

Table of Contents

Tribute to Evi	xl
Preface	xliv
Foreword	xlv
Acknowledgments	xlvi

SECTION ONE: BASIC ADMINISTRATION

Chapter 1 Where to Start	3
Essential duties of a system administrator	4
Controlling access	4
Adding hardware	4
Automating tasks	4
Overseeing backups	4
Installing and upgrading software	5
Monitoring	5
Troubleshooting	5
Maintaining local documentation	5
Vigilantly monitoring security	6
Tuning performance	6
Developing site policies	6
Working with vendors	6
Fire fighting	6

Suggested background	7
Linux distributions	8
Example systems used in this book	9
Example Linux distributions	10
Example UNIX distribution	11
Notation and typographical conventions	12
Units	13
Man pages and other on-line documentation	14
Organization of the man pages	14
man : read man pages	15
Storage of man pages	15
Other authoritative documentation	16
System-specific guides	16
Package-specific documentation	16
Books	17
RFC publications	17
Other sources of information	18
Keeping current	18
HowTos and reference sites	19
Conferences	19
Ways to find and install software	19
Determining if software is already installed	21
Adding new software	22
Building software from source code	23
Installing from a web script	24
Where to host	25
Specialization and adjacent disciplines	26
DevOps	26
Site reliability engineers	27
Security operations engineers	27
Network administrators	27
Database administrators	27
Network operations center (NOC) engineers	27
Data center technicians	28
Architects	28
Recommended reading	28
System administration and DevOps	28
Essential tools	29

Chapter 2 Booting and System Management Daemons 30

Boot process overview	30
System firmware	32
BIOS vs. UEFI	32
Legacy BIOS	33
UEFI	33
Boot loaders	35
GRUB: the GRand Unified Boot loader	35
GRUB configuration	36
The GRUB command line	37
Linux kernel options	38
The FreeBSD boot process	39
The BIOS path: boot0	39
The UEFI path	39
loader configuration	40
loader commands	40
System management daemons	41
Responsibilities of init	41
Implementations of init	42
Traditional init	43
systemd vs. the world	43
inits judged and assigned their proper punishments	44
systemd in detail	44
Units and unit files	45
systemctl : manage systemd	46
Unit statuses	47
Targets	49
Dependencies among units	50
Execution order	51
A more complex unit file example	52
Local services and customizations	53
Service and startup control caveats	54
systemd logging	56
FreeBSD init and startup scripts	57
Reboot and shutdown procedures	59
Shutting down physical systems	59
Shutting down cloud systems	59
Stratagems for a nonbooting system	60
Single-user mode	61
Single-user mode on FreeBSD	62
Single-user mode with GRUB	62
Recovery of cloud systems	62

Chapter 3	Access Control and Rootly Powers	65
Standard UNIX access control	66	
Filesystem access control	66	
Process ownership	67	
The root account	67	
Setuid and setgid execution	68	
Management of the root account	69	
Root account login	69	
su : substitute user identity	70	
sudo : limited su	70	
Example configuration	71	
sudo pros and cons	72	
sudo vs. advanced access control	73	
Typical setup	74	
Environment management	74	
sudo without passwords	75	
Precedence	75	
sudo without a control terminal	76	
Site-wide sudo configuration	76	
Disabling the root account	78	
System accounts other than root	78	
Extensions to the standard access control model	79	
Drawbacks of the standard model	80	
PAM: Pluggable Authentication Modules	80	
Kerberos: network cryptographic authentication	81	
Filesystem access control lists	81	
Linux capabilities	82	
Linux namespaces	82	
Modern access control	83	
Separate ecosystems	84	
Mandatory access control	84	
Role-based access control	85	
SELinux: Security-Enhanced Linux	85	
AppArmor	87	
Recommended reading	89	
Chapter 4	Process Control	90
Components of a process	90	
PID: process ID number	91	
PPID: parent PID	91	
UID and EUID: real and effective user ID	92	
GID and EGID: real and effective group ID	92	
Niceness	93	
Control terminal	93	

The life cycle of a process	93
Signals	94
kill : send signals	97
Process and thread states	97
ps : monitor processes	98
Interactive monitoring with top	101
nice and renice : influence scheduling priority	102
The /proc filesystem	104
strace and truss : trace signals and system calls	105
Runaway processes	107
Periodic processes	109
cron : schedule commands	109
The format of crontab files	110
Crontab management	112
Other crontabs	112
cron access control	113
systemd timers	113
Structure of systemd timers	114
systemd timer example	114
systemd time expressions	116
Transient timers	117
Common uses for scheduled tasks	118
Sending mail	118
Cleaning up a filesystem	118
Rotating a log file	118
Running batch jobs	118
Backing up and mirroring	119

Chapter 5 The Filesystem

120

Pathnames	122
Filesystem mounting and unmounting	122
Organization of the file tree	125
File types	126
Regular files	129
Directories	129
Hard links	129
Character and block device files	130
Local domain sockets	131
Named pipes	131
Symbolic links	131

