

# INDEX

## Symbols and Numbers

2FA (two-factor authentication),  
28–33

3164 syslog protocol, 143

5424 syslog protocol, 143

*/etc/group*, 22

*/etc/pam.d/common-password*, 15

*/etc/pam.d/sshd*, 30

*/etc/passwd*, 146

*/etc/resolv.conf*, 134

*/etc/shadow*, 22

*/etc/ssh/sshd\_config*, 32

*/etc/ufw/user.rules*, 52

*/home/bender/google\_authenticator*, 35

*/home/bender/.ssh/authorized\_keys*, 27

*/opt/engineering*, 19, 22, 42

*/opt/engineering/greeting.py*, 42, 46

*/opt/engineering/private.txt*, 19, 23

*/var/log*, 139

*/var/log/ufw.log*, 56

## A

Alertmanager, 111, 113, 120–123

- applying configuration changes,  
122–123
- configmap.yaml*, 121, 123
- email notifications, 121–122
- receivers, 121, 122, 123
- routing and notifications,  
121–123

alerts, 119–123

- Golden Signal, 120
- reviewing, 119–120
- routing, 121–123
- states, 120

Ansible

- apt module, 29, 39

- authorized\_key* module, 27
- blockinfile* module, 32
- commands, 9
  - ansible, 9, 30
  - ansible-playbook, 9, 11, 30
- copy* module, 30, 40
- file* module, 19
- group* module, 18
- handler, 33
- hostvars, 43
- installation, 7
- lineinfile* module, 15, 31, 32, 52
- lookup function, 27
- notify, 32
- package* module, 14
- playbook, 8
  - import\_tasks*, 8
- service* module, 33
- set\_fact* module, 42
- systemd* module, 41
- template module, 42
- ufw* module, 51
  - allow rule, 51
  - deny rule, 51
  - drop rule, 53
  - limit rule, 51
  - logging parameter, 51
  - reject rule, 51
- user* module, 16–17
  - group assignment, 19
  - options, 17, 19

*authorized\_keys.yml*, 27

awk command, 147–148

## B

*banner.go*, 102

bbs-warrior, 114–115

## C

- cgroups, 64–65
- CI/CD, 96–97, 105–106
  - ArgoCD, 106
  - code changes, 102, 103
  - delivery strategies
    - blue-green, 96–97
    - canary, 96–97
    - rolling, 96–97
  - GitLab CI/CD, 106
  - Jenkins, 106
  - pipelines, 97–105
- CM (configuration management), 4
- command-and-metadata-test.yaml*, 99
- commands, Docker
  - exec, 71
  - history, 73
  - inspect, 72, 142
  - ps, 142
  - rm, 72
  - stats, 74
  - du, 139
- complex passwords, 14–18
- containers, 61
- container-structure-test, 97
  - commandTests, 99
  - metadataTest, 99
- continuous integration and continuous deployment.  
*See* CI/CD

## D

- debugging, 125. *See also* troubleshooting
- declarative configuration style, 6, 88
- deployment.yaml*, 83, 89, 91–92, 98
- developers* group, 18, 22, 38, 42
- developers.j2*, 43
- development pipeline, 100–102
- df, 138
- dfid.pub*, 27
- DHCP (Dynamic Host Configuration Protocol), 5, 55
- dig, 136–137
- dmesg, 133, 144
- DNS (Domain Name System), 133–134
  - A record, 136

- Docker, 62, 72
  - client connectivity, 66
  - client installation, 66
  - commands
    - exec, 71
    - history, 73
    - inspect, 72, 142
    - ps, 142
    - rm, 72
    - stats, 74
    - du, 139
  - container images and layers, 62, 64
  - Dockerfiles, 62
    - instructions, 63
    - multistage build, 67
  - framework, 63
  - getting started, 62
  - installation, 65–66
  - namespaces and cgroups, 64–65
  - registry, 62
  - union filesystem (UFS), 64
- Dynamic Host Configuration Protocol (DHCP), 5, 55

## E

- errors
  - connection refused, 140–142
  - connection timeout, 140
  - high load average, 127–129
  - high memory usage, 129–131
  - high iowait, 131–133
  - hostname resolution failure, 133–138
  - out of disk space, 138–139

## F

- find, 138–139
- firewalls, 49–58
  - host-based, 49–58
  - network firewall, 49
- firewall.yml*, 51
- Firing alert state, 120
- free, 129–130

## G

- getent, 22
- Go programming language, 98

- go test, 98
- Golden Signals, 115
  - errors, 115
  - latency, 115
  - reviewing alerts in
    - Prometheus, 119
  - saturation, 115
  - traffic, 115
- Google Authenticator, 28–30, 34
- Grafana, 111, 113
  - grafana-service, 113
  - telnet-server Dashboard, 116
- greeting\_application\_file*, 42
- greeting.service*, 40
- Greeting web application, 45
  - greeting.py*, 40, 46
  - installing, 39
  - wsgi.py*, 40
- grep, 146
- gunicorn3, 39

## H

- head, 138
- HighConnectionRatePerSecond
  - alert, 120
- HighCPUThrottleRate alert, 120
- HighErrorRatePerSecond alert, 120
- high iowait, 131

