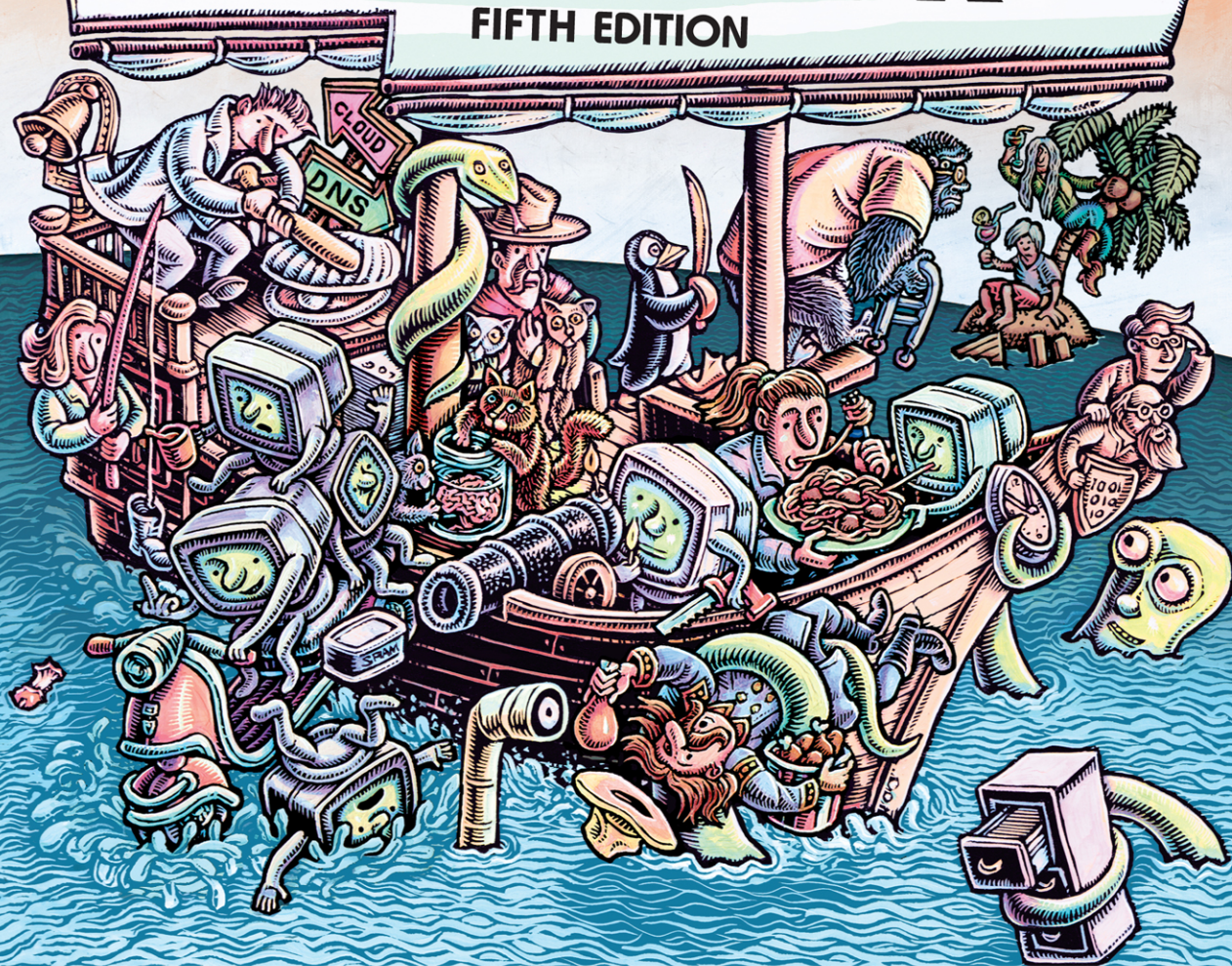


FIFTH EDITION



with James Garnett, Fabrizio Branca, and Adrian Mouat

UNIX[®] AND LINUX[®] SYSTEM ADMINISTRATION HANDBOOK

FIFTH EDITION

UNIX and Linux System Administration Handbook

Table of Contents

Cover

Half Title

Title Page

Copyright Page

Contents

Tribute to Evi

Preface

Foreword

Acknowledgments

SECTION ONE: BASIC ADMINISTRATION

Chapter 1 Where to Start

Essential duties of a system administrator

Controlling access

Adding hardware

Automating tasks

Overseeing backups

Installing and upgrading software

Monitoring

Troubleshooting

Maintaining local documentation

Vigilantly monitoring security

Tuning performance

Developing site policies

Table of Contents

Working with vendors

Fire fighting

Suggested background

Linux distributions

Example systems used in this book

Example Linux distributions

Example UNIX distribution

Notation and typographical conventions

Units

Man pages and other on-line documentation

Organization of the man pages

man: read man pages

Storage of man pages

Other authoritative documentation

System-specific guides

Package-specific documentation

Books

RFC publications

Other sources of information

Keeping current

HowTos and reference sites

Conferences

Ways to find and install software

Determining if software is already installed

Adding new software

Building software from source code

Installing from a web script

Where to host

Specialization and adjacent disciplines

DevOps

Site reliability engineers

Security operations engineers

Table of Contents

- Network administrators
- Database administrators
- Network operations center (NOC) engineers
- Data center technicians
- Architects

