INDEX

A

access permissions, 234
addgroup command, 274
agent.forwarder field, 195
Agent policies tab, 116
Amazon services, 164–166
Ansible, 113, 228
    ansible_play_batch object, 243
    becoming a superuser, 236
        markers, 244
    check mode, 233
    commands
        ad hoc, 233
        vars_files, 238
        vars_prompt, 239
    debug task, 254
    delegation, 241
    files
        ansible.cfg, 233
        ca-intermediate.yml, 262
        client-ssl.properties.j2, 251
        elasticsearch-user-passwords.yml, 255
        etchosts-all.yml, 242
        firewall-allow-ssh.yml, 248
        git-clone.yml, 250
        gpg-add.yml, 254
        inventory.conf, 231
        inventory-oneshot.yml, 268
        Kafka *client-ssl.properties*, 251–252
        kafka-configs.yml, 252
        kibana-encryption-keys.yml, 243
        newuser.yml, 240
        playbook_api_interaction.yml, 256
        playbook_basicauth.yml, 258
        playbook_newuser.yml, 238, 240
        playbook_template.yml, 252
        playbook_tls.yml, 266
        tarball.yml, 249
        tls-cachain.yml, 263
        tls-caroot.yml, 261
        tls-cert-flex.yml, 264
        tls-jks.yml, 266
        tls-pkcs12.yml, 265
        tls-setup.yml, 260
        vars.yml, 237, 249, 251, 253
        vault.yml, 237, 251
    fleet server, 256
    gathering system facts, 229
    hostvars object, 242
    installation, 230
    inventory, 228, 231
        dynamic, 232
    Jinja, 228
        from_json function, 259
        lookup function, 243, 259
        syntax, 242
        to_json function, 259
    loops, 260
    markers, 244
    modules
        ansible.posix.firewalld, 248
        apt, 236
        apt_key, 253
        blockinfile, 242–244, 263, 269, 297
        capturing output, 268
        command, 235
        community.general.ufw, 248
        copy, 234, 241, 250
        debug, 268
        expect, 254
        file, 260
        firewalld, 248
        get_url, 250
        git, 250
        import_tasks, 240
        include_tasks, 252
        java_keystore, 266
        local_action, 241, 269

Ansible *(continued)*
openssl_certificate, 265
openssl_csr, 261–262, 264
openssl_pkcs12, 265
openssl_privatekey, 261, 264
package, 236
passlib (Python), 238
reboot, 237
replace, 252
rpm_key, 253
set_fact, 257
shell, 235
shutdown, 237
systemd, 249
systemd_service, 236
template, 252
ufw, 249
unarchive, 250
uri, 258
user, 239–240
x509_certificate, 261, 263
patterns, 234
playbooks, 229
plays, 229
responding to prompts, 254
roles, 229
service restarts, 237
states, 236
superuser password, 236
task files, 240
templates, 229, 297
TLS automation, 260
variables
ansible_host, 242
inventory_hostname, 242
inventory_hostname_short, 242
vaults, 237
verbosity levels, 268
when statement, 248
ansible-inventory command, 231
ansible-playbook command, 239, 253
ansible-vault command, 237, 251
application programming interfaces (APIs), 7
asymmetric encryption, 14
AWS (Amazon Web Services), 164–165

B

Background Intelligent Transfer Service (BITS), 84, 94
backpressure, 54
bash profile, 238
Beats, 26, 122
keystore, 106
Boolean values, 9
bottlenecks, 4

C

cache, 8
drift, 296, 303
tools, 272
certificate authority (CA), 14
chain files, 22
generating, 15
intermediate configuration, 20
intermediate signing, 21
root configuration, 16
root generation, 19
self-signed, 20
certificate signing requests, 14, 56
Cisco, 54
clean-and-reload-filebeat.sh file, 59
Client Hello message, 14
clusters, 10
codecs
json_lines, 152, 160
line, 152, 160
nmap, 152, 154
plain, 152
comma-separated values (CSV), 5
conditional statements, 66
Filebeat processors, 66
use in processors, 68
consumers, 204–205
creating a new branch, 41
cURL, 78
curl commands, 87, 107, 303
custom headers, 155
custom indicator uploads, 303

