

AMAZON WEB SERVICES GUIDE



Version 1.8.5

Damian Ndunda

MUGUMOINI - NAIROBI

Amazon Web Services Guide

Copyright © March 2022 BICT Solutions.

Visit <https://businessict.weebly.com/cloud-computing.html>

Trademarks used belong Amazon.com, Inc. Icons used are reproduced from Amazon.com Trademark information about all of the companies and products mentioned herein are provided accordingly but cannot guarantee the accuracy of all information as information changes with time.

CONTENTS AT A GLANCE

AMAZON WEB SERVICES GUIDE.....	1
CONTENTS AT A GLANCE	3
TABLE OF CONTENTS	5
FOREWORD	54
CHAPTER – AWS INTRODUCTION	55
CHAPTER – MAIN AMAZON CLOUD WEB SERVICES	77
CHAPTER – MORE AMAZON CLOUD WEB SERVICES	167
CHAPTER – AWS SERVERLESS PLATFORMS	197
CHAPTER - CLOUD ADOPTION FRAMEWORK.....	263
CHAPTER - WORKING WITH SIMPLE STORAGE SERVICE	285
CHAPTER - IMAGES AND INSTANCES	322
CHAPTER - RESERVED INSTANCE (RI)	372
CHAPTER - AWS NETWORKING.....	376
CHAPTER – INTERNET PROTOCOL (IP) VERSION 4 AND 6	390
CHAPTER: - IPV6 ON AWS	459
CHAPTER - BUILDING YOUR OWN PRIVATE CLOUDS USING AMAZON VPC	513
CHAPTER - AMAZON VIRTUAL PRIVATE CLOUD (AMAZON VPC).....	552
CHAPTER - MONITORING YOUR AWS INFRASTRUCTURE.....	591
CHAPTER - PROGRAMMING YOUR INFRASTRUCTURE: THE COMMAND LINE, SDKS, AND CLOUDFORMATION.....	628
CHAPTER - AUTOMATING DEPLOYMENT: CLOUDFORMATION, ELASTIC BEANSTALK, AND OPSWORKS.....	684
CHAPTER - DATABASE-AS-A-SERVICE USING AMAZON RDS	727
CHAPTER - EXTENDED AWS SERVICES FOR YOUR APPLICATIONS	789
CHAPTER - AWS SECURITY	827
CHAPTER – COMMAND LINE INTERFACE	852
CHAPTER – DESIGNING FOR FAULT-TOLERANCE	992
CHAPTER – BABYLONJS BASICS	1038

CHAPTER – PENETRATION TESTING 1083
CHAPTER - TEN WAYS TO DEPLOY AWS QUICKLY 1087
CHAPTER - SERVICE CONTROL POLICIES (SCPS) 1098
CHAPTER - SIX STRATEGIES FOR MIGRATING APPLICATIONS TO THE CLOUD 1104
CHAPTER - TEN MUST-HAVE AWS SOFTWARE PACKAGES 1108
CHAPTER – AWS SUPPORT PLANS..... 1120
CHAPTER - PLANNING YOUR NEXT STEPS 1124
INDEX..... 1138
REFERENCES 1147

TABLE OF CONTENTS

AMAZON WEB SERVICES GUIDE	1
CONTENTS AT A GLANCE	3
TABLE OF CONTENTS	5
FOREWORD	54
CHAPTER – AWS INTRODUCTION	55
1 AWS DATA CENTER LOCATIONS.....	56
2 WHAT IS “CLOUD COMPUTING”?	56
Clouds are often divided into the following types:	57
■Public.....	57
■Private	57
■Hybrid.....	57
3 AMAZON AND CLOUD COMPUTING	58
AWS is a public cloud. Cloud computing services also have several classifications:	58
■Infrastructure as a service (IaaS)	58
■Platform as a service (PaaS)	58
■Software as a service (SaaS).....	58
4 CLOUD SERVICE LAYERS DIAGRAM	59
5 CLOUD SERVICE MODEL COMPARISON DIAGRAM.....	60
6 HOW YOU CAN BENEFIT FROM USING AWS	61
7 THE DIFFERENCES THAT DISTINGUISH AWS.....	61
Flexible	62
Cost-Effective	62
Scalable and Elastic	62
Secure.....	63
Physical security.	63
Secure services.	63
Data privacy.....	63
Experienced.....	63
QUESTIONS AND EXPLANATIONS:	64
Characteristics of a truly scalable application:	65