Recommended reading

- System administration and DevOps
- Essential tools

Chapter 2 Booting and System Management Daemons

Boot process overview

System firmware

- BIOS vs. UEFI
- Legacy BIOS
- UEFI

Boot loaders

GRUB: the GRand Unified Boot loader

- GRUB configuration
- The GRUB command line
- Linux kernel options

The FreeBSD boot process

- The BIOS path: boot0
- The UEFI path
- loader configuration
- loader commands

System management daemons

- Responsibilities of init
- Implementations of init
- Traditional init
- systemd vs. the world
- inits judged and assigned their proper punishments

systemd in detail

- Units and unit files

Table of Contents

systemctl: manage systemd

Unit statuses

Targets

Dependencies among units

Execution order

A more complex unit file example

Local services and customizations

Service and startup control caveats

systemd logging

FreeBSD init and startup scripts

Reboot and shutdown procedures

Shutting down physical systems

Shutting down cloud systems

Stratagems for a nonbooting system

Single-user mode

Single-user mode on FreeBSD

Single-user mode with GRUB

Recovery of cloud systems

Chapter 3 Access Control and Rootly Powers

Standard UNIX access control

Filesystem access control

Process ownership

The root account

Setuid and setgid execution

Management of the root account

Root account login

su: substitute user identity

sudo: limited su

Example configuration

sudo pros and cons

sudo vs. advanced access control

Typical setup

Environment management

Table of Contents

sudo without passwords

Precedence

sudo without a control terminal

Site-wide sudo configuration

Disabling the root account

System accounts other than root

Extensions to the standard access control model

Drawbacks of the standard model

PAM: Pluggable Authentication Modules

Kerberos: network cryptographic authentication

Filesystem access control lists

Linux capabilities

Linux namespaces

Modern access control

Separate ecosystems

Mandatory access control

Role-based access control

SELinux: Security-Enhanced Linux

AppArmor

Recommended reading

Chapter 4 Process Control

Components of a process

PID: process ID number

PPID: parent PID

UID and EUID: real and effective user ID

GID and EGID: real and effective group ID

Niceness

Control terminal

The life cycle of a process

Signals

kill: send signals

Process and thread states

ps: monitor processes

Table of Contents

Interactive monitoring with top

nice and renice: influence scheduling priority

The /proc filesystem

strace and truss: trace signals and system calls

Runaway processes

Periodic processes

- cron: schedule commands

 - The format of crontab files

 - Crontab management

 - Other crontabs

 - cron access control

- systemd timers

 - Structure of systemd timers

 - systemd timer example

 - systemd time expressions

 - Transient timers

Common uses for scheduled tasks

- Sending mail

- Cleaning up a filesystem

- Rotating a log file

- Running batch jobs

- Backing up and mirroring

Chapter 5 The Filesystem

Pathnames

Filesystem mounting and unmounting

Organization of the file tree

File types

- Regular files

- Directories

- Hard links

- Character and block device files

- Local domain sockets

- Named pipes

Table of Contents

Symbolic links

File attributes

The permission bits

The setuid and setgid bits

The sticky bit

ls: list and inspect files

chmod: change permissions

chown and chgrp: change ownership and group

umask: assign default permissions

Linux bonus flags

Access control lists

A cautionary note

ACL types

Implementation of ACLs

Linux ACL support

FreeBSD ACL support

POSIX ACLs

Interaction between traditional modes and ACLs

POSIX access determination

POSIX ACL inheritance

NFSv4 ACLs

NFSv4 entities for which permissions can be specified

NFSv4 access determination

ACL inheritance in NFSv4

NFSv4 ACL viewing

Interactions between ACLs and modes

NFSv4 ACL setup

Chapter 6 Software Installation and Management

Operating system installation

Installing from the network

Setting up PXE

Using kickstart, the automated installer for Red Hat and CentOS

Setting up a kickstart configuration file

Building a kickstart server

Table of Contents

Pointing kickstart at your config file

Automating installation for Debian and Ubuntu

Netbooting with Cobbler, the open source Linux provisioning server

Automating FreeBSD installation

Managing packages

Linux package management systems

rpm: manage RPM packages

dpkg: manage .deb packages

High-level Linux package management systems

Package repositories

RHN: the Red Hat Network

APT: the Advanced Package Tool

Repository configuration

An example /etc/apt/sources.list file

Creation of a local repository mirror

APT automation

yum: release management for RPM

FreeBSD software management

The base system

pkg: the FreeBSD package manager

The ports collection

Software localization and configuration

Organizing your localization

Structuring updates

Limiting the field of play

Testing

Recommended reading

Chapter 7 Scripting and the Shell

Scripting philosophy

Write microscripts

Learn a few tools well

Automate all the things

Table of Contents

Dont optimize prematurely
Pick the right scripting language
Follow best practices