File attributes.....	132
The permission bits.....	132
The setuid and setgid bits.....	133
The sticky bit.....	134
ls : list and inspect files.....	134
chmod : change permissions.....	136
chown and chgrp : change ownership and group.....	137
umask : assign default permissions.....	138
Linux bonus flags.....	139
Access control lists.....	140
A cautionary note.....	141
ACL types.....	141
Implementation of ACLs.....	142
Linux ACL support.....	142
FreeBSD ACL support.....	143
POSIX ACLs.....	143
Interaction between traditional modes and ACLs.....	144
POSIX access determination.....	146
POSIX ACL inheritance.....	146
NFSv4 ACLs.....	147
NFSv4 entities for which permissions can be specified.....	148
NFSv4 access determination.....	149
ACL inheritance in NFSv4.....	149
NFSv4 ACL viewing.....	150
Interactions between ACLs and modes.....	151
NFSv4 ACL setup.....	151

Chapter 6 Software Installation and Management 153

Operating system installation.....	154
Installing from the network.....	154
Setting up PXE.....	155
Using kickstart, the automated installer for Red Hat and CentOS.....	156
Setting up a kickstart configuration file.....	156
Building a kickstart server.....	158
Pointing kickstart at your config file.....	158
Automating installation for Debian and Ubuntu.....	159
Netbooting with Cobbler, the open source Linux provisioning server....	161
Automating FreeBSD installation.....	161
Managing packages.....	162
Linux package management systems.....	164
rpm : manage RPM packages.....	164
dpkg : manage .deb packages.....	166

High-level Linux package management systems	166
Package repositories	167
RHN: the Red Hat Network	169
APT: the Advanced Package Tool	169
Repository configuration	170
An example <code>/etc/apt/sources.list</code> file	171
Creation of a local repository mirror	172
APT automation	173
yum : release management for RPM	174
FreeBSD software management	175
The base system	175
pkg : the FreeBSD package manager	176
The ports collection	177
Software localization and configuration	178
Organizing your localization	179
Structuring updates	179
Limiting the field of play	180
Testing	180
Recommended reading	181
 Chapter 7 Scripting and the Shell	 182
Scripting philosophy	183
Write microscripts	183
Learn a few tools well	184
Automate all the things	184
Don't optimize prematurely	185
Pick the right scripting language	186
Follow best practices	187
Shell basics	189
Command editing	190
Pipes and redirection	190
Variables and quoting	192
Environment variables	193
Common filter commands	194
cut : separate lines into fields	194
sort : sort lines	194
uniq : print unique lines	195
wc : count lines, words, and characters	196
tee : copy input to two places	196
head and tail : read the beginning or end of a file	196
grep : search text	197

sh scripting	198
Execution	198
From commands to scripts	199
Input and output	201
Spaces in filenames	202
Command-line arguments and functions	203
Control flow	205
Loops	207
Arithmetic	209
Regular expressions	209
The matching process	210
Literal characters	210
Special characters	210
Example regular expressions	211
Captures	213
Greediness, laziness, and catastrophic backtracking	213
Python programming	215
The passion of Python 3	215
Python 2 or Python 3?	216
Python quick start	216
Objects, strings, numbers, lists, dictionaries, tuples, and files	218
Input validation example	220
Loops	221
Ruby programming	223
Installation	223
Ruby quick start	224
Blocks	225
Symbols and option hashes	227
Regular expressions in Ruby	227
Ruby as a filter	229
Library and environment management for Python and Ruby	229
Finding and installing packages	229
Creating reproducible environments	230
Multiple environments	231
virtualenv : virtual environments for Python	232
RVM: the Ruby enVironment Manager	232
Revision control with Git	235
A simple Git example	236
Git caveats	239
Social coding with Git	239
Recommended reading	241
Shells and shell scripting	241
Regular expressions	241
Python	242
Ruby	242

Chapter 8 User Management 243

Account mechanics	244
The /etc/passwd file	245
Login name	245
Encrypted password	246
UID (user ID) number	248
Default GID (group ID) number	249
GECOS field	249
Home directory	250
Login shell	250
The Linux /etc/shadow file	250
FreeBSD's /etc/master.passwd and /etc/login.conf files	252
The /etc/master.passwd file	252
The /etc/login.conf file	253
The /etc/group file	254
Manual steps for adding users	255
Editing the passwd and group files	256
Setting a password	257
Creating the home directory and installing startup files	257
Setting home directory permissions and ownerships	259
Configuring roles and administrative privileges	259
Finishing up	260
Scripts for adding users: useradd , adduser , and newusers	260
useradd on Linux	261
adduser on Debian and Ubuntu	262
adduser on FreeBSD	262
newusers on Linux: adding in bulk	263
Safe removal of a user's account and files	264
User login logout	265
Risk reduction with PAM	266
Centralized account management	266
LDAP and Active Directory	267
Application-level single sign-on systems	267
Identity management systems	268

Chapter 9 Cloud Computing 270

The cloud in context	271
Cloud platform choices	273
Public, private, and hybrid clouds	273
Amazon Web Services	274
Google Cloud Platform	275
DigitalOcean	275