Reference:.....	65
8 HOW MUCH DOES IT COST?.....	66
FREE TIER.....	66
BILLING.....	68
Based on hours of usage.....	68
Based on traffic.....	68
Based on storage usage.....	68
Pay-per-use opportunities.....	68
QUESTIONS AND EXPLANATIONS:.....	68
AWS Storage Gateway billing is as follows.....	71
Volume storage usage (per GB per month):.....	71
Snapshot Storage usage (per GB per month):.....	71
Virtual Tape Library usage (per GB per month):.....	71
Virtual Tape Shelf usage (per GB per month):You are billed for the virtual tape data you store in Amazon Glacier. You are only billed for the portion of virtual tape capacity that you use, not for the size of the virtual tape.....	71
AWS: WHAT ARE THE SIMPLE MONTHLY CALCULATOR, COST AND USAGE REPORT, COST EXPLORER AND BUDGETS?.....	72
AWS Simple Monthly Calculator.....	72
AWS Cost & Usage Report.....	72
AWS Budgets.....	73
AWS Cost Explorer.....	73
<i>AWS GLOBAL INFRASTRUCTURE PICTURE.....</i>	<i>74</i>
<i>AWS COMPUTING PLATFORM DIAGRAM.....</i>	<i>75</i>
CHAPTER – MAIN AMAZON CLOUD WEB SERVICES.....	77
1 COMPUTE & NETWORKING.....	77
Amazon Elastic Compute Cloud (Amazon EC2).....	77
QUESTIONS AND EXPLANATIONS:.....	79
Auto Scaling.....	81
QUESTIONS AND EXPLANATIONS:.....	81
Elastic Load Balancing (ELB).....	85
QUESTIONS AND EXPLANATIONS:.....	85
Elastic Load Balancing has all the advantages of an on-premises load balancer, plus several security benefits:.....	91
Amazon WorkSpaces.....	92
Amazon Virtual Private Cloud (Amazon VPC).....	94
Amazon Route 53.....	94
AWS Direct Connect.....	95
QUESTION:.....	96

Explanation:	96
AWS Direct Connect	96
You could expect the following benefits if you use AWS Direct Connect.	96
Reference:	97
2 STORAGE & CONTENT DELIVERY NETWORK	98
Amazon Simple Storage Service (Amazon S3)	98
QUESTIONS AND EXPLANATIONS:	100
Using multipart upload provides the following advantages:	102
Improved throughput—	102
Quick recovery from any network issues—	102
Pause and resume object uploads—	103
Begin an upload before you know the final object size—	103
Reference:	103
Amazon Glacier	103
QUESTION	103
Explanation	104
Amazon Elastic Block Storage (EBS)	104
QUESTIONS AND EXPLANATIONS:	104
AWS Storage Gateway	109
QUESTION:	109
Explanation:	110
AWS Storage Gateway	110
Reference:	110
AWS Import/Export	110
QUESTIONS AND EXPLANATIONS:	110
Amazon CloudFront	111
QUESTIONS AND EXPLANATIONS:	111
Amazon CloudFront	112
Amazon CloudFront billing is mainly affected by	112
Gateway-Cached Volume Architecture	113
You also allocate disks on-premises for the VM. These on-premises disks serve the following purposes:	115
Disks for use by the gateway as cache storage –	115
Disks for use by the gateway as the upload buffer –	115
Amazon CloudFront	116
Amazon CloudFront billing is mainly affected by	116
3 DATABASE	117

Amazon Relational Database Service (Amazon RDS).....	117
QUESTION	118
Explanation:	119
Amazon DynamoDB.....	119
QUESTION:	120
Explanation:	120
Local secondary index –	120
Global secondary index –	120
Reference:	120
Amazon ElastiCache	121
• Memcached–	121
• Redis –	121
Amazon Redshift	121
4 ANALYTICS	122
Amazon Elastic MapReduce (Amazon EMR).....	123
QUESTION:	123
Explanation:	123
The different cluster states of an Amazon EMR cluster are listed below.	123
STARTING	123
BOOTSTRAPPING.....	124
RUNNING.....	124
WAITING.....	124
TERMINATING	124
TERMINATED	124
TERMINATED_WITH_ERRORS	124
Reference:.....	124
Amazon Kinesis.....	124
AWS Data Pipeline.....	125
5 APPLICATION SERVICES	126
Amazon AppStream.....	126
SDKs.....	127
Amazon Simple Queue Service (Amazon SQS)	127
QUESTION	127
Explanation:	128
Amazon Simple Notification Service (Amazon SNS)	128
QUESTIONS AND EXPLANATIONS:	128