Shell basics

Command editing
Pipes and redirection
Variables and quoting
Environment variables
Common filter commands
 cut: separate lines into fields
 sort: sort lines
 uniq: print unique lines
 wc: count lines, words, and characters
 tee: copy input to two places
 head and tail: read the beginning or end of a file
 grep: search text

sh scripting

Execution
From commands to scripts
Input and output
Spaces in filenames
Command-line arguments and functions
Control flow
Loops
Arithmetic

Regular expressions

The matching process
Literal characters
Special characters
Example regular expressions
Captures
Greediness, laziness, and catastrophic backtracking

Python programming

The passion of Python 3

Table of Contents

Python 2 or Python 3?

Python quick start

Objects, strings, numbers, lists, dictionaries, tuples, and files

Input validation example

Loops

Ruby programming

Installation

Ruby quick start

Blocks

Symbols and option hashes

Regular expressions in Ruby

Ruby as a filter

Library and environment management for Python and Ruby

Finding and installing packages

Creating reproducible environments

Multiple environments

virtualenv: virtual environments for Python

RVM: the Ruby enVironment Manager

Revision control with Git

A simple Git example

Git caveats

Social coding with Git

Recommended reading

Shells and shell scripting

Regular expressions

Python

Ruby

Chapter 8 User Management

Account mechanics

The /etc/passwd file

Login name

Encrypted password

UID (user ID) number

Table of Contents

- Default GID (group ID) number

- GECOS field

- Home directory

- Login shell

- The Linux /etc/shadow file

- FreeBSD's /etc/master.passwd and /etc/login.conf files

 - The /etc/master.passwd file

 - The /etc/login.conf file

- The /etc/group file

- Manual steps for adding users

 - Editing the passwd and group files

 - Setting a password

 - Creating the home directory and installing startup files

 - Setting home directory permissions and ownerships

 - Configuring roles and administrative privileges

 - Finishing up

- Scripts for adding users: useradd, adduser, and newusers

 - useradd on Linux

 - adduser on Debian and Ubuntu

 - adduser on FreeBSD

 - newusers on Linux: adding in bulk

- Safe removal of a users account and files

- User login logout

- Risk reduction with PAM

- Centralized account management

 - LDAP and Active Directory

 - Application-level single sign-on systems

 - Identity management systems

Chapter 9 Cloud Computing

- The cloud in context

- Cloud platform choices

 - Public, private, and hybrid clouds

Table of Contents

Amazon Web Services

Google Cloud Platform

DigitalOcean

Cloud service fundamentals

Access to the cloud

Regions and availability zones

Virtual private servers

Networking

Storage

Identity and authorization

Automation

Serverless functions

Clouds: VPS quick start by platform

Amazon Web Services

aws: control AWS subsystems

Creating an EC2 instance

Viewing the console log

Stopping and terminating instances

Google Cloud Platform

Setting up gcloud

Running an instance on GCE

DigitalOcean

Cost control

Recommended Reading

Chapter 10 Logging

Log locations

Files not to manage

How to view logs in the systemd journal

The systemd journal

Configuring the systemd journal

Adding more filtering options for journalctl

Coexisting with syslog

Syslog

Table of Contents

Reading syslog messages

Rsyslog architecture

Rsyslog versions

Rsyslog configuration

- Modules

- sysklogd syntax

- Legacy directives

- RainerScript

Config file examples

- Basic rsyslog configuration

- Network logging client

- Central logging host

Syslog message security

Syslog configuration debugging

Kernel and boot-time logging

Management and rotation of log files

- logrotate: cross-platform log management

- newsyslog: log management on FreeBSD

Management of logs at scale

- The ELK stack

- Graylog

- Logging as a service

Logging policies

Chapter 11 Drivers and the Kernel

Kernel chores for system administrators

Kernel version numbering

- Linux kernel versions

- FreeBSD kernel versions

Devices and their drivers

- Device files and device numbers.