Cloud service fundamentals	276
Access to the cloud	277
Regions and availability zones	278
Virtual private servers	279
Networking	280
Storage	281
Identity and authorization	281
Automation	282
Serverless functions	282
Clouds: VPS quick start by platform	283
Amazon Web Services	283
aws : control AWS subsystems	284
Creating an EC2 instance	284
Viewing the console log	286
Stopping and terminating instances	287
Google Cloud Platform	288
Setting up gcloud	288
Running an instance on GCE	288
DigitalOcean	289
Cost control	291
Recommended Reading	293

Chapter 10 Logging 294

Log locations	296
Files not to manage	298
How to view logs in the systemd journal	298
The systemd journal	299
Configuring the systemd journal	300
Adding more filtering options for journalctl	301
Coexisting with syslog	301
Syslog	302
Reading syslog messages	303
Rsyslog architecture	304
Rsyslog versions	304
Rsyslog configuration	305
Modules	306
sysklogd syntax	307
Legacy directives	311
RainerScript	312
Config file examples	314
Basic rsyslog configuration	314
Network logging client	315
Central logging host	316
Syslog message security	317
Syslog configuration debugging	318

Kernel and boot-time logging.....	318
Management and rotation of log files	319
logrotate : cross-platform log management	319
newsyslog : log management on FreeBSD.....	321
Management of logs at scale	321
The ELK stack	321
Graylog.....	322
Logging as a service	323
Logging policies	323
Chapter 11 Drivers and the Kernel	325
Kernel chores for system administrators.....	326
Kernel version numbering.....	327
Linux kernel versions.....	327
FreeBSD kernel versions	328
Devices and their drivers.....	328
Device files and device numbers.....	329
Challenges of device file management.....	330
Manual creation of device files	331
Modern device file management	331
Linux device management.....	331
Sysfs: a window into the souls of devices.....	332
udevadm : explore devices.....	333
Rules and persistent names	334
FreeBSD device management	337
Devfs: automatic device file configuration	337
devd : higher-level device management.....	338
Linux kernel configuration	339
Tuning Linux kernel parameters.....	339
Building a custom kernel.....	341
If it ain't broke, don't fix it	341
Setting up to build the Linux kernel.....	341
Configuring kernel options	342
Building the kernel binary.....	343
Adding a Linux device driver	344
FreeBSD kernel configuration	344
Tuning FreeBSD kernel parameters.....	344
Building a FreeBSD kernel	345
Loadable kernel modules	346
Loadable kernel modules in Linux.....	346
Loadable kernel modules in FreeBSD	348
Bootting	348
Linux boot messages	349
FreeBSD boot messages	353

Booting alternate kernels in the cloud	355
Kernel errors	356
Linux kernel errors	356
FreeBSD kernel panics	359
Recommended reading	359
Chapter 12 Printing	360
CUPS printing	361
Interfaces to the printing system	361
The print queue	362
Multiple printers and queues	363
Printer instances	363
Network printer browsing	363
Filters	364
CUPS server administration	365
Network print server setup	365
Printer autoconfiguration	366
Network printer configuration	367
Printer configuration examples	367
Service shutoff	368
Other configuration tasks	368
Troubleshooting tips	369
Print daemon restart	369
Log files	369
Direct printing connections	370
Network printing problems	370
Recommended reading	371

SECTION TWO: NETWORKING

Chapter 13 TCP/IP Networking	375
TCP/IP and its relationship to the Internet	375
Who runs the Internet?	376
Network standards and documentation	376
Networking basics	378
IPv4 and IPv6	379
Packets and encapsulation	381
Ethernet framing	382
Maximum transfer unit	382

Packet addressing	384
Hardware (MAC) addressing	384
IP addressing	385
Hostname “addressing”	385
Ports	385
Address types	386
IP addresses: the gory details	387
IPv4 address classes	387
IPv4 subnetting	388
Tricks and tools for subnet arithmetic	390
CIDR: Classless Inter-Domain Routing	391
Address allocation	392
Private addresses and network address translation (NAT)	392
IPv6 addressing	394
IPv6 address notation	395
IPv6 prefixes	396
Automatic host numbering	397
Stateless address autoconfiguration	397
IPv6 tunneling	398
IPv6 information sources	398
Routing	398
Routing tables	399
ICMP redirects	401
IPv4 ARP and IPv6 neighbor discovery	401
DHCP: the Dynamic Host Configuration Protocol	402
DHCP software	403
DHCP behavior	404
ISC’s DHCP software	404
Security issues	406
IP forwarding	406
ICMP redirects	407
Source routing	407
Broadcast pings and other directed broadcasts	407
IP spoofing	408
Host-based firewalls	408
Virtual private networks	409
Basic network configuration	410
Hostname and IP address assignment	411
Network interface and IP configuration	412
Routing configuration	414
DNS configuration	415
System-specific network configuration	416