Amazon Simple Workflow Service (Amazon SWF)	131
QUESTIONS AND EXPLANATIONS:	131
Amazon Simple Email Service (Amazon SES)	133
QUESTIONS AND EXPLANATIONS:	133
Every Amazon SES sender has a unique set of sending limits, which are calculated by Amazon SES on an ongoing basis:	134
Sending quota –	134
send rate –	134
Note	134
Domain Keys Identified Mail (DKIM)	135
Amazon CloudSearch.....	137
Amazon Elastic Transcoder.....	138
6 DEPLOYMENT AND MANAGEMENT	139
AWS Identity and Access Management (IAM).....	139
Manage IAM users and their access –	139
Manage federated users and their permissions –	140
QUESTIONS AND EXPLANATIONS:	141
AWS CloudTrail.....	145
Amazon CloudWatch	146
QUESTIONS AND EXPLANATIONS:	146
AWS Elastic Beanstalk	153
QUESTIONS AND EXPLANATIONS:	154
AWS Elastic Beanstalk	155
AWS CloudFormation.....	156
The template, (a JSON-format, text-based file) and stack	156
AWS CloudFormation.....	156
QUESTIONS AND EXPLANATIONS:	156
A stack.....	159
AWS OpsWorks	159
AWS CloudHSM	160
QUESTIONS AND EXPLANATIONS:	160
Using Reduced Redundancy Storage	162
For example,.....	162
Note	162
7 CREATING AN AWS ACCOUNT	165
Signing up	165
QUESTIONS AND EXPLANATIONS:	165

Resource-based permissions are supported by	166
CHAPTER – MORE AMAZON CLOUD WEB SERVICES	167
<i>Chime</i>	167
<i>Lightsail</i>	167
<i>Fargate</i>	167
<i>Batch</i>	168
<i>Artifact</i>	168
<i>DataPipeline</i>	168
<i>VPN</i>	169
<i>Direct connect</i>	170
<i>Lumberyard</i>	170
<i>CodeCommit</i>	170
<i>CodeDeploy</i>	171
<i>CodePipeline</i>	171
<i>Inspector</i>	171
<i>TrustedAdvisor</i>	172
<i>Xray</i>	172
<i>OpsWorks</i>	172
<i>Concierge</i>	173
<i>Certificate Manager</i>	173
<i>App Stream</i>	174
<i>Machine Image</i>	174
<i>System Manager</i>	174
<i>Cognito</i>	175
<i>Inspector</i>	175
<i>ECS</i>	175
<i>Organisation</i>	176
<i>Support Plans</i>	177
<i>Rekognition</i>	177
<i>Shield</i>	177
<i>WAF</i>	178
<i>Cost and usage report</i>	178
<i>IAM Role</i>	179

<i>Gamelift</i>	179
<i>Guardduty</i>	179
<i>Abuseteam</i>	179
<i>Technical account manager</i>	180
<i>Cost Explorer</i>	180
<i>Storage gateway</i>	181
<i>CloudHSM</i>	181
<i>Cloud9</i>	181
<i>Quicksight</i>	182
<i>Proton</i>	182
<i>MobileHub</i>	183
<i>EMR</i>	183
<i>Step funtions</i>	183
<i>Athena</i>	184
<i>Pinpoint</i>	184
<i>SSO</i>	184
<i>Compliance Program</i>	185
<i>Guardduty</i>	185
<i>KMS</i>	186
<i>Codestar</i>	186
<i>Snowball</i>	186
<i>Snowmobile</i>	187
<i>Migration hub</i>	187
<i>Neptune</i>	188
<i>Storage gateway</i>	188
<i>Mobile hub</i>	189
<i>Aurora</i>	189
<i>Amazon Managed Blockchain</i>	190
<i>Outposts</i>	190
<i>Perspective</i>	191
<i>SageMaker</i>	191
<i>Lex</i>	192
<i>Infrastructure event manager</i>	192

<i>Budgets</i>	192
<i>Health dashboard</i>	193
<i>Config</i>	193
<i>Penetration testing</i>	194
<i>Billing</i>	194
<i>Kinesis</i>	195
CHAPTER – AWS SERVERLESS PLATFORMS	197
<i>Serverless on AWS</i>	197
Serverless services on AWS	197
Compute	198
AWS Lambda	198
AWS Fargate	198
Application integration	198
Amazon EventBridge	198
AWS Step Functions	198
Amazon SQS	199
Amazon SNS	199
Amazon API Gateway	199
AWS AppSync	199
Data store	199
Amazon S3	200
Amazon DynamoDB	200
Amazon RDS Proxy	200
Amazon Aurora Serverless	200
Use cases	201
☒ Build web applications	201
☒ Process data at nearly any scale	217
☒ Automate batch processing	246
☒ Index and store documents and images automatically	259
<i>ServerlessIoT Platform Accelerator</i>	260
Modernize your IoT backend with serverless ingestion pipelines to accelerate data flow and monitoring metrics	260
Benefits	261
1 Accelerated Deployment	261
2 Fast-Track to Production	261
3 Proven Best Practices	261
4 Access Actionable Insights	261