- Challenges of device file management

- Manual creation of device files

- Modern device file management

Table of Contents

Linux device management

Sysfs: a window into the souls of devices

udevadm: explore devices

Rules and persistent names

FreeBSD device management

Devfs: automatic device file configuration

devd: higher-level device management

Linux kernel configuration

Tuning Linux kernel parameters

Building a custom kernel

If it aint broke, dont fix it

Setting up to build the Linux kernel

Configuring kernel options

Building the kernel binary

Adding a Linux device driver

FreeBSD kernel configuration

Tuning FreeBSD kernel parameters

Building a FreeBSD kernel

Loadable kernel modules

Loadable kernel modules in Linux

Loadable kernel modules in FreeBSD

Booting

Linux boot messages

FreeBSD boot messages

Booting alternate kernels in the cloud

Kernel errors

Linux kernel errors

FreeBSD kernel panics

Recommended reading

Chapter 12 Printing

CUPS printing

Interfaces to the printing system

The print queue

Multiple printers and queues

Table of Contents

Printer instances

Network printer browsing

Filters

CUPS server administration

Network print server setup

Printer autoconfiguration

Network printer configuration

Printer configuration examples

Service shutoff

Other configuration tasks

Troubleshooting tips

Print daemon restart

Log files

Direct printing connections

Network printing problems

Recommended reading

SECTION TWO: NETWORKING

Chapter 13 TCP/IP Networking

TCP/IP and its relationship to the Internet

Who runs the Internet?

Network standards and documentation

Networking basics

IPv4 and IPv6

Packets and encapsulation

Ethernet framing

Maximum transfer unit

Packet addressing

Hardware (MAC) addressing

IP addressing

Hostname addressing

Ports

Address types

Table of Contents

IP addresses: the gory details

- IPv4 address classes

- IPv4 subnetting

- Tricks and tools for subnet arithmetic

- CIDR: Classless Inter-Domain Routing

- Address allocation

- Private addresses and network address translation (NAT)

- IPv6 addressing

 - IPv6 address notation

 - IPv6 prefixes

 - Automatic host numbering

 - Stateless address autoconfiguration

 - IPv6 tunneling

 - IPv6 information sources

Routing

- Routing tables

- ICMP redirects

IPv4 ARP and IPv6 neighbor discovery

DHCP: the Dynamic Host Configuration Protocol

- DHCP software

- DHCP behavior

- ISCs DHCP software

Security issues

- IP forwarding

- ICMP redirects

- Source routing

- Broadcast pings and other directed broadcasts

- IP spoofing

- Host-based firewalls

- Virtual private networks

Basic network configuration

- Hostname and IP address assignment

- Network interface and IP configuration

- Routing configuration

Table of Contents

DNS configuration

System-specific network configuration

Linux networking

NetworkManager

ip: manually configure a network

Debian and Ubuntu network configuration

Red Hat and CentOS network configuration

Linux network hardware options

Linux TCP/IP options

Security-related kernel variables

FreeBSD networking

ifconfig: configure network interfaces

FreeBSD network hardware configuration

FreeBSD boot-time network configuration

FreeBSD TCP/IP configuration

Network troubleshooting

ping: check to see if a host is alive

traceroute: trace IP packets

Packet sniffers

tcpdump: command-line packet sniffer

Wireshark and TShark: tcpdump on steroids

Network monitoring

SmokePing: gather ping statistics over time

iPerf: track network performance

Cacti: collect and graph data

Firewalls and NAT

Linux iptables: rules, chains, and tables

iptables rule targets

iptables firewall setup

A complete example

Linux NAT and packet filtering

IPFilter for UNIX systems

Cloud networking

Table of Contents

AWSs virtual private cloud (VPC)

- Subnets and routing tables

- Security groups and NACLs

- A sample VPC architecture

- Creating a VPC with Terraform

Google Cloud Platform networking

DigitalOcean networking

Recommended reading

- History

- Classics and bibles

- Protocols

Chapter 14 Physical Networking

Ethernet: the Swiss Army knife of networking

- Ethernet signaling

- Ethernet topology

- Unshielded twisted-pair cabling

- Optical fiber

- Ethernet connection and expansion

 - Hubs

 - Switches

 - VLAN-capable switches

 - Routers

- Autonegotiation

- Power over Ethernet

- Jumbo frames

Wireless: Ethernet for nomads

- Wireless standards

- Wireless client access

- Wireless infrastructure and WAPs

 - Wireless topology

 - Small money wireless

 - Big money wireless

- Wireless security

SDN: software-defined networking

Table of Contents

Network testing and debugging

Building wiring

- UTP cabling options

- Connections to offices

- Wiring standards

Network design issues

- Network architecture vs. building architecture

- Expansion

- Congestion

- Maintenance and documentation

Management issues

Recommended vendors

- Cables and connectors

- Test equipment

- Routers/switches

Recommended reading

Chapter 15 IP Routing

Packet forwarding: a closer look

Routing daemons and routing protocols

- Distance-vector protocols

- Link-state protocols

- Cost metrics

- Interior and exterior protocols

Protocols on parade

- RIP and RIPv2: Routing Information Protocol

- OSPF: Open Shortest Path First

- EIGRP: Enhanced Interior Gateway Routing Protocol

- BGP: Border Gateway Protocol

Routing protocol multicast coordination

Routing strategy selection criteria

Routing daemons

- routed: obsolete RIP implementation

Table of Contents

Quagga: mainstream routing daemon

XORP: router in a box

Cisco routers

Recommended reading

Chapter 16 DNS: The Domain Name System

DNS architecture

Queries and responses

DNS service providers

DNS for lookups

resolv.conf: client resolver configuration

nsswitch.conf: who do I ask for a name?