D

data engineering, xxi
data enrichment, 185, 225–226
data pipelines, 6, 10
data serialization formats, 8

deserialization, 8
directional tags, 185
Domain Name System (DNS) hostname resolution, 56

E

ECMAScript, 67
Elastic Agent, 6, 98–99
  architecture, 98
  certificate locations, 119
  downloading, 112, 114
  fleets, 98
  fleet server, 99
  incident response procedures, 118
  installation, 112, 114
    failure, 113
    stand-alone, 122
  integrations, 116
  wildcard configuration file, 100
elastic-agent.yml file, 121
Elastic Common Schema (ECS), 10, 53–54
Elastic Defend tamper protection, 119
Elasticsearch, 6, 99
  API status, 107
  `_cat/health`, 107
  `_cluster/health`, 107
  `curl` commands, 107
  downloading, 104
  elasticsearch-reset-password program, 255
  `filter_path`, 107
  heap.options file, 106
  ingest pipelines, 123
    creating custom, 123
    renames, 69
  installation, 104
  keystore, 106
  Logstash API key, 119, 288
  startup, 106
  system passwords, 106
elasticsearch.yml file, 105
Endgame, Elastic acquisition of, 99
enriching data, 5, 181, 225–226
/etc/hosts file, 56
event logs
  Application, 82
  file locations, 82
  PowerShell/Operational, 84
  Security, 83
  Sysmon, 83
  Windows, 82
    Defender, 83
    PowerShell, 83
`export` command, 237
Extensible Markup Language (XML), 5

F

Filebeat, 6
  certificate signing requests, 56
  connecting to external systems, 64
  dotted field names, 61
  excluding lines, 63
  `filebeat.config.modules` option, 222
  inputs
    filestream, 58
    Kafka, 64–65
  installation, 55
    Windows, 78
  modules, 69–70
    `system`, 290
    `threatintel`, 283, 290, 296
    `Zeek`, 70
  OpenSSL configuration files, 55
  outputs, 71
    file, 75
    Kafka, 73
    Logstash, 58, 76
    Redis, 74
  parsers, 60
  private keys, 56
  privatizing data, 77
  processors, 66, 71
  publishing to Kafka, 221
  Redis keys, 75
  registry files, 59
  signed certificates, 57
  subject alternative names, 56
  tagging, 63
  testing, 70
filebeat.yml file, 57
file-io.conf file, 160
file ownership, 234

firewall
clutter, 55
ports, 27
Firewalld, 27, 103, 208, 248
allowing SSH, 28
fleet servers
Ansible simulation, 256
Elastic Agent, 99
installation, 112–113
integrations, 111
new service tokens, 111
output settings, 111
role, 99
Flink, 304

G

Git, 172
adding, 34, 37, 38
branches, 34, 41
deleting, 44
checkout, 41
cloning, 34
commands
`config`, 35
`fetch`, 47
`init`, 36
`log`, 39
commits, 34, 37, 39
initializing locally, 36
merges, 34, 44
pulls, 34
rebasing, 47
rejected, 46
pushes, 34, 39
deleting, 44
rejected, 46
`set-upstream origin`, 37
remote, 43
`remote add origin`, 36
repository, 34
resetting, 47
stashing, 48
`stash pop`, 48
status, 38
`status --short`, 38, 40
GitHub, xxv, 35
.gitignore file, 40
GitLab, 35
GNU Privacy Guard (GPG), 104
Golang, 54
groups, 275

H

hosts file
on Linux, 103
on Windows, 86, 103
remembering to update, 119
Hypertext Transfer Protocol (HTTP), xxv
basic authentication, 258
input in Logstash, 154
output in Logstash, 156
hypervisor, xxiv

I

`id` command, 275
indentation, 9
integrations, 99, 116
assets, 116, 123
Elastic Agent, 116
fleet server, 111
guidelines, 117
Iptables, 117
monitor processes, 116
Network Packet Capture, 116
intel-distribute.conf file, 296
`Invoke-WebRequest` command, 78
iocs.csv file, 303
Iptables, 117

