

Table of Contents

Chapter 1 - Introduction to Splunk.....	9
What is Splunk?.....	10
Install Splunk on Windows.....	10
Install Splunk on Linux.....	16
Access Splunk web interface.....	18
Chapter 2 - First steps.....	23
Splunk Home.....	24
Data sources.....	24
What is an index?.....	25
Create an index.....	25
Add data to Splunk.....	28
Chapter 3 - Searching overview.....	37
Launch search app.....	38
Search rules.....	39
Example search.....	39
Boolean expressions.....	41
Fields.....	42
Pipes.....	44
Time range picker.....	45
top command.....	48
stats command.....	49
sort command.....	49
where command.....	50
Chapter 4 - Collecting Windows logs.....	55
Windows inputs.....	56
Collect event logs from a local Windows machine.....	56
Collect performance counters.....	60
Collect Windows host information.....	66
Chapter 5 - Universal forwarders.....	75
What are universal forwarders?.....	76
Set up a receiver.....	76
Install a Splunk forwarder on Windows.....	78
Starting and stopping universal forwarders.....	81
Monitor logs using forwarders.....	81

Monitor remote Windows event logs.....	83
Install a Splunk forwarder on Linux.....	84
Configure a Splunk forwarder on Linux.....	86
Chapter 6 - Alerting and reporting.....	91
Alerts overview.....	92
Create an alert.....	92
Create an alert that runs a script.....	94
Reports overview.....	95
Create a report.....	96
Share a report.....	98