` option, Postfix 671
software
  see also software packages
  installation from source code 23–24
  installing from a web script 24
  package management 21–23
Software as a Service (SaaS) 276
Software-Defined Networking (SDN) 473
software delivery 5
software packages
  see also software
  localization 178–181
  management 162–164
Solaris 11
SolarWinds 1050
Sony 990
sort command 194
/etc/apt/sources.list file 171
SOX (Sarbanes-Oxley Act) 1130
spam
  see also email
  blacklists 630
  cloud-based services 606
  open relay 628, 629
  Sender ID 606
  and **sendmail** 628–632
  SPF (Sender Policy Framework) 601
spear phishing 984
spectrum allocation, wireless 471
SPF (Sender Policy Framework) 601, 606
SPF (Sender Policy Framework) DNS records 525
splattercast 529
split DNS 541
/var/spool directory 126
`SPOOL_DIRECTORY` variable, Exim 641
Spotify 692
Squid caching server 689
/usr/src directory 126
SRE (Site Reliability Engineer) 27
/srv directory 126
SRV DNS records 523
ss command 418, 988, 1074
SSD (Solid State Disk) 717, 721–722, 725–728, 1073, 1084
SSH 1016–1027
  agent 1020–1021
  aliases, host 1022
  client 1018–1019
  connection multiplexing 1023
  essentials 1016–1018
  file transfer 1027
  keys 1019–1020
  password authentication, disabling 1022
  port 1022
  port forwarding 1023
  server 1024–1026
  SSHFP verification 1026
ssh-add command 870, 1016, 1020
ssh-agent command 870, 1016
ssh-agent daemon 1020
ssh command 1016–1027, 1018–1019
ssh_config file 1017
sshd_config file 996, 1010, 1017, 1025–1026
sshd daemon 843, 1016, 1024–1026
/etc/ssh directory 1017
~/.ssh directory 1018
SSHD (solid state hybrid drive) 728
SSHFP DNS record 1026
SSHFP host key verification 1026
ssh-keygen command 1016, 1019
ssh-keyscan command 1016
SSIDs, wireless 471
SSL (Secure Sockets Layer) 681, 1009

- SSO (Single Sign-On) 578–595
  - *see also* LDAP
  - account management 266–269
  - for applications 267
  - concepts 578
  - elements of 579
  - and Kerberos 586–589
  - LDAP 580–586
  - PAM 579
  - and SaaS 578
  - SAML 578
- **sssd.conf** file 589
- **sssd** daemon 579, 587–589, 589, 823
- Stack Overflow 19
- staging environment 954
- standard error 190
- standard input 190
- standard output 190
- standards
  - *see also* IEEE standards
  - CJIS (Criminal Justice Information Systems) 1128
  - COBIT 1128
  - Common Criteria 1034
  - contingency planning 1130
  - Critical Infrastructure Protection (CIP) 1129
  - Family Educational Rights and Privacy Act (FERPA) 1128
  - Federal Information Security Management Act (FISMA) 1128
  - FISMA 1032
  - Gramm-Leach-Bliley Act (GLBA) 1129
  - Health Insurance Portability and Accountability Act (HIPAA) 1032, 1129
  - IEEE 802.1* 460, 467, 468, 469, 470
  - Information Technology Infrastructure Library (ITIL) 1130
  - ISO 27001:2013 1032, 1123, 1129
  - ISO 27002:2013 1129
  - NERC CIP 1032
  - NIST SP 800-34 1120, 1130
  - NIST SP 800-53 1130
  - NIST SP 800 series 1033
  - OWASP 1034
- standards *continued*
  - Payment Card Industry Data Security Standard (PCI DSS) 1129
  - PCI DSS 1033
  - Red Flag Rule 1130
  - RJ-45 wiring 463
  - Safe Harbor 1129
  - Sarbanes-Oxley Act (SOX) 1130
  - security 1031–1034
  - TIA/EIA-568A 463
  - TIA/EIA-606-B 476
  - wireless 469
  - wiring 475
- standard services 386
- Stanford Law School 1008
- STARTTLS extension, **sendmail** 637
- startup scripts 57
- **statd** daemon 798
- stateful inspection firewalls 1029
- State University of New York (SUNY) Buffalo 1170
- static code analysis 958
- static routes 400, 490
- StatsD 1042, 1052–1054, 1054
- StatusCake 1051
- `STDERR` file descriptor 190
- `STDIN` file descriptor 190
- `STDOUT` file descriptor 190
- STD (Standard) 378
- sticky bit 134
- STOP signal 95, 96
- storage
  - block 281
  - ephemeral 281
  - layers of 740
  - object 281
- storage management *see* disks
- **/etc/carbon/storage-schemas.conf** file 1052
- **strace** command 105–107
- Stuxnet worm 981
- subdomains, DNS 503
- **submit.cf** file 617
- subnetting 388–389
- Subversion 962
- **su** command 70
- **sudo** command xli, 70–77, 992
  - configuration, example 71
  - configuration, site-wide 76
  - pros and cons 72
- **sudo** command *continued*
  - using with Ansible 854
  - using without password 75
  - using with Salt 877
  - vs. advanced access control 73
  - without a control terminal 76
- **/etc/sudoers** file 71–73
- Sumo Logic 323
- Sun Microsystems 911
- superblock, filesystem 764
- superuser *see* root account
- Supervisor 1060
- **supervisord** daemon 1060
- SUSE Linux 8
- **swapctl** command 771
- **swapon** command 768, 771, 1082
- **/proc/sys/vm/swappiness** parameter 1082
- swap space 770–771, 1081
- Swarm 947
- Sweet, Michael 361
- switches, Ethernet 465
- symbolic links 128, 131–132
- **sync** system call 765
- **/etc/sysconfig** directory 55, 419–421
- **sysctl** command 339, 344, 357, 427, 1056
- **/etc/sysctl.conf** file 339, 344, 424, 427
- Sysdig Cloud 1050, 1059
- **sysdig** tool 1057, 1058
- **/sys** directory 126, 332
- **/usr/src/sys** directory 345
- sysfs filesystem 332
- syslog 302–318
  - *see also* log files
  - *see also* logging
  - actions 310
  - and DNS logging 568–574
  - facility names 309
  - messages 303–304
  - security 317
  - severity levels 309
  - and **systemd** journal 301
- **/etc/syslog.conf** file 307–311
- **syslogd** daemon 303
- **/var/log/syslog*** file 297
- system administration
  - adjacent disciplines 26–28
  - conferences 19
  - essential tasks 4–7
  - GUI tools 7