J

Java, 54
Java Development Kit, 209
Java KeyStores (JKS), 210
JavaScript, 67
JavaScript Object Notation (JSON), 9
dotted field names, 61
newline-delimited, 58
Java Virtual Machine (JVM), 106
Jinja, 228
`from_json` function, 259
`lookup` function, 243, 259
Python, 228
syntax, 242
`to_json` function, 259
`jq` tool, 11, 109
jvm.options file, 152

K

Kafka, 7, 135, 204, 225
- advertised listeners, 207
- bootstrap hosts, 207
- bootstrap servers, 65
- brokers, 64, 205
- connectors, 207
- consumer groups, 65, 135, 161, 204
- consumers, 204–205
- controllers, 205
- design considerations, 225
- Filebeat, 221
  - input, 64
  - output, 73
- files
  - *broker.properties*, 211
  - *client-ssl.properties*, 211, 214, 217, 251–252
  - *controller.properties*, 211
  - *kafka-console-consumer.sh*, 220
  - *kafka-console-producer.sh*, 217
  - *kafka-topics.sh*, 217–218
  - *server.properties*, 211, 214
- headers, 73
- *kafka* (user), 209
- listeners, 207
- Logstash, 223–224
  - input, 161, 224
  - output, 162, 223
- messages, 205
- over-provisioning, 206
- partitions, 205
  - leaders and followers, 206
  - write speed, 206
- ports, 208
- producers, 204–205
- publishing, 8, 204
- read-only replicas, 206
- replication, 206
- Rsyslog, 219
- streams, 207
- subscribing, 8, 204
  - to Kafka, 220, 222, 224
- topics, 65, 135, 205
  - creating, 217–218
  - listing, 217

kafka.service file, 215

keystore
- Elasticsearch, 106
- Kibana, 109
- Logstash and Beats, 106

keytool, 210

Kibana, 99
- dark mode, 110
- Dev Tools, 288
- Discover, 114
- downloading, 108
- generating encryption keys, 108
- GUI browser address, 110
- keystore, 109
- *kibana.yml* file, 108, 244
- `network.direction` query, 185
- searching for IPs/CIDR, 115
- search syntax, 115, 117

KRaft, 204

L

latency, 4

libbeat library, 94

load balancing, 4

Logstash, 6, 114
- API key, 288
  - for Elasticsearch, 119
- backpressure, 54
- *beats-mtls.conf* upgrade, 122
- codecs, 152
  - `json_lines`, 152, 160
  - `line`, 152, 160
  - `nmap`, 152, 154
  - `plain`, 152
- configuration, 26
  - flex, 23
  - test, 27
- control flow, 186
- downloading, 25
- `elastic_agent` accepting Beats, 122
- field comparisons, 187
- files
  - *display-stdout.conf*, 171
  - *elasticagent-mtls.conf*, 121
  - *file-io.conf*, 160
  - *generator-to-pipeline.conf*, 170
  - *grok-dissect-date.conf*, 176
  - *http-poller.conf*, 158
  - *logstash-input.conf*, 168

Logstash *(continued)*
logstash-output.conf, 168
memcached-get-indicators.conf, 300
memcached-set-indicators.conf, 298
nmap-http.conf, 153
pipelines.yml, 167, 169, 171, 282
plain-kafka-consumer.conf, 72
redis-set-indicators.conf, 283
ruby-simple.conf, 195
s3-input.conf, 165
s3-output.conf, 166
filters. *See* Logstash filters
inputs
beats, 26
elastic_agent, 121, 283
file, 159
generator, 175
http, 283
HTTP, 154
http_poller, 156, 158
Kafka, 161, 224
logstash, 167, 298
plaintext Kafka, 72
Redis, 163
S3, 165
syslog, 26
syslog TCP, 143
installation, 150
install plugin, 152
_jsonparsefailure tag, 159
Kafka, 223–224
keystore, 106
to Logstash, 167
metadata fields, 76
outputs
elasticsearch, 289
file, 160
Filebeat, 58, 76
HTTP, 156
Kafka, 162, 223
logstash, 296
null, 170, 300
Redis, 164
S3, 166
parentheses, 188
publishing to Kafka, 223
restricting outward flow, 297
running, 27, 59
configurations, 151
pipelines, 169
setting up TLS, 23
subscribing to Kafka, 224
test command, 122
testing configuration, 151
virtual addresses, 170
whitespace, 153, 174
Logstash filters, 174
arrays, 189
avoiding backslashes, 192
CIDR, 181
comparisons
array, 189, 196
field, 187
number, 190
regular expression, 190
string comparison, 189
control flow, 186
csv, 285
date, 178
dictionary files, 184
directional tags, 185
dissect, 178
drop, 198–199, 285
equality and inequality, 188
extractnumbers, 174
field existence, 188
field membership, 188
grok (language), 175–176
gsub, 193–194
json, 224
kv, 191
memcached, 298
mutate, 76, 175, 178, 193, 284
copy function, 193
lowercase function, 194
remove_field function, 175
strip function, 178
parentheses, 188
prune, 191
quotation marks, 188
ruby, 286
Ruby (language), 195
sleep, 169
split, 193, 285
syntax, 174