The DNS namespace

Registering a domain name

Creating your own subdomains

How DNS works

Name servers

Authoritative and caching-only servers

Recursive and nonrecursive servers

Resource records

Delegation

Caching and efficiency

Multiple answers and round robin DNS load balancing

Debugging with query tools

The DNS database

Parser commands in zone files

Resource records

The SOA record

NS records

A records

AAAA records

PTR records

MX records

Table of Contents

CNAME records

SRV records

TXT records

SPF, DKIM, and DMARC records

DNSSEC records

The BIND software

Components of BIND

Configuration files

The include statement

The options statement

The (TSIG) key statement

The server statement

The masters statement

The logging statement

The statistics-channels statement

The zone statement

Configuring the primary server for a zone

Configuring a secondary server for a zone

Setting up a forwarding zone

The controls statement for rndc

Split DNS and the view statement

BIND configuration examples

The localhost zone

A small security company

Zone file updating

Zone transfers

Dynamic updates

DNS security issues

Access control lists in BIND, revisited

Open resolvers

Running in a chrooted jail

Secure server-to-server communication with TSIG and TKEY

Setting up TSIG for BIND

Table of Contents

DNSSEC

DNSSEC policy

DNSSEC resource records

Turning on DNSSEC

Key pair generation

Zone signing

The DNSSEC chain of trust

DNSSEC key rollover

DNSSEC tools

Idns tools, nlnetlabs.nl/projects/ldns

dnssec-tools.org

RIPE tools, ripe.net

OpenDNSSEC, opendnssec.org

Debugging DNSSEC

BIND debugging

Logging in BIND

Channels

Categories

Log messages

Sample BIND logging configuration

Debug levels in BIND

Name server control with rndc

Command-line querying for lame delegations

Recommended reading

Books and other documentation

On-line resources

The RFCs

Chapter 17 Single Sign-On

Core SSO elements

LDAP: lightweight directory services

Uses for LDAP

The structure of LDAP data

OpenLDAP: the traditional open source LDAP server

389 Directory Server: alternative open source LDAP server

Table of Contents

LDAP Querying

Conversion of passwd and group files to LDAP

Using directory services for login

Kerberos

Linux Kerberos configuration for AD integration

FreeBSD Kerberos configuration for AD integration

sssd: the System Security Services Daemon

nsswitch.conf: the name service switch

PAM: cooking spray or authentication wonder?

PAM configuration

PAM example

Alternative approaches

NIS: the Network Information Service

rsync: transfer files securely

Recommended reading

Chapter 18 Electronic Mail

Mail system architecture

User agents

Submission agents

Transport agents

Local delivery agents

Message stores

Access agents

Anatomy of a mail message

The SMTP protocol

You had me at EHLO

SMTP error codes

SMTP authentication

Spam and malware

Forgeries

SPF and Sender ID

DKIM

Message privacy and encryption

Table of Contents

Mail aliases

- Getting aliases from files
- Mailing to files
- Mailing to programs
- Building the hashed alias database

Email configuration

sendmail

- The switch file
- Starting sendmail
- Mail queues
- sendmail configuration
- The m4 preprocessor
- The sendmail configuration pieces
- A configuration file built from a sample .mc file
- Configuration primitives
- Tables and databases
- Generic macros and features
 - OSTYPE macro
 - DOMAIN macro
 - MAILER macro
 - FEATURE macro
 - use_cw_file feature
 - redirect feature
 - always_add_domain feature
 - access_db feature
 - virtusertable feature
 - ldap_routing feature
 - Masquerading features
 - MAIL_HUB and SMART_HOST macros

Client configuration

m4 configuration options

Spam-related features in sendmail

- Relay control
- User or site blacklisting
- Throttles, rates, and connection limits

Table of Contents

Security and sendmail

- Ownerships
- Permissions
- Safer mail to files and programs
- Privacy options
- Running a chrooted sendmail (for the truly paranoid)
- Denial of service attacks
- TLS: Transport Layer Security

sendmail testing and debugging

- Queue monitoring
- Logging

Exim

Exim installation

Exim startup

Exim utilities

Exim configuration language

Exim configuration file

Global options

- Options
- Lists
- Macros

Access control lists (ACLs)

Content scanning at ACL time

Authenticators

Routers

- The accept router
- The dnslookup router
- The manualroute router
- The redirect router
- Per-user filtering through .forward files

Transports

- The appendfile transport
- The smtp transport

Retry configuration

Rewriting configuration

Local scan function

Table of Contents

Logging

Debugging

Postfix

Postfix architecture

Receiving mail

Managing mail-waiting queues

Sending mail

Security

Postfix commands and documentation

Postfix configuration

What to put in main.cf.

