

# **for509\_index**

## **accessing aws**

FOR509 - Book 3.pdf : 24,25,73

## **amazon detective**

FOR509 - Book 3.pdf : 138,139,140,145

## **amazon lightsail**

FOR509 - Book 3.pdf : 75

## **application logs**

FOR509 - Book 1.pdf : 18,23

FOR509 - Book 2.pdf : 16

FOR509 - Book 3.pdf : 98,100,101,130

FOR509 - Book 4.pdf : 18

FOR509 - Book 5.pdf : 60

## **assisted log enabler**

FOR509 - Book 3.pdf : 136,137

## **athena**

FOR509 - Book 3.pdf : 29,91,119,131,132,133,134,135,136,137

## **aws audit manager**

FOR509 - Book 3.pdf : 7,8

## **aws dns**

FOR509 - Book 3.pdf : 106,107

## **aws organizations**

FOR509 - Book 3.pdf : 5,67

## **aws security analytics bootstrap**

FOR509 - Book 3.pdf : 137

## **aws security reference architecture (sra)**

FOR509 - Book 3.pdf : 11

**aws systems manager commands to hunt for**

FOR509 - Book 3.pdf : 155

**aws transfer acceleration**

FOR509 - Book 3.pdf : 120,121

**azcopy snapshot**

FOR509 - Book 2.pdf : 88

**azure access**

FOR509 - Book 1.pdf : 90,91

**azure network security group**

FOR509 - Book 2.pdf : 107

**azure resource id**

FOR509 - Book 2.pdf : 8,9,10

**azure resource manager**

FOR509 - Book 2.pdf : 6,7,11

**azure storage explorer**

FOR509 - Book 2.pdf : 60,61,64,79,96,101,102,116,119,120

**azure structure**

FOR509 - Book 2.pdf : 4

**azure tenant**

FOR509 - Book 1.pdf : 3,93,118

FOR509 - Book 2.pdf : 4

**azure threat research matrix**

FOR509 - Book 2.pdf : 122,126

**azure virtual network (vnet)**

FOR509 - Book 2.pdf : 104

**beats**

FOR509 - Book 1.pdf : 11,13

**blobs**

FOR509 - Book 1.pdf : 45

FOR509 - Book 2.pdf : 17,46,61,63,64,96,116

**cloud access options**

FOR509 - Book 1.pdf : 21,24

**cloud models**

FOR509 - Book 1.pdf : 18

**coldsnap**

FOR509 - Book 3.pdf : 83

**costs**

FOR509 - Book 1.pdf : 27,28

FOR509 - Book 2.pdf : 48,72,122

FOR509 - Book 3.pdf : 59,152

**ebs**

FOR509 - Book 1.pdf : 29

FOR509 - Book 2.pdf : 70,88

FOR509 - Book 3.pdf : 10,17,67,68,77,78,79,80,81,82,84,86,87,92,100,121

**ec2 global view**

FOR509 - Book 3.pdf : 68,75

**ec2 types**

FOR509 - Book 3.pdf : 66

**efs**

FOR509 - Book 1.pdf : 29

FOR509 - Book 3.pdf : 73,87,88,89,90,97,151

**elastic stack**

FOR509 - Book 1.pdf : 11,12

### **entra id activity logs**

FOR509 - Book 1.pdf : 94

### **entra id incident response**

FOR509 - Book 1.pdf : 97,102

### **entra id logs**

FOR509 - Book 1.pdf : 92,93,94,98,100

FOR509 - Book 2.pdf : 36,48,50

### **etcd**

FOR509 - Book 4.pdf : 22,44,49,50,59

### **event triggers**

FOR509 - Book 3.pdf : 145,151

### **exchange mailbox actions**

FOR509 - Book 1.pdf : 48,49

### **file operations**

FOR509 - Book 1.pdf : 70,71,76,78,79,81

FOR509 - Book 5.pdf : 118

### **file sharing**

FOR509 - Book 1.pdf : 72,73,74,75

FOR509 - Book 4.pdf : 75,123,130

### **forensic vm**

FOR509 - Book 2.pdf : 85,86,89

### **glue**

FOR509 - Book 2.pdf : 104

FOR509 - Book 3.pdf : 119,131,132,133,134,135,137,147

### **google workspace admin audit logs**

FOR509 - Book 5.pdf : 47

**google workspace editions**

FOR509 - Book 4.pdf : 65,66,78

**google workspace permissions**

FOR509 - Book 4.pdf : 67

**iaas**

FOR509 - Book 1.pdf : 3,18

FOR509 - Book 5.pdf : 73

**internet gateways**

FOR509 - Book 3.pdf : 95,98

**key logs for investigations**

FOR509 - Book 1.pdf : 23

**kibana**

FOR509 - Book 1.pdf : 11

FOR509 - Book 2.pdf : 107,108,109,110

**kql**

FOR509 - Book 1.pdf : 62

FOR509 - Book 2.pdf : 54,57,126

FOR509 - Book 3.pdf : 148

FOR509 - Book 4.pdf : 29

**log analytics workspace**

FOR509 - Book 2.pdf : 48,49,50,51,52,53,54,55,61,78,97,103,112,123