translate, 181–182, 184, 272
unstructured data, 175
urldecode, 174
useragent, 174
loops, 197, 260
Lumberjack, 167

M

Markdown, 37
Memcached, 272, 295
configuration files
RHEL, 277
Ubuntu, 276
/etc/memcached.conf file, 276
/etc/sysconfig/memcached file, 277
get command, 280
installation, 273
set command, 279
telnet, 279
MinIO, 164
module logging, 84, 93
mutate filter
copy function, 193
Logstash, 175, 178, 193, 284
lowercase function, 194
remove_field function, 175
strip function, 178
mutual TLS (mTLS), 15

N

needless complexity, 6
Network Address Translation (NAT), 11
newline-delimited JSON (NDJSON), 58
Nmap, 155
Notepad++, 11

O

OpenJDK, 209
OpenSSL, 16
chain files, 111
CA, 57
client configuration files, 85
commands
CA, 18, 21, 24, 101
pkcs12, 102
rand, 275
req, 18–19, 21, 24, 86, 101, 130
rsa, 130
s_client, 282
verify, 22, 25, 57, 86, 102, 131
x509, 19, 22, 102, 131
default_md key, 18
Filebeat
certificate signing requests, 56
configuration files, 55
private keys, 56
signed certificates, 57
flex certificates, 23
PKCS#12, 102, 265
Rsyslog configuration file, 130
signing_policy section, 18
subject alternative names, 56
subject_key_identifier section, 19
unencrypted private keys, 102
wildcard certificates, 100
openssl pkcs12 module, 210, 265
origin (Git), 38

P

P12 file, 210
Packetbeat, 98, 116
Palo Alto Networks, 54
parsers, 60–62
ndjson, 60
PFX file, 210
PKCS#12, 102, 265, 297
pkcs12 command, 102, 210
PowerShell
execution policy, 89
list available event logs, 94
module logging, 93
script blocks, 84, 91–93
private keys, 14, 56
unencrypted, 102
processors, 65
add_tags, 66
conditional statements in, 68
drop_fields, 69, 77
dropping event codes, 95
Filebeat, 66, 71
script, 67, 77
timestamp, 68
Winlogbeat, 94
producers, 204–205
Project Discovery, 57
public keys, 14, 35

PuTTY, 11
Python
    Flask, 157
    Jinja, 228
    `passlib` module, 238
    `subprocess` module, 235
    virtualenv package, 157
    web server, 87, 104, 211, 274