Take the next step	261
CHAPTER - CLOUD ADOPTION FRAMEWORK	263
Launch	263
Realize Value	263
<i>PERSPECTIVES IN THE AWS CLOUD ADOPTION FRAMEWORK</i>	264
Business Perspective	264
Common Roles:	264
Capabilities:	264
IT Finance	264
IT Strategy	264
Benefits Realization	264
Business Risk Management	265
People Perspective	265
Common Roles:	265
Capabilities:	265
Resource Management	265
Incentive Management	265
Career Management	265
Training Management	265
Organizational Change Management	266
Governance Perspective	266
Common Roles:	266
Capabilities:	266
Portfolio Management	266
Program and Project Management	266
Business Performance Measurement	266
License Management	266
Platform Perspective	267
Common Roles:	267
Capabilities:	267
Systems and Solution Architecture	267
Compute, Network, Storage, and Database Provisioning	267
Application Development	267
Security Perspective	267
Common Roles:	268
Capabilities:	268

Identity and Access Management (IAM)	268
Detective Control	268
Infrastructure Security	268
Data Protection	268
Incident Response	268
Operations Perspective	268
Common Roles:	269
Capabilities:	269
Service Monitoring	269
Application Performance Monitoring (APM)	269
Resource Inventory Management	269
Release/Change Management	269
Reporting and Analytics	269
Business Continuity/Disaster Recovery	269
IT Service Catalog	270
WHAT IS AWS WELL-ARCHITECTED TOOL?	271
The AWS Well-Architected Framework	271
Definitions In AWS WA Tool and the AWS Well-Architected Framework:	272
A workload	272
Milestones	272
Lenses	273
High risk issues (HRIs)	273
Medium risk issues (MRIs)	273
The AWS Serverless Application Lens	273
The AWS SaaS Lens	273
The AWS Foundational Technical Review (FTR) Lens	274
THE 5 PILLARS OF THE AWS WELL-ARCHITECTED FRAMEWORK	275
1. Operational Excellence	275
Design Principles	275
There are five design principles for operational excellence in the cloud:	275
Best Practices	276
2. Security	276
Design Principles	276
There are seven design principles for security in the cloud:	276
Best Practices	276
3. Reliability	277

Design Principles.....	277
There are five design principles for reliability in the cloud:.....	277
Best Practices	277
4. Performance Efficiency.....	278
Design Principles.....	278
There are five design principles for performance efficiency in the cloud:.....	278
Best Practices	278
5. Cost Optimization.....	278
Design Principles.....	278
There are five design principles for cost optimization in the cloud:.....	278
Best Practices	279
Conclusion	279
<i>DESIGN PRINCIPLES</i>	280
There are five design principles for operational excellence in the cloud:.....	280
Perform operations as code:	280
Make frequent, small, reversible changes:.....	280
Refine operations procedures frequently:	280
Anticipate failure:	280
Learn from all operational failures:	281
<i>VERTICAL SCALING AND HORIZONTAL SCALING IN AWS</i>	282
Vertical Scaling	282
Horizontal Scaling.....	283
How To Achieve Effective Horizontal Scaling	284
CHAPTER - WORKING WITH SIMPLE STORAGE SERVICE	285
1 INTRODUCING AMAZON S3	285
FEW BUCKET RULES:.....	285
S3 also provides different storage classes for the objects that you store on it.	285
General purpose	286
Amazon S3 Standard (S3 Standard)	286
Key Features:	286
Reduced Redundancy Storage (RRS):	286
Unknown or changing access.....	287
Amazon S3 Intelligent-Tiering (S3 Intelligent-Tiering)	287
Key Features:	288
Infrequent access.....	288
Amazon S3 Standard-Infrequent Access (S3 Standard-IA)	288