Linux networking	417
NetworkManager	417
ip : manually configure a network	418
Debian and Ubuntu network configuration	419
Red Hat and CentOS network configuration	419
Linux network hardware options	421
Linux TCP/IP options	422
Security-related kernel variables	424
FreeBSD networking	425
ifconfig : configure network interfaces	425
FreeBSD network hardware configuration	426
FreeBSD boot-time network configuration	426
FreeBSD TCP/IP configuration	427
Network troubleshooting	428
ping : check to see if a host is alive	429
traceroute : trace IP packets	431
Packet sniffers	434
tcpdump : command-line packet sniffer	435
Wireshark and TShark: tcpdump on steroids	436
Network monitoring	437
SmokePing: gather ping statistics over time	437
iPerf: track network performance	437
Cacti: collect and graph data	438
Firewalls and NAT	440
Linux iptables : rules, chains, and tables	440
iptables rule targets	441
iptables firewall setup	442
A complete example	442
Linux NAT and packet filtering	444
IPFilter for UNIX systems	445
Cloud networking	448
AWS's virtual private cloud (VPC)	448
Subnets and routing tables	449
Security groups and NACLs	450
A sample VPC architecture	451
Creating a VPC with Terraform	452
Google Cloud Platform networking	455
DigitalOcean networking	456
Recommended reading	457
History	457
Classics and bibles	458
Protocols	458

Chapter 14 Physical Networking 459

Ethernet: the Swiss Army knife of networking	460
Ethernet signaling	460
Ethernet topology	461
Unshielded twisted-pair cabling	462
Optical fiber	464
Ethernet connection and expansion	465
Hubs	465
Switches	465
VLAN-capable switches	466
Routers	467
Autonegotiation	467
Power over Ethernet	468
Jumbo frames	468
Wireless: Ethernet for nomads	469
Wireless standards	469
Wireless client access	470
Wireless infrastructure and WAPs	470
Wireless topology	471
Small money wireless	472
Big money wireless	472
Wireless security	473
SDN: software-defined networking	473
Network testing and debugging	474
Building wiring	475
UTP cabling options	475
Connections to offices	475
Wiring standards	475
Network design issues	476
Network architecture vs. building architecture	477
Expansion	477
Congestion	478
Maintenance and documentation	478
Management issues	478
Recommended vendors	479
Cables and connectors	479
Test equipment	480
Routers/switches	480
Recommended reading	480

Chapter 15	IP Routing	481
	Packet forwarding: a closer look	482
	Routing daemons and routing protocols	485
	Distance-vector protocols	486
	Link-state protocols	487
	Cost metrics	487
	Interior and exterior protocols	488
	Protocols on parade	488
	RIP and RIPvng: Routing Information Protocol	488
	OSPF: Open Shortest Path First	489
	EIGRP: Enhanced Interior Gateway Routing Protocol	490
	BGP: Border Gateway Protocol	490
	Routing protocol multicast coordination	490
	Routing strategy selection criteria	490
	Routing daemons	492
	routed : obsolete RIP implementation	492
	Quagga: mainstream routing daemon	493
	XORP: router in a box	494
	Cisco routers	494
	Recommended reading	496
Chapter 16	DNS: The Domain Name System	498
	DNS architecture	499
	Queries and responses	499
	DNS service providers	500
	DNS for lookups	500
	resolv.conf : client resolver configuration	500
	nsswitch.conf : who do I ask for a name?	501
	The DNS namespace	502
	Registering a domain name	503
	Creating your own subdomains	503
	How DNS works	503
	Name servers	504
	Authoritative and caching-only servers	505
	Recursive and nonrecursive servers	505
	Resource records	506
	Delegation	506
	Caching and efficiency	508
	Multiple answers and round robin DNS load balancing	508
	Debugging with query tools	509
	The DNS database	512
	Parser commands in zone files	512
	Resource records	513
	The SOA record	516

NS records	518
A records	519
AAAA records	519
PTR records	520
MX records	521
CNAME records	522
SRV records	523
TXT records	524
SPF, DKIM, and DMARC records	525
DNSSEC records	525
The BIND software	525
Components of BIND	525
Configuration files	526
The include statement	527
The options statement	528
The acl statement	534
The (TSIG) key statement	534
The server statement	535
The masters statement	535
The logging statement	536
The statistics-channels statement	536
The zone statement	536
Configuring the master server for a zone	537
Configuring a slave server for a zone	538
Setting up the root server hints	539
Setting up a forwarding zone	539
The controls statement for rndc	540
Split DNS and the view statement	541
BIND configuration examples	543
The localhost zone	543
A small security company	544
Zone file updating	547
Zone transfers	548
Dynamic updates	549
DNS security issues	551
Access control lists in BIND, revisited	552
Open resolvers	553
Running in a chrooted jail	554
Secure server-to-server communication with TSIG and TKEY	554
Setting up TSIG for BIND	555
DNSSEC	557
DNSSEC policy	558
DNSSEC resource records	558
Turning on DNSSEC	560
Key pair generation	560