FOR509 - Book 4.pdf : 28,29,30

**logstash**

FOR509 - Book 1.pdf : 11,12,13,14

FOR509 - Book 2.pdf : 17,38,116

FOR509 - Book 3.pdf : 38

FOR509 - Book 4.pdf : 108

**mailaccesstype: bind vs. sync**

FOR509 - Book 1.pdf : 52

#### **mailitemsaccessed fields for ir**

FOR509 - Book 1.pdf : 50,51

#### **management groups**

FOR509 - Book 2.pdf : 4

#### **matter**

FOR509 - Book 1.pdf : 0,6,9,103,120

FOR509 - Book 2.pdf : 0,103

FOR509 - Book 3.pdf : 0,12,53,67,104,106

FOR509 - Book 4.pdf : 0,35

FOR509 - Book 5.pdf : 0,47

#### **nat gateway**

FOR509 - Book 3.pdf : 98

#### **network acls**

FOR509 - Book 3.pdf : 99

#### **network security groups**

FOR509 - Book 2.pdf : 104

FOR509 - Book 3.pdf : 95,96,97

#### **network virtual appliance**

FOR509 - Book 2.pdf : 105

#### **nodes**

FOR509 - Book 3.pdf : 57

FOR509 - Book 4.pdf : 9,10,13,14,20,25,28,31,32,33,39,45

#### **nsg flow logs**

FOR509 - Book 2.pdf : 111,112,113

#### **ops agent**

FOR509 - Book 5.pdf : 96,97

**paas**

FOR509 - Book 1.pdf : 3,18,20

FOR509 - Book 5.pdf : 73

**playbooks**

FOR509 - Book 2.pdf : 122,125

FOR509 - Book 3.pdf : 154

**pods**

FOR509 - Book 4.pdf : 8,9,10,13,14,21,30,33,34,46,47,48,50,54,55

**policy evaluation**

FOR509 - Book 3.pdf : 16,19

FOR509 - Book 5.pdf : 16

**pricing**

FOR509 - Book 1.pdf : 21,27,28

FOR509 - Book 2.pdf : 70,71,124

FOR509 - Book 3.pdf : 67,81,104,118,132,143,144,152

**rbac**

FOR509 - Book 2.pdf : 6,7,11

FOR509 - Book 3.pdf : 25

FOR509 - Book 4.pdf : 19,29,31,32,52

FOR509 - Book 5.pdf : 4

**record type**

FOR509 - Book 1.pdf : 33,34,36,47,70,72,76,79,94

**regions**

FOR509 - Book 1.pdf : 28

FOR509 - Book 2.pdf : 70,104

FOR509 - Book 3.pdf : 32,40,67,68,80,107

FOR509 - Book 4.pdf : 64

**resource groups**

FOR509 - Book 2.pdf : 4,7,13

## **role assignments**

FOR509 - Book 1.pdf : 38

FOR509 - Book 2.pdf : 11,12,13

FOR509 - Book 4.pdf : 29

## **route 53**

FOR509 - Book 3.pdf : 106,107,108,109,130

## **s3 logging**

FOR509 - Book 3.pdf : 125,131

## **saas**

FOR509 - Book 1.pdf : 3,4,18

FOR509 - Book 4.pdf : 95

## **search examples**

FOR509 - Book 1.pdf : 16

## **security groups**

FOR509 - Book 3.pdf : 68,99

## **sentinel**

FOR509 - Book 2.pdf : 122,123,124

## **serverless**

FOR509 - Book 1.pdf : 19,29

FOR509 - Book 3.pdf : 15,49,142,143,147,151

FOR509 - Book 5.pdf : 73,74

## **sharepoint log**

FOR509 - Book 1.pdf : 80

## **sidecar**

FOR509 - Book 4.pdf : 12,19,30,34

## **step functions**

FOR509 - Book 3.pdf : 135,142,152

**storage log schema**

FOR509 - Book 2.pdf : 102

**sts tokens**

FOR509 - Book 3.pdf : 16,24,73,115

**subscriptions**

FOR509 - Book 2.pdf : 4,5,10,39,68,75,108,109,110

FOR509 - Book 3.pdf : 150

**takeout**

FOR509 - Book 4.pdf : 75,76,81,82,133,134,135,136,137,138,139,141,142

**terminology across clouds**

FOR509 - Book 1.pdf : 29

**ual in large enterprises**

FOR509 - Book 1.pdf : 44

**ual records**

FOR509 - Book 1.pdf : 33

**vault**

FOR509 - Book 1.pdf : 74

FOR509 - Book 2.pdf : 45,46

FOR509 - Book 4.pdf : 66,77,89,102,138

**vhd**

FOR509 - Book 1.pdf : 90

FOR509 - Book 2.pdf : 87,88,96

FOR509 - Book 3.pdf : 77

FOR509 - Book 4.pdf : 125

FOR509 - Book 5.pdf : 94

**virtual private cloud**

FOR509 - Book 3.pdf : 90,95,96,130

**vm creation events**

FOR509 - Book 2.pdf : 73,74

**vpc firewall rules**

FOR509 - Book 5.pdf : 129

**vpc subnets**

FOR509 - Book 3.pdf : 97

**wad**

FOR509 - Book 2.pdf : 17,78,79

**web console**

FOR509 - Book 1.pdf : 24

FOR509 - Book 3.pdf : 24,25,27,32,33,38,45,46,49,70