Key Features:	289
Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA)	289
Key Features:	289
Archive.....	290
Amazon S3 Glacier (S3 Glacier)	290
Key Features:	290
Amazon S3 Glacier Deep Archive (S3 Glacier Deep Archive)	290
Key Features:	291
S3 on Outposts.....	291
S3 Outposts storage class	291
Key Features:	291
Table of Performance across the S3 Storage Classes.....	292
QUESTION	293
2 GETTING STARTED WITH S3	295
CREATING BUCKETS.....	295
UPLOADING YOUR FIRST OBJECT TO A BUCKET	297
S3 object actually comprises:	297
• Key:	297
• Value:	297
• Version ID:	297
• Metadata:	297
• Sub resources:	298
• Access control:	298
VIEWING UPLOADED OBJECTS	299
ACCESSING BUCKETS AND OBJECTS USING S3CMD	300
MANAGING AN OBJECT'S AND BUCKET'S PERMISSIONS.....	302
Namely resource-based policies and user-based policies, as follows:	302
• Resource-based policies:	302
• Bucket policies:	303
QUESTION: 238.....	307
Explanation:	307
Amazon S3 provides four different access control mechanisms:.....	307
With IAM policies,.....	308
USING BUCKETS TO HOST YOUR WEBSITES.....	308
S3 EVENTS AND NOTIFICATION	310
S3 supports notifications on the following set of events:	310
• Object created:	310

• Objects removed:	310
• Object lost:	310
THE PARAMETERS ARE AS FOLLOWS:.....	311
• Name:	311
• Events:	311
• Prefix:.....	311
• Suffix:	311
• Send To:	311
• SNS topic:	311
BUCKET VERSIONING AND LIFECYCLE MANAGEMENT	312
There are a few rules that you have to keep in mind, however, when performing transition actions:	315
CROSS-REGION REPLICATION	316
3 PLANNING YOUR NEXT STEPS	318
QUESTIONS AND EXPLANATIONS:	319
BitTorrent.....	320
In client/server distribution, the entire object is transferred point-to-point from Amazon S3 to every authorized user who requests that object.	320
BitTorrent addresses this problem by recruiting the very clients that are downloading the object as distributors themselves:.....	320
The benefit for publishers	320
4 RECOMMENDATIONS AND BEST PRACTICES	321
CHAPTER - IMAGES AND INSTANCES	322
1 EC2	322
EC2 USE CASES	322
Hosting environments:	322
Dev/Test environments:	322
Backup and disaster recovery:.....	322
Marketing and advertisements:	322
High Performance Computing (HPC):	322
QUESTIONS AND EXPLANATIONS:	323
2 IMAGES AND INSTANCES	324
UNDERSTANDING IMAGES	324
AMIs can be broadly classified into two main categories depending on the way they store their root volume or hard drive:	325
• EBS-backed AMI:.....	325
• Instance store-backed AMI:	326
Amazon Linux AMI.....	327
UNDERSTANDING INSTANCES	327
AWS currently supports five instance types or families:	328

General purpose:	328
Compute optimized:	328
Memory optimized:	328
Storage optimized:	328
GPU instances:	328
EC2 INSTANCE PRICING OPTIONS.....	329
ON-DEMAND INSTANCES	329
RESERVED INSTANCES (RI).....	329
SPOT INSTANCES	329
QUESTIONS AND EXPLANATIONS:	330
WORKING WITH INSTANCES	331
STAGE 1 – CHOOSE AMI	333
STAGE 2 – CHOOSE AN INSTANCE TYPE.....	334
STAGE 3 – CONFIGURE INSTANCE DETAILS	335
• Number of instances:.....	335
• Purchasing option:	335
• Network:	336
• Subnet:.....	336
• Auto-assign Public IP:.....	337
• IAM role:	337
• Shutdown behaviour:	337
• Enable termination protection:	337
• Monitoring:	337
• Tenancy:.....	337
STAGE 4 – ADD STORAGE	337
STAGE 5 – TAG INSTANCES	338
QUESTIONS AND EXPLANATIONS:	339
STAGE 6 – CONFIGURE SECURITY GROUPS.....	342
STAGE 7 – REVIEW INSTANCE LAUNCH	342
CONNECTING TO YOUR INSTANCE	344
USING YOUR WEB BROWSER:	344
USING PUTTY	347
USING SSH	352
QUESTION	353
Explanation:	354
CONFIGURING YOUR INSTANCES	354
LAUNCHING INSTANCES USING THE AWS CLI	356