Zone signing	562
The DNSSEC chain of trust	564
DNSSEC key rollover	565
DNSSEC tools	566
ldns tools, nlnetlabs.nl/projects/ldns	566
dnssec-tools.org	566
RIPE tools, ripe.net	567
OpenDNSSEC, opendnssec.org	567
Debugging DNSSEC	567
BIND debugging	568
Logging in BIND	568
Channels	569
Categories	570
Log messages	570
Sample BIND logging configuration	573
Debug levels in BIND	573
Name server control with rndc	574
Command-line querying for lame delegations	575
Recommended reading	576
Books and other documentation	577
On-line resources	577
The RFCs	577
Chapter 17 Single Sign-On	578
Core SSO elements	579
LDAP: “lightweight” directory services	580
Uses for LDAP	580
The structure of LDAP data	581
OpenLDAP: the traditional open source LDAP server	582
389 Directory Server: alternative open source LDAP server	583
LDAP Querying	584
Conversion of passwd and group files to LDAP	585
Using directory services for login	586
Kerberos	586
Linux Kerberos configuration for AD integration	587
FreeBSD Kerberos configuration for AD integration	587
sssd : the System Security Services Daemon	589
nsswitch.conf : the name service switch	590
PAM: cooking spray or authentication wonder?	590
PAM configuration	591
PAM example	592
Alternative approaches	594
NIS: the Network Information Service	594
rsync : transfer files securely	594
Recommended reading	595

Chapter 18 Electronic Mail	596
Mail system architecture	597
User agents	597
Submission agents	598
Transport agents	598
Local delivery agents	599
Message stores	599
Access agents	599
Anatomy of a mail message	600
The SMTP protocol	603
You had me at EHLO	604
SMTP error codes	604
SMTP authentication	604
Spam and malware	605
Forgeries	606
SPF and Sender ID	606
DKIM	607
Message privacy and encryption	607
Mail aliases	608
Getting aliases from files	610
Mailing to files	611
Mailing to programs	611
Building the hashed alias database	612
Email configuration	612
sendmail	613
The switch file	614
Starting sendmail	615
Mail queues	616
sendmail configuration	617
The m4 preprocessor	617
The sendmail configuration pieces	618
A configuration file built from a sample .mc file	619
Configuration primitives	620
Tables and databases	620
Generic macros and features	621
OSTYPE macro	621
DOMAIN macro	621
MAILER macro	622
FEATURE macro	622
use_cw_file feature	622
redirect feature	623
always_add_domain feature	623
access_db feature	623
virtusertable feature	624

ldap_routing feature	624
Masquerading features	625
MAIL_HUB and SMART_HOST macros	626
Client configuration	626
m4 configuration options	627
Spam-related features in sendmail	628
Relay control	629
User or site blacklisting	630
Throttles, rates, and connection limits	631
Security and sendmail	632
Ownerships	633
Permissions	634
Safer mail to files and programs	634
Privacy options	635
Running a chrooted sendmail (for the truly paranoid)	636
Denial of service attacks	636
TLS: Transport Layer Security	637
sendmail testing and debugging	638
Queue monitoring	638
Logging	639
Exim	640
Exim installation	640
Exim startup	642
Exim utilities	642
Exim configuration language	643
Exim configuration file	644
Global options	645
Options	645
Lists	646
Macros	647
Access control lists (ACLs)	647
Content scanning at ACL time	650
Authenticators	651
Routers	652
The accept router	653
The dnslookup router	653
The manualroute router	653
The redirect router	654
Per-user filtering through .forward files	655
Transports	655
The appendfile transport	655
The smtp transport	656
Retry configuration	656
Rewriting configuration	657
Local scan function	657

Logging	657
Debugging	658
Postfix	658
Postfix architecture	659
Receiving mail	659
Managing mail-waiting queues	660
Sending mail	660
Security	661
Postfix commands and documentation	661
Postfix configuration	661
What to put in main.cf	662
Basic settings	662
Null client	662
Use of postconf	663
Lookup tables	663
Local delivery	664
Virtual domains	665
Virtual alias domains	666
Virtual mailbox domains	667
Access control	667
Access tables	669
Authentication of clients and encryption	670
Debugging	670
Looking at the queue	671
Soft-bouncing	671
Recommended reading	672
sendmail references	672
Exim references	672
Postfix references	672
RFCs	673

Chapter 19 Web Hosting

674

HTTP: the Hypertext Transfer Protocol	674
Uniform Resource Locators (URLs)	675
Structure of an HTTP transaction	676
HTTP requests	677
HTTP responses	677
Headers and the message body	678
curl : HTTP from the command line	679
TCP connection reuse	680
HTTP over TLS	681
Virtual hosts	681

Web software basics	682
Web servers and HTTP proxy software	683
Load balancers	684
Caches	686
Browser caches	687
Proxy cache	688
Reverse proxy cache	688
Cache problems	688
Cache software	689
Content delivery networks	689
Languages of the web	691
Ruby	691
Python	691
Java	691
Node.js	691
PHP	692
Go	692
Application programming interfaces (APIs)	692
Web hosting in the cloud	694
Build versus buy	694
Platform-as-a-Service	695
Static content hosting	695
Serverless web applications	696
Apache httpd	696
httpd in use	697
httpd configuration logistics	698
Virtual host configuration	699
HTTP basic authentication	701
Configuring TLS	702
Running web applications within Apache	702
Logging	703
NGINX	704
Installing and running NGINX	704
Configuring NGINX	705
Configuring TLS for NGINX	708
Load balancing with NGINX	708
HAProxy	710
Health checks	711
Server statistics	712
Sticky sessions	712
TLS termination	713
Recommended reading	714
Retry configuration	656
Rewriting configuration	657
Local scan function	657