## I

- IaC (Infrastructure as Code), 3, 4
- idempotent, 15
- imperative, 87
- Inactive alert state, 120
- iostat, 132
- iotop, 133
- ip command, 54
- iptables, 50

## J

- journal, 143
- journalctl, 144
  - common commands,
    - 144–145
  - priority level, 145
  - reverse order, 144
- journalld, 144

## K

- K8s. *See* Kubernetes
- kubectl client, 78, 112, 144
  - apply, 88, 93, 104, 112, 122
  - cluster-info, 82
  - create, 87
  - delete pod, telnet-server, 92
  - explain, 84
  - get, 88
  - get cronjobs.batch, 114
  - get deployment, 93
  - get endpoints, 91
  - get pods, 88, 103, 92, 105
  - get services, with label flag, 89
  - logs, 93
  - logs, Alertmanager, 123
  - rollout, 104, 105, 122
  - scale, 92
- Kubernetes, 77
  - cluster connectivity, 82
  - cluster overview, 78
  - Configmaps, 81
  - Control Plane nodes, 78
  - Deployments, 79
  - general overview, 78
  - kubectl, 82
  - manifest, 79
    - containers, 86
    - labels, 83
    - metadata name field, 84
    - replicas, 85
    - selector field, 85
    - Service fields, 87
    - spec, 85
    - template, 85
    - top-level fields, 83
  - Namespaces, 81, 112
  - node, 78
  - node affinity, 78
  - Pods, 79
  - replicas, 79
  - ReplicaSet, 79
  - reviewing manifests, 82
  - rollout history, 104
  - routing alerts, 121
  - scale, 89
  - Secrets, 81
  - Service resource, 87

- Kubernetes (*continued*)
  - Services, 80
    - ClusterIP, 83, 89
    - EXTERNAL-IP, 90, 103
    - LoadBalancer, 83, 89
    - NodePort, 113
  - StatefulSets, 80
  - strategy field, 85
  - troubleshooting, 91
    - ImagePullBackOff, 91
  - Volumes, 80
  - worker nodes, 78
  - workload resources, 79

## L

- libpam-google-authenticator, 29
- libpam-pwquality, 14
- Linux groups, 18
- Linux user types
  - normal, 16
  - root, 16
  - system, 16
- load average, 127
- logrotate, 139
- logs, 109, 143–144
  - /var/log/auth.log*, 35, 47, 143, 146
  - /var/log/dmesg*, 144
  - /var/log/kern.log*, 143
  - /var/log/syslog*, 35, 47, 143, 146
  - searching, 142–148
- lo (loopback), 55
- lsuf, 133, 139
- ltrace, 151

## M

- mean time to recovery (MTTR), 105
- memory manager (OOM), 143
- metrics, 109, 115–119
  - flapping, 119
  - patterns, 116
    - RED, 116
    - USE, 116
- microservice, 115
- minikube
  - commands
    - ip, 74
    - kubect1, 82, 84, 87

- service, 90, 113
- tunnel, 89, 103
- installing, 65
- mkpasswd, 17
- modules, Ansible
  - apt, 29, 39
  - authorized\_key, 27
  - blockinfile, 32
  - copy, 30, 40
  - file, 19
  - group, 18
  - lineinfile, 15, 31, 32, 52
  - package, 14
  - service, 33
  - set\_fact, 42
  - systemd, 41
  - template, 42
  - ufw, 51
  - user, 16–17
- monitoring sample application,
  - 111–115
    - monitoring* directory, 112
    - monitoring stack, 110
      - installing, 112
      - telnet-server, 111
      - verifying installation, 113
- MTTR (mean time to recovery), 105

## N

- nameserver, 134
- Namespaces, 64–65, 81, 112
- netstat, 141
- nginx, 39
- nmap (network mapper), 55, 57
  - fast scan, 56
  - filtered, 56
  - scanning ports, 55
  - service names and versions, 56

## O

- oathtool, 28, 35
  - installing, 35
- observability, 109
- OOM (out of memory manager), 143
- orchestration, 77
- OS-level virtualization, 62

## P

- pam\_google\_authenticator.so*, 30
- PAM (Pluggable Authentication Module), 14
- pam\_pwquality*, 14–15, 17–21
- parsing logs, 146
- passphrase, 26
- Pending alert state, 120
- Persistent Volume (PV), 80
- probing processes, 148
- Prometheus, 111, 114
  - alert rule, configuration, 119
  - Alerts page, 120
  - configmap.yaml*, 114, 119
  - prometheus.rules*, configuration, 119
  - prometheus-service*, 114
  - running a query web interface, 118
  - severity Critical, rule label, 120
- PromQL, 118
- provisioning, 3
  - firewall, 53
  - SSH, 33
  - sudoers, 44
  - user and group, 20
- ps*, 129, 131
  - CMD column, 131
  - Public Key pair, 26
  - RSS column, 131
- public keys
  - authentication, 26–28
  - copying, 27
  - rsa, 27
- PV (Persistent Volume), 80
- pwgen*, 17
- python3-flask*, 39