STAGE 1 – CREATE A KEY PAIR	356
STAGE 2 – CREATE A SECURITY GROUP	357
STAGE 3 – ADD RULES TO YOUR SECURITY GROUP	358
STAGE 4 – LAUNCH THE INSTANCE	359
QUESTION:	360
Explanation:	360
500 security groups and add up to 100 rules	360
Reference:	361
3 CLEANING UP!	361
QUESTIONS AND EXPLANATIONS:	361
Amazon EC2 provides the following features:	365
Overview of Creating Amazon EBS-Backed AMIs	367
4 PLANNING YOUR NEXT STEPS	370
5 RECOMMENDATIONS AND BEST PRACTICES	371
CHAPTER - RESERVED INSTANCE (RI)	372
<i>Why Should I Use RIs?</i>	372
Save Money and Maintain Flexibility	372
Reserve Capacity	372
<i>How do RIs Work?</i>	372
<i>Amazon EC2 RI Types</i>	372
Standard RIs:	372
Convertible RIs:	373
Scheduled RIs:	373
Standard and Convertible RI Features	373
The following summarizes features of all RIs.	373
Standard and Convertible RI Payment Attributes	374
Offering class:	374
Term:	374
Payment option:	374
RI Attributes	374
Instance type:	374
Platform description:	374
Tenancy:	374
Availability Zone (optional):	374
<i>Amazon EC2 RI Pricing</i>	375
<i>RI Marketplace</i>	375

CHAPTER - AWS NETWORKING.....	376
<i>BRUSHING UP ON NETWORKING BASICS</i>	376
✓ The physical layer (Layer 1):	376
✓ The data-link layer (Layer 2):	376
✓ The network layer (Layer 3):.....	376
Virtual LANS — keeping data private	376
Use of VLANs for cloud computing carries some drawbacks:.....	377
✓ A delay in the account setup:	377
✓ A limit on the number of VLANs that a router can manage:.....	377
✓ A limit on the number of computers that can be attached to a specific VLAN:.....	377
The Amazon alternative to VLANs	377
✓ The limitation on the number of VLANs would limit the number of customers Amazon could support with its AWS service.	377
✓ The limitation on the number of computers a customer could have within a single VLAN would limit the number of instances that could be used in its applications.	377
It implemented a networking design with these features:.....	378
✓ The use of Layer 3 technology throughout the infrastructure:.....	378
✓ The requirements that every instance is assigned an IP address and all traffic to that instance must be directed by IP address:	378
✓ No use or support of VLAN technology:.....	378
<i>AWS NETWORK IP ADDRESSING</i>	378
Figure 1: The public DNS and private IP address for a single instance.	380
Figure 2: AWS IP addresses and network traffic.	381
Figure 3: Intraregional and interregional AWS traffic.	382
Three choices for network traffic:	383
✓ Intraregional:	383
✓ Interregional:	383
✓ Extraregional:.....	383
Every instance that’s launched is assigned an address from the general pool of IP addresses — clearly an issue, for two reasons:	383
✓ People need to be able to find your site if they want to access your application for an extended period.	383
✓ In a complex application topology, every instance is dynamically assigned a private IP address at launch-time, and it needs to be able to find other instances.	383
.....	383
<i>AWS IP ADDRESS MAPPING</i>	384
<i>AWS DIRECT CONNECT</i>	384
<i>HIGH-PERFORMANCE AWS NETWORKING</i>	384
<i>AWS ELASTIC IP ADDRESSES</i>	385
How An Elastic IP address works:	385

1. You request an Elastic IP from AWS.....	385
2. You assign the Elastic IP address to an instance you run.....	385
3. You run the instance with the Elastic IP address.....	385
Points To Mind:	385
Elastic IP address pricing	386
Elastic IP addresses and AWS network scope.....	386
AWS INSTANCE METADATA	386
A large amount of instance-specific data is available via the metadata IP address, such as.....	386
INSTANCE IP ADDRESS COMMUNICATION	387
Figure 4: Instance activity flow in a configuration management mechanism application.....	387
✓ Launch:	388
✓ Self-discover:	388
✓ Self-configure:	388
✓ Update configuration management:	388
✓ Connect to other application instances:.....	388
CHAPTER – INTERNET PROTOCOL (IP) VERSION 4 AND 6	390
Benefits of IPv6	390
IPv4 vs IPv6	391
Classful IPv4 Addresses	392
Special IPv4 Addresses	394
Bogon IPv4 Addresses	395
Difference Between IPv4 and IPv6 Diagram	397
The Main Issues Of The Current Ipv4 Protocol:.....	398
Rapid depletion of the address space.....	398
Lack of hierarchy support.....	398
Complex network configuration.....	398
Lack of built-in authentication and confidentiality.....	398
A new protocol suite must satisfy the following basic requirements:.....	398
Request For Comment (RFC) References.....	399
TABLE IPV6 RFCs.....	399
Advantages of IPv6.....	400
Disadvantages of IPv6.....	401
IPv6 Security	402
IPV6 ADDRESSING	402
Tenets for IPv6 adoption.....	403
• Re-evaluate network controls —	403