SECTION THREE: STORAGE

Chapter 20	Storage	717
	I just want to add a disk!	718
	Linux recipe	719
	FreeBSD recipe	720
	Storage hardware	721
	Hard disks	722
	Hard disk reliability	723
	Failure modes and metrics	723
	Drive types	724
	Warranties and retirement	725
	Solid state disks	725
	Rewritability limits	726
	Flash memory and controller types	726
	Page clusters and pre-erasing	727
	SSD reliability	727
	Hybrid drives	728
	Advanced Format and 4KiB blocks	729
	Storage hardware interfaces	730
	The SATA interface	730
	The PCI Express interface	730
	The SAS interface	731
	USB	732
	Attachment and low-level management of drives	733
	Installation verification at the hardware level	733
	Disk device files	734
	Ephemeral device names	735
	Formatting and bad block management	735
	ATA secure erase	737
	hdparm and camcontrol : set disk and interface parameters	738
	Hard disk monitoring with SMART	738
	The software side of storage: peeling the onion	739
	Elements of a storage system	740
	The Linux device mapper	742
	Disk partitioning	742
	Traditional partitioning	744
	MBR partitioning	745
	GPT: GUID partition tables	746
	Linux partitioning	746
	FreeBSD partitioning	747

Logical volume management	747
Linux logical volume management	748
Volume snapshots	750
Filesystem resizing	751
FreeBSD logical volume management	753
RAID: redundant arrays of inexpensive disks	753
Software vs. hardware RAID	753
RAID levels	754
Disk failure recovery	756
Drawbacks of RAID 5	757
mdadm : Linux software RAID	758
Creating an array	758
mdadm.conf : document array configuration	760
Simulating a failure	761
Filesystems	762
Traditional filesystems: UFS, ext4, and XFS	763
Filesystem terminology	764
Filesystem polymorphism	765
Filesystem formatting	766
fsck : check and repair filesystems	766
Filesystem mounting	767
Setup for automatic mounting	768
USB drive mounting	770
Swapping recommendations	770
Next-generation filesystems: ZFS and Btrfs	772
Copy-on-write	772
Error detection	772
Performance	773
ZFS: all your storage problems solved	773
ZFS on Linux	774
ZFS architecture	774
Example: disk addition	775
Filesystems and properties	776
Property inheritance	777
One filesystem per user	778
Snapshots and clones	779
Raw volumes	780
Storage pool management	781
Btrfs: “ZFS lite” for Linux	783
Btrfs vs. ZFS	783
Setup and storage conversion	784
Volumes and subvolumes	786
Volume snapshots	787
Shallow copies	788

Data backup strategy	788
Recommended reading	790
Chapter 21 The Network File System	791
Meet network file services	791
The competition	792
Issues of state	792
Performance concerns	793
Security	793
The NFS approach	794
Protocol versions and history	794
Remote procedure calls	795
Transport protocols	795
State	796
Filesystem exports	796
File locking	797
Security concerns	798
Identity mapping in version 4	799
Root access and the nobody account	800
Performance considerations in version 4	801
Server-side NFS	801
Linux exports	802
FreeBSD exports	804
nfsd : serve files	806
Client-side NFS	807
Mounting remote filesystems at boot time	810
Restricting exports to privileged ports	810
Identity mapping for NFS version 4	810
nfsstat : dump NFS statistics	811
Dedicated NFS file servers	812
Automatic mounting	812
Indirect maps	814
Direct maps	814
Master maps	815
Executable maps	815
Automount visibility	816
Replicated filesystems and automount	816
Automatic automounts (V3; all but Linux)	817
Specifics for Linux	817
Recommended reading	818

Chapter 22	SMB	819
	Samba: SMB server for UNIX.....	820
	Installing and configuring Samba.....	821
	File sharing with local authentication.....	822
	File sharing with accounts authenticated by Active Directory.....	822
	Configuring shares.....	823
	Sharing home directories.....	823
	Sharing project directories.....	824
	Mounting SMB file shares.....	825
	Browsing SMB file shares.....	826
	Ensuring Samba security.....	826
	Debugging Samba.....	827
	Querying Samba's state with smbstatus	827
	Configuring Samba logging.....	828
	Managing character sets.....	829
	Recommended reading.....	829

SECTION FOUR: OPERATIONS

Chapter 23	Configuration Management	833
	Configuration management in a nutshell.....	834
	Dangers of configuration management.....	834
	Elements of configuration management.....	835
	Operations and parameters.....	835
	Variables.....	837
	Facts.....	838
	Change handlers.....	838
	Bindings.....	838
	Bundles and bundle repositories.....	839
	Environments.....	839
	Client inventory and registration.....	840
	Popular CM systems compared.....	841
	Terminology.....	842
	Business models.....	842
	Architectural options.....	843
	Language options.....	845
	Dependency management options.....	846
	General comments on Chef.....	848
	General comments on Puppet.....	849
	General comments on Ansible and Salt.....	850
	YAML: a rant.....	850