Basic settings

Null client

Use of postconf

Lookup tables

Local delivery

Virtual domains

Virtual alias domains

Virtual mailbox domains

Access control

Access tables

Authentication of clients and encryption

Debugging

Looking at the queue

Soft-bouncing

Recommended reading

sendmail references

Exim references

Postfix references

RFCs

Chapter 19 Web Hosting

HTTP: the Hypertext Transfer Protocol

Uniform Resource Locators (URLs)

Structure of an HTTP transaction

HTTP requests

Table of Contents

HTTP responses

Headers and the message body

curl: HTTP from the command line

TCP connection reuse

HTTP over TLS

Virtual hosts

Web software basics

Web servers and HTTP proxy software

Load balancers

Caches

Browser caches

Proxy cache

Reverse proxy cache

Cache problems

Cache software

Content delivery networks

Languages of the web

Ruby

Python

Java

Node.js

PHP

Go

Application programming interfaces (APIs)

Web hosting in the cloud

Build versus buy

Platform-as-a-Service

Static content hosting

Serverless web applications

Apache httpd

httpd in use

httpd configuration logistics

Virtual host configuration

HTTP basic authentication

Configuring TLS

Table of Contents

Running web applications within Apache

Logging

NGINX

Installing and running NGINX

Configuring NGINX

Configuring TLS for NGINX

Load balancing with NGINX

HAProxy

Health checks

Server statistics

Sticky sessions

TLS termination

Recommended reading

SECTION THREE: STORAGE

Chapter 20 Storage

I just want to add a disk!

Linux recipe

FreeBSD recipe

Storage hardware

Hard disks

Hard disk reliability

Failure modes and metrics

Drive types

Warranties and retirement

Solid state disks

Rewritability limits

Flash memory and controller types

Page clusters and pre-erasing

SSD reliability

Hybrid drives

Advanced Format and 4KiB blocks

Storage hardware interfaces

The SATA interface

Table of Contents

The PCI Express interface

The SAS interface

USB

Attachment and low-level management of drives

Installation verification at the hardware level

Disk device files

Ephemeral device names

Formatting and bad block management

ATA secure erase

hdparm and camcontrol: set disk and interface parameters

Hard disk monitoring with SMART

The software side of storage: peeling the onion

Elements of a storage system

The Linux device mapper

Disk partitioning

Traditional partitioning

MBR partitioning

GPT: GUID partition tables

Linux partitioning

FreeBSD partitioning

Logical volume management

Linux logical volume management

Volume snapshots

Filesystem resizing

FreeBSD logical volume management

RAID: redundant arrays of inexpensive disks

Software vs. hardware RAID

RAID levels

Disk failure recovery

Drawbacks of RAID 5

mdadm: Linux software RAID

Creating an array

mdadm.conf: document array configuration

Simulating a failure

Table of Contents

Filesystems

Traditional filesystems: UFS, ext4, and XFS

- Filesystem terminology
- Filesystem polymorphism
- Filesystem formatting
- fsck: check and repair filesystems
- Filesystem mounting
- Setup for automatic mounting
- USB drive mounting
- Swapping recommendations

Next-generation filesystems: ZFS and Btrfs

- Copy-on-write
- Error detection
- Performance

ZFS: all your storage problems solved

- ZFS on Linux
- ZFS architecture
- Example: disk addition
- Filesystems and properties
- Property inheritance
- One filesystem per user
- Snapshots and clones
- Raw volumes
- Storage pool management

Btrfs: ZFS lite for Linux

- Btrfs vs. ZFS
- Setup and storage conversion
- Volumes and subvolumes
- Volume snapshots
- Shallow copies

Data backup strategy

Recommended reading

Table of Contents

Chapter 21 The Network File System

Meet network file services

- The competition

- Issues of state

- Performance concerns

- Security

The NFS approach

- Protocol versions and history

- Remote procedure calls

- Transport protocols

- State

- Filesystem exports

- File locking

- Security concerns

- Identity mapping in version 4

- Root access and the nobody account

- Performance considerations in version 4

Server-side NFS

- Linux exports

- FreeBSD exports

- anfsd: serve files

Client-side NFS

- Mounting remote filesystems at boot time

- Restricting exports to privileged ports

Identity mapping for NFS version 4

nfsstat: dump NFS statistics

Dedicated NFS file servers

Automatic mounting

- Indirect maps

- Direct maps

- Master maps

- Executable maps

Table of Contents

Automount visibility

Replicated filesystems and automount

Automatic automounts (V3; all but Linux)