- system administration *continued*
  - keeping current 18
  - metrics 1127
  - prioritization 1126–1127
  - resources for reading about 18
  - service descriptions 1125–1135
- system administrator
  - and CI/CD 950
  - common tasks 1124
  - distinguishing characteristics 1040
  - history 1169–1170
  - localization guidelines 178–179
  - professional attributes of 1040
  - responsibilities 1110
  - role in DevOps 1110
  - roles 1115
  - tool box 1103
- `SYSTEM_ALIASES_FILE` variable, Exim 641
- system calls, tracing 105
- **system-config-kickstart** tool 156
- **systemctl** command 46–47, 61
- **systemd** daemon 30–31, 43, 44–57, 93, 971
  - and **init** scripts 55
  - caveats 54
  - dependencies 50–51
  - and Docker 932
  - execution order 51
  - journal 295, 298–299, 299–302
  - logging 56
  - management of 46–47
  - targets 49–50, 50
  - timers 113–117
  - unit files 45
  - unit statuses 47–49
  - vs. **init** 43
- **systemd-journald** daemon 299–302, 319
- **systemd-journal-remote** tool 301
- System V UNIX 1169

T

- **tail** command 196
- tape, magnetic 789–790
- targets, **systemd** 50
- task management 1111
- T-BERD line analyzer 474
- **tcpdump** tool 434–437, 675
- TCP/IP 378
  - *see also* IP
  - *see also* IPv6
  - *see also* networking
  - connection reuse 680
  - Fast Open (TFO) 680
- **tcsh** shell 189
- technical debt 1105
- **tee** command 196
- Teleport 1027
- **telinit** command 61
- temperature
  - data center 1096
  - effect on hard disks 723
- TERM signal 95, 96
- Terraform 282, 452–455, 965, 973–975
- **terraform** command 453
- **/bin/test** command 205
- testing
  - acceptance 958
  - infrastructure 958
  - integration 958
  - performance 958
  - software localization 180–181
  - static code analysis 958
  - unit 958, 966–967
- **testparm** command 821
- TFO (TCP Fast Open) 680
- The Open Group 268
- Thompson, Ken 1166
- ThoughtWorks 949
- threads 91, 97–109
- threat categories, disaster 1119
- Thycotic 994
- TIA/EIA-568A wiring 464
- ticket-granting ticket, Kerberos 587
- ticketing 1111
- ticketing systems 1114
- time-to-live field, IP 431
- TLS (Transport Layer Security) 632, 637, 681, 1009
- **/tmp** directory 125, 126
- **/usr/tmp** directory 126
- **/var/tmp** directory 126
- **/tmp** filesystem 743
- token ring 381
- toolbox 1103
- TO_* options, **sendmail** 628
- **top** command 101–102, 1075, 1089
- Torvalds, Linus 18, 235, 1172
- Townsend, Jennine 68
- **traceroute** command 430, 431–434
- Track-It! 1114
- Transport Layer Security (TLS) 409, 632, 637, 681, 1009
- Tridgell, Andrew 820
- Tripwire 1062
- Troan, Erik 319
- Troposphere 282
- troubleshooting
  - *see also* performance
  - Amazon Web Services (AWS) instances 63
  - BIND 568–576
  - booting 60–61
  - cloud systems 62–63
  - DigitalOcean instances 63
  - DNS 568–576
  - Docker 942–944
  - Exim 658
  - Google Compute Engine (GCE) instances 64
  - HTTP connections 675, 679–680
  - kernel 356–359
  - network 428–436, 474–475
  - performance 1088–1090
  - Postfix 670
  - printing 369–371
  - Salt 892
  - Samba 827–829
  - **sendmail** 638
  - SMTP 604
  - syslog 318–319
  - TLS servers 1014
  - web caching 688
- Trump, Donald J. 607
- trunks, Ethernet 467
- **truss** command 105–107
- TrustedBSD 83
- **tshark** command 436
- Ts'o, Theodore 764
- TSTP signal 95, 96
- TTL (time-to-live), DNS 508
- **tugboat** cli tool 289, 456
- **tune2fs** command 767
- **tunefs** command 769
- Tweedie, Stephen 764
- Twofish 1006
- TXT DNS records 524
- typographical conventions 12–13