Introduction to Ansible	852
Ansible example	853
Client setup	855
Client groups	857
Variable assignments	858
Dynamic and computed client groups	859
Task lists	860
state parameters	862
Iteration	862
Interaction with Jinja	863
Template rendering	863
Bindings: plays and playbooks	864
Roles	866
Recommendations for structuring the configuration base	868
Ansible access options	869
Introduction to Salt	871
Minion setup	873
Variable value binding for minions	874
Minion matching	876
Salt states	877
Salt and Jinja	878
State IDs and dependencies	880
State and execution functions	882
Parameters and names	883
State binding to minions	886
Highstates	886
Salt formulas	887
Environments	888
Documentation roadmap	892
Ansible and Salt compared	893
Deployment flexibility and scalability	893
Built-in modules and extensibility	894
Security	894
Miscellaneous	895
Best practices	895
Recommended reading	899
Chapter 24 Virtualization	900
Virtual vernacular	901
Hypervisors	901
Full virtualization	901
Paravirtualization	902
Hardware-assisted virtualization	902
Paravirtualized drivers	902

Modern virtualization	903
Type 1 vs. type 2 hypervisors	903
Live migration	904
Virtual machine images	904
Containerization	904
Virtualization with Linux	905
Xen	906
Xen guest installation	907
KVM	908
KVM guest installation	909
FreeBSD bhyve	910
VMware	910
VirtualBox	911
Packer	911
Vagrant	913
Recommended reading	914

Chapter 25 Containers

915

Background and core concepts	916
Kernel support	917
Images	917
Networking	918
Docker: the open source container engine	919
Basic architecture	919
Installation	921
Client setup	921
The container experience	922
Volumes	926
Data volume containers	927
Docker networks	927
Namespaces and the bridge network	928
Network overlays	930
Storage drivers	930
dockerd option editing	930
Image building	932
Choosing a base image	933
Building from a Dockerfile	933
Composing a derived Dockerfile	934
Registries	936

Containers in practice	937
Logging.....	938
Security advice	939
Restrict access to the daemon	939
Use TLS	940
Run processes as unprivileged users	940
Use a read-only root filesystem.....	941
Limit capabilities.....	941
Secure images	941
Debugging and troubleshooting.....	942
Container clustering and management.....	942
A synopsis of container management software.....	944
Kubernetes.....	944
Mesos and Marathon	946
Docker Swarm.....	947
AWS EC2 Container Service	947
Recommended reading	948

Chapter 26 Continuous Integration and Delivery 949

CI/CD essentials	951
Principles and practices	951
Use revision control	952
Build once, deploy often	952
Automate end-to-end	952
Build every integration commit	952
Share responsibility.....	953
Build fast, fix fast	953
Audit and verify.....	953
Environments	953
Feature flags.....	955
Pipelines.....	955
The build process.....	956
Testing	957
Deployment.....	959
Zero-downtime deployment techniques.....	960
Jenkins: the open source automation server.....	961
Basic Jenkins concepts	962
Distributed builds.....	963
Pipeline as code.....	963

CI/CD in practice	964
UlsahGo, a trivial web application	966
Unit testing UlsahGo	966
Taking first steps with the Jenkins Pipeline	968
Building a DigitalOcean image	970
Provisioning a single system for testing	972
Testing the droplet	975
Deploying UlsahGo to a pair of droplets and a load balancer	976
Concluding the demonstration pipeline	977
Containers and CI/CD	978
Containers as a build environment	979
Container images as build artifacts	979
Recommended reading	980
Chapter 27 Security	981
Elements of security	983
How security is compromised	983
Social engineering	983
Software vulnerabilities	984
Distributed denial-of-service attacks (DDoS)	985
Insider abuse	986
Network, system, or application configuration errors	986
Basic security measures	987
Software updates	987
Unnecessary services	988
Remote event logging	989
Backups	989
Viruses and worms	989
Root kits	990
Packet filtering	991
Passwords and multifactor authentication	991
Vigilance	991
Application penetration testing	992
Passwords and user accounts	992
Password changes	993
Password vaults and password escrow	993
Password aging	995
Group logins and shared logins	996
User shells	996
Rootly entries	996

Security power tools.....	996
Nmap: network port scanner	996
Nessus: next-generation network scanner.....	998
Metasploit: penetration testing software.....	999
Lynis: on-box security auditing	999
John the Ripper: finder of insecure passwords.....	1000
Bro: the programmable network intrusion detection system.....	1000
Snort: the popular network intrusion detection system	1001
OSSEC: host-based intrusion detection	1002
OSSEC basic concepts	1002
OSSEC installation	1003
OSSEC configuration	1004
Fail2Ban: brute-force attack response system.....	1004
Cryptography primer.....	1005
Symmetric key cryptography	1005
Public key cryptography	1006
Public key infrastructure	1007
Transport Layer Security	1009
Cryptographic hash functions	1009
Random number generation.....	1011
Cryptographic software selection.....	1012
The openssl command.....	1012
Preparing keys and certificates	1013
Debugging TLS servers	1014
PGP: Pretty Good Privacy.....	1014
Kerberos: a unified approach to network security	1015
SSH, the Secure SHell.....	1016
OpenSSH essentials	1016
The ssh client.....	1018
Public key authentication	1019
The ssh-agent	1020
Host aliases in ~/.ssh/config	1022
Connection multiplexing.....	1023
Port forwarding.....	1023
sshd : the OpenSSH server.....	1024
Host key verification with SSHFP	1026
File transfers	1027
Alternatives for secure logins	1027
Firewalls.....	1027
Packet-filtering firewalls	1028
Filtering of services.....	1028
Stateful inspection firewalls.....	1029
Firewalls: safe?.....	1029