Specifics for Linux

Recommended reading

Chapter 22 SMB

Samba: SMB server for UNIX

Installing and configuring Samba

File sharing with local authentication

File sharing with accounts authenticated by Active Directory

Configuring shares

Sharing home directories

Sharing project directories

Mounting SMB file shares

Browsing SMB file shares

Ensuring Samba security

Debugging Samba

Querying Samba's state with smbstatus

Configuring Samba logging

Managing character sets

Recommended reading

SECTION FOUR: OPERATIONS

Chapter 23 Configuration Management

Configuration management in a nutshell

Dangers of configuration management

Elements of configuration management

Operations and parameters

Variables

Facts

Change handlers

Bindings

Table of Contents

Bundles and bundle repositories

Environments

Client inventory and registration

Popular CM systems compared

Terminology

Business models

Architectural options

Language options

Dependency management options

General comments on Chef

General comments on Puppet

General comments on Ansible and Salt

YAML: a rant

Introduction to Ansible

Ansible example

Client setup

Client groups

Variable assignments

Dynamic and computed client groups

Task lists

state parameters

Iteration

Interaction with Jinja

Template rendering

Bindings: plays and playbooks

Roles

Recommendations for structuring the configuration base

Ansible access options

Introduction to Salt

Minion setup

Variable value binding for minions

Minion matching

Salt states

Table of Contents

- Salt and Jinja
- State IDs and dependencies
- State and execution functions
- Parameters and names
- State binding to minions
- Highstates
- Salt formulas
- Environments
- Documentation roadmap

Ansible and Salt compared

- Deployment flexibility and scalability
- Built-in modules and extensibility
- Security
- Miscellaneous

Best practices

Recommended reading

Chapter 24 Virtualization

Virtual vernacular

Hypervisors

- Full virtualization
- Paravirtualization
- Hardware-assisted virtualization
- Paravirtualized drivers
- Modern virtualization
- Type 1 vs. type 2 hypervisors

Live migration

Virtual machine images

Containerization

Virtualization with Linux

Xen

Xen guest installation

KVM

KVM guest installation

Table of Contents

FreeBSD bhyve

VMware

VirtualBox

Packer

Vagrant

Recommended reading

Chapter 25 Containers

Background and core concepts

Kernel support

Images.

Networking

Docker: the open source container engine

Basic architecture

Installation

Client setup

The container experience

Volumes

Data volume containers

Docker networks

Namespaces and the bridge network

Network overlays

Storage drivers

dockerd option editing

Image building

Choosing a base image

Building from a Dockerfile

Composing a derived Dockerfile

Registries

Containers in practice

Logging

Security advice

Restrict access to the daemon

Use TLS

Table of Contents

- Run processes as unprivileged users

- Use a read-only root filesystem

- Limit capabilities

- Secure images

- Debugging and troubleshooting

Container clustering and management

- A synopsis of container management software

- Kubernetes

- Mesos and Marathon

- Docker Swarm

- AWS EC2 Container Service

Recommended reading

Chapter 26 Continuous Integration and Delivery

CI/CD essentials

Principles and practices

- Use revision control

- Build once, deploy often

- Automate end-to-end

- Build every integration commit

- Share responsibility

- Build fast, fix fast

- Audit and verify

- Environments

- Feature flags

Pipelines

- The build process

- Testing

- Deployment

- Zero-downtime deployment techniques

Jenkins: the open source automation server

- Basic Jenkins concepts

- Distributed builds

- Pipeline as code

CI/CD in practice

- UlsahGo, a trivial web application

- Unit testing UlsahGo

Table of Contents

- Taking first steps with the Jenkins Pipeline
- Building a DigitalOcean image
- Provisioning a single system for testing
- Testing the droplet
- Deploying UlsahGo to a pair of droplets and a load balancer
- Concluding the demonstration pipeline

Containers and CI/CD

- Containers as a build environment
- Container images as build artifacts

Recommended reading

Chapter 27 Security

Elements of security

How security is compromised

- Social engineering
- Software vulnerabilities
- Distributed denial-of-service attacks (DDoS)
- Insider abuse
- Network, system, or application configuration errors

Basic security measures

- Software updates
- Unnecessary services
- Remote event logging
- Backups
- Viruses and worms
- Root kits
- Packet filtering
- Passwords and multifactor authentication
- Vigilance
- Application penetration testing

Passwords and user accounts

- Password changes
- Password vaults and password escrow
- Password aging
- Group logins and shared logins