U

UA (mail User Agent) 597
UBER (Uncorrectable Bit Error Rate) 728
Ubiquiti 472
Ubuntu Linux 8, 10
udevadm command 331, 333, 335
/etc/udev/udev.conf file 334
udevd daemon 331, 334–337
UDP (User Datagram Protocol) 378
UEFI (Unified Extensible Firmware Interface) 32, 33–35
  bootstrap path 34, 39
UFS filesystem 763–771
ufw command 441, 991, 1028
UIDs *see* user IDs
ulimit command 1090
umask command 138
umask, default 253, 258
umount command 123–124, 768
uname command 327, 346, 923
Uncorrectable Bit Error Rate (UBER) 728
unicast, IP 386
unicast packets 461
unicast Reverse Path Forwarding (uRPF) 408
Uniform Resource Locators (URLs) 675–676
uninterruptible power supplies 1092–1093
uniq command 195
United Nations 376
units 13–14
unit tests 958, 966–967
Universal Plug and Play (UPnP) 394
Universal Serial Bus (USB) interface 732–733
University of California at Berkeley 946, 1168
University of Cambridge 612, 640, 906
University of Colorado at Boulder xl, 1170
University of Maryland 1170
University of Utah 1170
UNIX
  see also FreeBSD
  as a firewall 409, 440–448
  history of 1166–1168
  origin of name 1167
  philosophy 1168
  reasons to choose 1071
UNIX *continued*
  security of 982
  and viruses 989
unlink system call 131
unshielded twisted pair *see* UTP cables
unsolicited commercial email *see* spam
updatedb command 21
updates, software 987–988
uptime command 1041, 1054, 1080, 1089
Uptime Institute, The 1101–1102
/dev/urandom device 330, 1012
URI (Uniform Resource Identifier) 675
URLs (Uniform Resource Locators) 675–676
URN (Uniform Resource Name) 675
uRPF (unicast Reverse Path Forwarding) 408
USB drive mounting 770
USB (Universal Serial Bus) interface 732–733
U.S. Department of Defense 376
`use_cw_file` feature, **sendmail** 622
USENIX Association 1134, 1171
user accounts 243–269
  adding 255–260, 260–264
  attributes 250–252
  centralized management 266–269
  defaults 253–254
  deleting 260–264, 264
  encrypted passwords 246
  GECOS field 245, 249
  GID 245, 249
  home directory 250, 257–259, 259
  identity management 268–269
  idle timeout 253
  locking 78, 265–266
  login name 245–246
  login shell 250
  nobody 800
  password algorithm 247
  password expiration 251
  password quality 247
  passwords 992–996
  password, setting 257
  password strength 247
  pseudo-accounts 79–80
user accounts *continued*
  RBAC 259
  removing 260–264, 264
  shadow passwords 251–252
  startup files 258
  UID 245, 248
  umask 253, 258
useradd command 255, 261–262
/etc/default/useradd file 261
userdel command 265
userdel.local script 265
user IDs 92, 244, 245, 248
  mapping to names 67
  real, effective, and saved 67
usermod command 251, 265
usernames *see* user accounts
USR1 signal 95
USR2 signal 95
/usr directory 125, 126
UTP cables 460, 462, 475
UUID 770