• Design for scale —	403
• Phase your IPv6 adoption —	403
<i>Figures Above: IPV6 Addressing</i>	405
<i>Figure: In IPV6 the interface ID contains the 48 bits MAC Address</i>	406
Text Representation	407
Colon-hexadecimal form.	407
Compressed form	407
Mixed form.	407
<i>INTERNET PROTOCOL VERSION 6 OVERVIEW</i>	408
IPv6 offers the following significant features:	408
Some considerations regarding the main differences between IPv4 and IPv6 follow:.....	408
• Headers —	408
IPv6 uses two distinct types of headers:.....	408
• Flow labeling —	409
• Address assignment —	409
• Error correction —	409
• Neighbor Discovery Protocol —	409
IPv6 addresses.....	409
The main categories of IPv6 addresses are:.....	409
IPv6 adoption strategies and mechanisms	410
Two main drivers for IPv6 adoption.	410
A summary of IPv6 adoption drivers:	410
• Mandated IPv6 endpoints —	410
• Interoperability with IPv6 networks —	410
• Public IPv4 exhaustion —	410
• Private IPv4 exhaustion —	410
The four main driving forces, and the corresponding adoption strategy:	411
• Private IPv4 exhaustion —	411
Adoption strategy —	411
• Public IPv4 exhaustion —	411
Adoption strategy —	411
• Interoperability with IPv6-only networks —	411
Adoption strategy —	411
• Mandated IPv6 endpoints —	412
Adoption strategy —	412
Interoperability	412
Planning IPv6 adoption in the AWS Cloud network	412

Elastic network interfaces in an IP network could operate in three different modes:	412
• IPv4-only mode —	412
• IPv6-only mode —	412
• Dual-stack mode —	412
IPv6 addressing plan on AWS	412
There are two options for IPv6 address assignment:	413
AWS-assigned IPv6 VPC CIDR	413
BYOIPv6 VPC CIDR	413
VPC subnet addressing	413
Address Types	414
Unicast address	414
(I) Link-local addresses	414
(II) Site-local addresses	415
(III) Global IPv6 unicast addresses	415
Multicast address	415
Anycast address	415
Special addresses	416
Unicast addresses	417
Default route	417
Unspecified address	417
Local addresses	418
Unique local addresses	418
Transition from IPv4	419
IPv6 In summary	419
<i>Figure: IPV6 Subnetting www.ripe.net</i>	421
IPV6 MULTIPLE ADDRESS TYPES TABLE	423
Interfaces will have multiple addresses	424
CONVERSION OF BINARY, OCTAL AND HEXADECIMAL NUMBERS	425
Decimal, Binary, Octal, and Hexadecimal Numbers Table	425
From Binary to Decimal	425
From Binary to Octal	426
From Binary to Hexadecimal	426
From Octal to Binary	427
From Hexadecimal to Binary	427
From Decimal to Binary	428
From Decimal to octal to Hexadecimal	428
Binary to Decimal to Hexadecimal Online Converter	429

<i>IPV6 ON AWS INTRO</i>	430
Enable IPv6 in your VPC.....	430
To connect to the Internet, you have two options:.....	430
<i>DUAL-STACK IPV6 ARCHITECTURES FOR AWS AND HYBRID NETWORKS</i>	431
Introduction	431
1. Dual-stack Amazon VPC.....	431
<i>Figure. 1. : Dual-stack Amazon VPC</i>	434
<i>Figure. 2: Dual-stack EC2 instances</i>	436
2. Dual-stack VPC Internet connectivity	436
<i>Figure. 3: Dual-stack VPC Internet connectivity</i>	437
<i>Figures. 4: VPC route tables configuration for Internet connectivity</i>	441
The table below summarizes the above options for the different types of IPv6 CIDRs:	441
3. Dual-stack public endpoints for your applications using Elastic Load Balancing	441
<i>Figures. 5: Dual-stack ALB</i>	445
The ALB inbound security groups need to allow traffic from both IPv4 and IPv6 clients:	445
The diagram below shows the dual-stack NLB deployment and route tables configuration:	445
4. Dual-stack VPC connectivity with VPC peering.....	448
<i>Figure. 7: Dual-stack VPC Peering</i>	449
5. Dual-stack VPC connectivity at scale using AWS Transit Gateway	449
<i>Figures. 8: Dual-stack AWS Transit Gateway Routing</i>	453
6. AWS VPN and Direct Connect in dual-stack hybrid networks	453
<i>Figure. 9: Dual-stack AWS Site-to-site VPN</i>	453
<i>Figures. 10: Dual-stack Amazon Direct Connect</i>	456
7. Amazon CloudFront dual-stack distributions	456
CHAPTER: - IPV6 ON AWS	459
<i>DESIGNING AN IPV6 AWS CLOUD NETWORK</i>	459
Amazon VPC design.....	459
Some of the aspects typically considered:	459
VPC IP address assignment.....	459
Subnet address assignment	459
IP addressing of the elastic network interface	460
Examples of resources include:.....	460
Figure: Dual-stack Amazon VPC	461
IP addressing at the resource's networking stack	462
Supporting Amazon VPC services	462
Instance Metadata Service (IMDS)	462