Table of Contents

User shells

Rootly entries

Security power tools

Nmap: network port scanner

Nessus: next-generation network scanner

Metasploit: penetration testing software

Lynis: on-box security auditing

John the Ripper: finder of insecure passwords

Bro: the programmable network intrusion detection system

Snort: the popular network intrusion detection system

OSSEC: host-based intrusion detection

OSSEC basic concepts

OSSEC installation

OSSEC configuration

Fail2Ban: brute-force attack response system

Cryptography primer

Symmetric key cryptography

Public key cryptography

Public key infrastructure

Transport Layer Security

Cryptographic hash functions

Random number generation

Cryptographic software selection

The openssl command

Preparing keys and certificates

Debugging TLS servers

PGP: Pretty Good Privacy

Kerberos: a unified approach to network security

SSH, the Secure SHell

OpenSSH essentials

The ssh client

Public key authentication

The ssh-agent

Host aliases in ~/.ssh/config

Table of Contents

- Connection multiplexing
- Port forwarding
- sshd: the OpenSSH server
- Host key verification with SSHFP
- File transfers
- Alternatives for secure logins

Firewalls

- Packet-filtering firewalls
- Filtering of services
- Stateful inspection firewalls
- Firewalls: safe?

Virtual private networks (VPNs)

- IPsec tunnels
- All I need is a VPN, right?

Certifications and standards

- Certifications
- Security standards
 - ISO 27001:2013
 - PCI DSS
 - NIST 800 series
 - The Common Criteria
 - OWASP: the Open Web Application Security Project
 - CIS: the Center for Internet Security

Sources of security information

- SecurityFocus.com, the BugTraq mailing list, and the OSS mailing list
- Schneier on Security
- The Verizon Data Breach Investigations Report
- The SANS Institute
- Distribution-specific security resources
- Other mailing lists and web sites

When your site has been attacked

Recommended reading

Chapter 28 Monitoring

Table of Contents

An overview of monitoring

- Instrumentation
- Data types
- Intake and processing
- Notifications
- Dashboards and UIs

The monitoring culture

The monitoring platforms

- Open source real-time platforms
 - Nagios and Icinga
 - Sensu
- Open source time-series platforms
 - Graphite
 - Prometheus
 - InfluxDB
 - Munin
- Open source charting platforms
- Commercial monitoring platforms
- Hosted monitoring platforms

Data collection

- StatsD: generic data submission protocol
- Data harvesting from command output

Network monitoring

Systems monitoring

- Commands for systems monitoring
- collectd: generalized system data harvester
- sysdig and dtrace: execution tracers

Application monitoring

- Log monitoring
- Supervisor + Munin: a simple option for limited domains
- Commercial application monitoring tools

Security monitoring

- System integrity verification
- Intrusion detection monitoring

Table of Contents

SNMP: the Simple Network Management Protocol

- SNMP organization

- SNMP protocol operations

- Net-SNMP: tools for servers

- Tips and tricks for monitoring

- Recommended reading

Chapter 29 Performance Analysis

- Performance tuning philosophy

- Ways to improve performance

- Factors that affect performance

- Stolen CPU cycles

- Analysis of performance problems

- System performance checkup

 - Taking stock of your equipment

 - Gathering performance data

 - Analyzing CPU usage

 - Understanding how the system manages memory

 - Analyzing memory usage

 - Analyzing disk I/O

 - fio: testing storage subsystem performance

 - sar: collecting and reporting statistics over time

 - Choosing a Linux I/O scheduler

 - perf: profiling Linux systems in detail

- Help! My server just got really slow!

- Recommended reading

Chapter 30 Data Center Basics

- Racks

- Power

 - Rack power requirements

 - kVA vs. kW

 - Energy efficiency

Table of Contents

Metering

Cost

Remote control

Cooling and environment

Cooling load estimation

Roof, walls, and windows

Electronic gear

Light fixtures

Operators

Total heat load

Hot aisles and cold aisles

Humidity

Environmental monitoring

Data center reliability tiers

Data center security

Location

Perimeter

Facility access

Rack access

Tools

Recommended reading

Chapter 31 Methodology, Policy, and Politics

The grand unified theory: DevOps

DevOps is CLAMS

Culture

Lean

Automation

Measurement

Sharing

System administration in a DevOps world

Ticketing and task management systems

Common functions of ticketing systems

Ticket ownership

User acceptance of ticketing systems

Table of Contents

Sample ticketing systems

Ticket dispatching

Local documentation maintenance

Infrastructure as code

Documentation standards

Environment separation

Disaster management

Risk assessment

Recovery planning

Staffing for a disaster

Security incidents

IT policies and procedures

The difference between policies and procedures

Policy best practices

Procedures

Service level agreements

Scope and descriptions of services

Queue prioritization policies

Conformance measurements

Compliance: regulations and standards

Legal issues

Privacy

Policy enforcement

Control = liability

Software licenses

Organizations, conferences, and other resources

Recommended reading

Index

A Brief History of System Administration

Colophon

About the Contributors

Table of Contents

Past Contributors

About the Authors