## R

- resident set size (RSS), 131
- resolv.conf*, 134
  - edns0*, 135
  - trust-ad*, 135
- resolvectl*, 135
- resolver, 135
- restart\_ssh.yaml*, 33

- RollingUpdate, 85
- RSS (resident set size), 131
- runbook, 120

## S

- Secure Shell (SSH). *See* SSH (secure shell protocol)
- service.yaml*, 83, 87, 91
- shadow file, 17. *See also* */etc/shadow*
- site.yaml*, 8, 20, 33, 44, 53
- skaffold, 97, 100
  - build section, 98
  - deploy, 100–101
  - deploy section, 99
  - dev, 100, 102
  - reviewing, 98–99
  - skaffold.yaml*, 98, 100
  - structureTests*, 99
  - test section, 98
- socket statistics (*ss*), 140–141
  - listening, 140
  - socket owner, process, 140
- ssh-keygen*, 26
- SSH (secure shell protocol), 7, 25
  - session, 145
- SSH server
  - AuthenticationMethods, 31
  - ChallengeResponseAuthentication, 32
  - configuring, 31
  - keyboard-interactive, 31
  - Match, 32
  - publickey, 31
  - restarting with Ansible handler, 32
- strace*, 133, 148
  - follow child processes, 149
  - output to file, 150
  - PID, 149
  - string size, 149
  - summary, 149
  - track specific system calls, 150
- sudo*, 37, 38, 47
- sudoers, 38, 42, 45, 146
  - Aliases, 41
  - Cmd\_Alias, 43
  - creating file, 42
  - Defaults, 41

- sudoers (*continued*)
    - file anatomy, 41
    - Host\_Alias, 43
    - Jinja2 template, 43
    - LOCAL\_VM, 43
    - policy planning, 38
    - testing sudoers policy, 45
      - accessing Greeting, 45
      - editing *greeting.py*, 46
      - sudoedit, 46
      - systemctl start and stop, 46
    - User Specifications, 41
    - validate, 43
  - sudoers.yml*, 42
  - sudo su, as bender user, 22
  - syslog*, 149
    - 3164 protocol, 143
    - 5424 protocol, 143
    - format, 143
  - system calls
    - accept4, 149
    - close, 149
    - recvfrom, 149
    - sendto, 149
  - systemd*, 39, 43, 46
    - reload, 41
    - resolved, 134
    - resolver, 135
    - systemctl, 46
- T**
- tail, 76, 144
  - tcpdump, 141
  - TCP three-way handshake, 142
  - telnet, 89, 94, 103, 105
  - telnet-server, 86, 88, 89, 92, 98, 101, 104
    - accessing via Kubernetes, 89
    - creating Deployment and Services, 87
    - Deployment manifest, 44
    - get deployments, 88
    - Grafana dashboard, 117
    - metric Service, 87
    - Pod
      - killing, 92
      - logs, 93–94
    - scaling Deployment, 92
    - Service manifest, 87
    - rollback, Kubernetes, 104
    - telnet-server-metrics, service
      - name, 89
    - telnet via Kubernetes, 91
    - testing Kubernetes deployment, 89
  - telnet-server (application), 66
    - building container image, 68
    - connecting, 74
    - containerizing, 66
    - Dockerfile, 67
    - getting logs, 75
    - Grafana dashboard, 117
    - running container, 70
    - testing with telnet, 74, 103, 105
    - verifying container image, 69
  - three-way handshake, 142
    - ACK, 142
    - SYN, 142
    - SYN-ACK, 142
  - time-based one-time password (TOTP), 28
  - top, 128
    - COMMAND column, 128
    - CPU percent column, 128
    - MEM percent column, 128
    - PID column, 128
    - RES column, 128
    - output, 128
  - traces, 109
  - troubleshooting, 125–142
    - connection refused error, 140–142
    - high iowait, 131–133
    - high load average error, 127–129
    - high memory usage error, 129–131
    - hostname resolution failure, 133–137
    - out of disk space error, 138–139
  - two-factor authentication (2FA), 28–33
  - two\_factor.yml*, 28, 29, 30, 33
- U**
- Ubuntu VM setup, 9–11
  - UFW (Uncomplicated Firewall), 50
    - BLOCK, 57
    - chains, 50
    - LIMIT BLOCK, 58
    - logging, 56–57

- rate limiting, 57–58
- rules, 50
- testing, 54

uptime, 127

*user\_and\_group.yml*, 16, 18–20

## **V**

Vagrant, 4

- commands, 6
  - vagrant plugin install, 5
  - vagrant provision, 21, 34, 45, 54
  - vagrant ssh, 21
  - vagrant status, 11
  - vagrant up, 9, 11
- guest additions, 4

- installation, 4
  - vagrant* user, 21, 22, 31
- Vagrantfile, 4, 54
  - box, 5
    - networking, 5–6
    - providers, 6
- Vagrantfile, 4, 54
- visudo, 43
- vmstat, 129, 130, 132

## **W**

*web\_application.yml*, 39

## **Y**

YAML (Yet Another Markup Language), 6, 83, 98