Virtual private networks (VPNs)	1030
IPsec tunnels	1030
All I need is a VPN, right?	1031
Certifications and standards	1031
Certifications	1031
Security standards	1032
ISO 27001:2013	1032
PCI DSS	1033
NIST 800 series	1033
The Common Criteria	1034
OWASP: the Open Web Application Security Project	1034
CIS: the Center for Internet Security	1034
Sources of security information	1034
SecurityFocus.com, the BugTraq mailing list, and the OSS mailing list ..	1035
Schneier on Security	1035
The Verizon Data Breach Investigations Report	1035
The SANS Institute	1035
Distribution-specific security resources	1036
Other mailing lists and web sites	1036
When your site has been attacked	1037
Recommended reading	1038

Chapter 28 Monitoring

1040

An overview of monitoring	1041
Instrumentation	1042
Data types	1042
Intake and processing	1043
Notifications	1043
Dashboards and UIs	1044
The monitoring culture	1044
The monitoring platforms	1045
Open source real-time platforms	1046
Nagios and Icinga	1046
Sensu	1047
Open source time-series platforms	1047
Graphite	1047
Prometheus	1048
InfluxDB	1049
Munin	1049
Open source charting platforms	1049
Commercial monitoring platforms	1050
Hosted monitoring platforms	1051

Data collection	1051
StatsD: generic data submission protocol	1052
Data harvesting from command output	1054
Network monitoring	1055
Systems monitoring	1056
Commands for systems monitoring	1057
collectd : generalized system data harvester	1057
sysdig and dtrace : execution tracers	1058
Application monitoring	1059
Log monitoring	1059
Supervisor + Munin: a simple option for limited domains	1060
Commercial application monitoring tools	1060
Security monitoring	1061
System integrity verification	1061
Intrusion detection monitoring	1062
SNMP: the Simple Network Management Protocol	1063
SNMP organization	1064
SNMP protocol operations	1065
Net-SNMP: tools for servers	1065
Tips and tricks for monitoring	1068
Recommended reading	1069

Chapter 29 Performance Analysis 1070

Performance tuning philosophy	1071
Ways to improve performance	1073
Factors that affect performance	1074
Stolen CPU cycles	1075
Analysis of performance problems	1076
System performance checkup	1077
Taking stock of your equipment	1077
Gathering performance data	1079
Analyzing CPU usage	1079
Understanding how the system manages memory	1081
Analyzing memory usage	1082
Analyzing disk I/O	1084
fiio : testing storage subsystem performance	1085
sar : collecting and reporting statistics over time	1086
Choosing a Linux I/O scheduler	1086
perf : profiling Linux systems in detail	1087
Help! My server just got really slow!	1088
Recommended reading	1090

Chapter 30	Data Center Basics	1091
	Racks.....	1092
	Power.....	1092
	Rack power requirements.....	1093
	kVA vs. kW.....	1094
	Energy efficiency.....	1095
	Metering.....	1095
	Cost.....	1096
	Remote control.....	1096
	Cooling and environment.....	1096
	Cooling load estimation.....	1097
	Roof, walls, and windows.....	1097
	Electronic gear.....	1097
	Light fixtures.....	1098
	Operators.....	1098
	Total heat load.....	1098
	Hot aisles and cold aisles.....	1098
	Humidity.....	1100
	Environmental monitoring.....	1100
	Data center reliability tiers.....	1101
	Data center security.....	1102
	Location.....	1102
	Perimeter.....	1102
	Facility access.....	1102
	Rack access.....	1103
	Tools.....	1103
	Recommended reading.....	1104
Chapter 31	Methodology, Policy, and Politics	1105
	The grand unified theory: DevOps.....	1106
	DevOps is CLAMS.....	1107
	Culture.....	1107
	Lean.....	1108
	Automation.....	1109
	Measurement.....	1110
	Sharing.....	1110
	System administration in a DevOps world.....	1110
	Ticketing and task management systems.....	1111
	Common functions of ticketing systems.....	1112
	Ticket ownership.....	1112
	User acceptance of ticketing systems.....	1113
	Sample ticketing systems.....	1114
	Ticket dispatching.....	1114

Local documentation maintenance	1115
Infrastructure as code	1116
Documentation standards	1116
Environment separation	1118
Disaster management	1119
Risk assessment	1119
Recovery planning	1120
Staffing for a disaster	1121
Security incidents	1122
IT policies and procedures	1122
The difference between policies and procedures	1123
Policy best practices	1124
Procedures	1124
Service level agreements	1125
Scope and descriptions of services	1125
Queue prioritization policies	1126
Conformance measurements	1127
Compliance: regulations and standards	1127
Legal issues	1131
Privacy	1131
Policy enforcement	1132
Control = liability	1132
Software licenses	1133
Organizations, conferences, and other resources	1133
Recommended reading	1135

Index	1136
A Brief History of System Administration	1166
Colophon	1176
About the Contributors	1178
About the Authors	1179