

Table of Contents

Preface	1
Chapter 1: Introducing Kibana	9
Elastic Stack	10
Elasticsearch	11
Logstash	12
Kibana	13
Beats	14
Filebeat	15
Metricbeat	15
Packetbeat	15
Auditbeat	16
Winlogbeat	16
Heartbeat	17
Use cases of Elastic Stack	17
System Performance Monitoring	18
Log Management	18
Application Performance Monitoring	18
Security, Monitoring, and Alerting with Elastic Stack	19
Security	19
Monitoring	19
Alerting	19
Data Visualization	20
Installing Elastic Stack	20
Elasticsearch	21
Installation using the tar file	21
Installation using Homebrew	21
Installation using MSI Windows installer	21
Installation using the Debian package	22
Installation with the RPM package	22
Logstash	23
Using APT Package Repositories	23
Using YUM Package Repositories	24
Kibana	24
Installing Kibana with .tar.gz	25
Installing Kibana using the Debian package	25
Installing Kibana using RPM	26
Using zypper on OpenSUSE-based distributions	26
Installing Kibana on Windows	27
Beats	27
Packetbeat	27
Metricbeat	28

Filebeat	29
Summary	30
Chapter 2: Getting Data into Kibana	31
Difference between Beats and Logstash	32
Configuring Beats to get data	32
Filebeat	33
Packetbeat	36
Metricbeat	39
Configuring Logstash to get data	40
Configuring Logstash to read CSV data	41
Configuring Logstash to read RDBMS data	43
Configuring index patterns in Kibana	47
Summary	51
Chapter 3: Exploring Data	53
Discover your data	54
Limit Your Field Display	55
Expanded View of the Data	56
Dissect Your Data	57
The time Filter	57
The Quick Time Range Filter	58
The Relative Time Range Filter	58
The Absolute Time Range Filter	59
The Recent Time Range Filter	59
Search bar to search your data	60
Filter Your Data	61
Save Your Filtered Data	64
Save Your Search	64
Manage Saved Searches	66
Summary	67
Chapter 4: Visualizing Data	69
Data visualization	70
Data aggregation	70
Visualization types	71
Area chart	72
Heat map	74
Pie chart	76
Data table	78
Metric	79
Tag cloud	81
Inspecting visualizations	82
Sharing a visualization	83
Dashboard	86
Summary	91

Chapter 5: X-Pack with Machine Learning	93
Introduction to X-Pack	94
Installation	94
Security	96
Role management	97
User management	99
Monitoring	101
Alerting	102
Reporting	106
Machine learning	108
Single-metric job	109
Multimetric job	111
Summary	114
Chapter 6: Monitoring Applications with APM	115
APM components	116
APM agents	117
APM Server	119
Install APM Server	121
APT	121
YUM	122
Install APM Server on Windows	122
Run APM Server	123
Configure dashboard using APM Server	123
APM Server monitoring	124
Elasticsearch	125
Kibana	125
Configure Django application with APM	125
Summary	131
Chapter 7: Kibana Advanced Tools	133
Timelion	134
.es() function	135
.static() function	136
.bars() function	138
.points() function	138
.color() function	139
.derivative() function	140
.label() function	140
.range() function	141
.holt() function	142
Use cases of Timelion	143
Dev Tools	147
Console	148
Search Profiler	149
Grok Debugger	150
Summary	152

Other Books You May Enjoy	153
----------------------------------	-----

Index	157
--------------	-----