V

Vagrant 913
van Rossum, Guido 187
/var directory 125, 126, 743
variables, environment 193–194
Varnish caching server 689
vault, password 993–995
VAX 1169
Velocity conference 20
vendors we like 479
Venema, Wietse 612, 658
VeriSign 1007
Veritas 748
Verizon Data Breach Investigations Report 1035
vgchange command 748
vgck command 748
vgcreate command 748, 749
vgdisplay command 748, 751
vgextend command 748
vgscan command 748
Viavi 474, 480
vi command 7
vigr command 257
.viminfo file 258
.vimrc file 258
vipw command 247, 252, 256
virsh command 909
virt-install command 907–908, 909–910

virt-manager package 907–908
virtual_alias_* options, Postfix 666
VirtualBox 911
virtualenv package 232
virtual hosts, web server 681–683
- in **httpd** 681–683
- in NGINX 705

virtualization 900–914
- *see also* KVM
- *see also* Xen
- containerization 904–905
- on FreeBSD 910
- full 901–902
- hardware-assisted 902
- HVM (Hardware Virtual Machine 902
- hypervisors 901–904
- images 904, 911–913
- on Linux 905–910
- live migration 904
- paravirtualization 902
- provisioning 913
- PVH (ParaVirtualized Hardware) 903
- PVHVM (ParaVirtualized HVM) 903
- QEMU 903
- type 1 vs. type 2 903–904
- vs. containers 906

virtual_mailbox_* options, Postfix 667
Virtual Private Network (VPN) 409–411, 1030
virtual private servers 279
`virtusertable` feature, **sendmail** 624
/etc/mail/virtuserable file 624
viruses 989–990
virus scanning
- *see also* email

Visa 1033
visudo command 72
Vixie, Paul 529
VLANs 466
- trunking 467
- wireless 471

vmstat command 1057, 1072, 1075, 1079–1080, 1089
VMware 910
VMware ESXi 904
VMware Identity Manager 268
VMware vCloud Air 273
VMware Workstation 904
VMWorld conference 20
volume groups 748
- relations to other layers 740–742

VPN (Virtual Private Network) 409–411, 1030–1031
vtysh daemon 493
vulnerabilities, software 984–985
vulnerability scanning 998–999

W

Wall, Larry 187
Watson, Robert 83
wc command 196
web hosting 682–694
- APIs 692–694
- architecture 683, 685
- build vs. buy 694
- cache 686
- in the cloud 694
- components 683
- proxy server 688
- reverse proxy 688
- serverless 696
- server types 682
- static content 695
- TCP connection reuse 680
- virtual hosts 681–683

Well-Known Service (WKS) ports 1028
wget command 24
wheel group 70, 249
whereis command 21
which command 21
Whisper 1049
Wi-Fi networks 470
Wi-Fi Protected Access (WPA) 473
WINCH signal 95
Windows Defender 990
Wired Equivalent Privacy (WEP) 473
wireless networks 469–473
- access points (APs) 471
- channels 471
- frequency spectrum 471
- security 473
- SSIDs 471
- topology 471
- VLANs 471

Wireshark 434–437
wiring, building 475
wisdom, Evi's tenets of xli
World Wide Web Consortium 268
worms 989–990
WPA *see* Wi-Fi Protected Access
wpa_supplicant command 470
write hole, RAID 5 753, 758
/var/log/wtmp file 297, 298

X

X.500 directory service 580
Xen 902, 906–907
- *see also* virtualization
- components 907
- dom0 906
- guest installation 907–908
- overhead 906
- virtual block devices (VBDs) 907

/etc/xen directory 907
/var/log/xen/* files 297
XenServer 904
XFS filesystem 763–771
xfs_growfs command 752
xl tool 908
XML (Extensible Markup Language) 692
/var/log/Xorg.n.log file 297
XORP (eXtensible Open Router Platform) 494

Y

YAML 845, 850–852, 878–880
Ylönen, Tatu 1016
yum command 22, 164, 166, 167, 174–175
/var/log/yum.log file 297

Z

zebra daemon 493
Zenoss 1050, 1110
/dev/zero file 330
zero downtime deployment 960–961
zfs command 775, 776
ZFS filesystem 742, 756, 772–773, 773–783
- clones 779–780
- disk addition 775–776
- and Docker 930

ZFS filesystem *continued*
inheritance, property 777
and Linux 774
properties, filesystem 776–777
RAID 775
raw volumes 780–781
snapshots 779–780
spare disks 783
storage pool 774, 781–783
vs. Btrfs 783–784
Zimmermann, Phil 1014
Zix 608
zombie processes 98
zones, DNS 502
forward 502
forwarding 539
localhost 543, 544
master 537
reverse 502, 520, 521
signing 562
slave 538
transfers 548
zpool command 775, 776
Zulip 1108