R

RainerScript, 133
README.md file, 37
Red Hat Enterprise Linux (RHEL), 10
    Memcached configuration files, 277
Redis, 162, 272
    channel mode, 162
    commands
        `acl`, 278
        `get`, 278
        `info`, 278
        `set`, 277
    configuration files, 275
    cyber threat intelligence node, 281
    Filebeat output, 74
    followers, 280, 291
    installation, 273
    leaders, 280
    list mode, 162
    Logstash input, 163
    Logstash output, 164
    maintenance, 295
    redis.conf file, 275, 291
    redis-get-indicators.conf file, 292
    replication, 280
    Ruby filters, 287
    Ruby gem, 273
`redis-benchmark` command, 279
`redis-cli` command, 277, 292
regular expressions, 142, 176, 190
retro hunts, 288, 304
RFC 3164 format, 62, 128, 175
RFC 5424 format, 62, 128, 137, 191
RHEL (Red Hat Enterprise Linux), 10
    Memcached configuration files, 277
Rsyslog, 6, 129, 219
    actions, 137, 141
    advanced format, 133
    basic format, 132
    case-insensitive
        match, 145
        regex, 142
        string, 141
    compressing whitespace, 140
    configuration
        client, 144
        main, 132
        OpenSSL, 130
        server, 144
        testing, 133
    `constant` keyword, 139
    creating new variables, 142
    dynamic filenames, 140
    /etc/rsyslog.d/ directory, 132
    files
        /etc/rsyslog.conf, 132
        rsyslog-imkafka.conf, 220
        rsyslog-omkafka.conf, 219
        send-to-filebeat.conf, 63
    global TLS settings, 134
    input modules, 134
        `imfile`, 136
        `imkafka`, 135, 220
        `imptcp`, 134–135, 145
    installation, 129
    Kafka, 219
    OpenSSL configuration file, 130
    output modules, 136
        `jsonify`, 140
        `omfile`, 136
        `omfwd`, 137, 144
        `omkafka`, 219
    properties, 138
        global, 133
        `rawmsg`, 140
    `property` keyword, 139
    property replacer, 138, 142
    publishing to Kafka, 219
    regular expressions, 142
    replacing text, 141
    rulesets, 141
    `sp-if-no-1st-sp` modifier, 142
    stream drivers, 135
    subscribing to Kafka, 220

templates, 137, 145
list, 139
string, 138
Ruby, 54, 195
Redis gem, 273
Ruby filters
array comparison, 196
`code` option, 195, 287, 293
deduplicate tags, 294–295
`init` option, 195, 287, 293
loops, 197
Redis, 287
`require` command, 196
`socket` class, 196
value conversions, 198

S

S3, Amazon, 164–166
script block logging, 84, 91
Secure Shell (SSH), xxv, 27, 35
agent, 29, 35, 230
alias, 29
configuration files, 29, 35, 233
creating keys, 28
enabling, 28
hardening, 31
`IdentityFile` command, 35
`publickey` key, 35
`ssh-copy-id` command, 30
tunnels, 27, 163
security information event manager (SIEM), 3
semistructured data, 5
serialization, 8
Server Hello message, 14
server.properties file, 211–212
service restarts, 237
Splunk, 156
stand-alone agent
configuring a policy, 120
elastic-agent.yml file, 121
installation, 122
policy, 118
preparing, 119
standardizing data, 5
building data pipelines more easily, 10
structured data, 5
Structured Query Language (SQL), 5
subject alternative names (SANs), 18, 56
IP addresses, 24
Subject Distinguished Name (DN), 18
symmetric encryption, 15
syslog, 128
Sysmon, 90
downloading, 90
event logs, 83
Hartong, Olaf, 90
installation, 91

T

`tar` command, 210
telnet, 279
temporarily stashing changes, 48
temporary data centralization, 7
throughput, 4
time-series data, 5
Transmission Control Protocol (TCP), xxiv
truststores, 211

U

Ubuntu, 10
Memcached configuration files, 276
virtual machines, 103
Uncomplicated Firewall (UFW), 27, 62, 116, 208, 248, 282
allowing SSH, 28
Unix sockets, 276, 287
unstructured data, 5, 175
`update-ca-certificates` command, 275
`useradd` command, 209
User Datagram Protocol (UDP), xxiv
`usermod` command, 70, 274

V

version control systems, 34
virtual environments, 157
virtual machines, xxiv, 10, 103
Visual Studio Code, 11

W

`watch` command, 76
`wget` command, 210–211, 274
wildcard configuration files, 100

Windows
event logs, 82
free evaluation copy, 10
Windows Event Collector (WEC), 82
`winget` command, 34
Winlogbeat, 6, 82
downloading, 84
dropping BITS events, 94
installation, 10
service, 89–90
OpenSSL client configuration files, 85
processors, 94
winlogbeat.yml, 87
WinSCP, 11, 87

X

XML (Extensible Markup Language), 5
`Xms` (minimum) value, 106
`Xmx` (maximum) value, 106

Y

YAML Ain't Markup Language (YAML), 9

Z

Zeek, 54, 69, 116
zero-trust environments, 15
Zookeeper, 204