Route 53 DNS resolver.....	462
Network Time Protocol server.....	462
Amazon VPC connectivity options for IPv6	463
VPC peering	463
Figures: Dual-stack IPv6 VPC peering.....	465
AWS Transit Gateway.....	466
IPv6 connectivity into Transit Gateway	466
Figures: Dual-stack AWS Transit Gateway routing.....	469
IPv6 traffic within and between Transit Gateways.....	470
You can attach the following resources to your Transit Gateway:	470
AWS Transit Gateway Connect Attachments for IPv6	470
Figures: AWS Transit Gateway Connect dual-stack IPv6 routing	473
AWS PrivateLink	474
Figures: AWS PrivateLink in a dual-stack scenario.....	476
VPC sharing.....	476
Amazon VPC internet access	477
Internet reachable IPv6 resources.....	477
Figures: Internet access for a VPC public subnet	479
Figures: Internet access from a VPC private subnet	482
Hybrid connectivity design	482
AWS Direct Connect	482
There are three types of VIFs:.....	483
Transit and Private VIF IPv6 peerings —	483
Advertising IPv6 prefixes from AWS	483
Advertising IPv6 prefixes to AWS.....	483
Public VIF IPv6 peerings —	484
Routing IPv6 over public and private or transit VIFs.....	484
Figures: Direct Connect dual-stack support	486
Amazon-managed VPN.....	486
AWS Site-to-Site VPN connectivity configuration comprises multiple parts:.....	486
Customer gateways	487
VPN connections.....	487
Customer gateway configuration	487
Figures: AWS VPN dual-stack configuration.....	490
Designing DNS for IPv6.....	490
PTR records.....	490
Alias records	491

DNS resolution within a host	491
Amazon Route 53 DNS records	491
Route 53 provides features for two use cases:	491
Public IPv6 DNS resolution	492
DNS resolution within a VPC	492
Private DNS resolution	492
IPV6 SECURITY AND MONITORING CONSIDERATIONS	492
Network-level access control	492
Amazon VPCs feature two network access control mechanisms, and these exist irrespectively of which version of the IP protocol is used (IPv4 or IPv6):	492
Security groups —	492
Network access control lists —	493
Network ACLs differ from security groups in several ways:	493
VPC Flow Logs	493
Table 1 — VPC Flow Logs default format	494
VPC Traffic Mirroring	495
AWS Web Application Firewall	495
Web ACL	495
AWS Shield	495
AWS Network Firewall	496
AWS Systems Manager	496
SCALING THE DUAL-STACK NETWORK DESIGN IN AWS	496
Elastic Load Balancing	496
Figures: Dual-stack IPv4/IPv6 internet-facing Network Load Balancer	500
AWS Global Accelerator	500
Amazon CloudFront	501
The request flow for life of an HTTP request in IPv6:	501
Figures: Amazon CloudFront dual-stack IPv4/IPv6 support	503
ADVANCED DUAL-STACK NETWORK DESIGNS	504
AWS Transit Gateway Connect attachment	504
For dynamic route exchange over the GRE tunnels AWS Transit Gateway Connect supports the following modes of BGP:	504
Centralized internet outbound traffic with IPv6	504
Figures: Centralized internet outbound traffic with NAT66	507
Using TGW with IPv6 to work around IPv4 address overlap	508
Figure: IPv6-only routing with AWS Transit Gateway	511
FURTHER READING	512
CHAPTER - BUILDING YOUR OWN PRIVATE CLOUDS USING AMAZON VPC	513

1 VPC CONCEPTS AND TERMINOLOGIES	514
Subnets.....	514
The default VPC comes preconfigured with the following set of configurations:	514
Security groups and network ACLs	515
Routing tables	515
VPC endpoints	516
Internet Gateways.....	518
NAT instances.....	518
DNS and DHCP Option Sets	520
Domain Name Servers (DNS).....	520
Domain name	520
• NTP servers:.....	520
• NetBIOS name server:.....	520
• NetBIOS node type:	521
QUESTION	521
Explanation:	521
AWS S3 has the following predefined groups:	521
I. Authenticated Users group:	521
II. All Users group:	521
III. Log Delivery group:	522
2 WORKING WITH VPCS	522
VPC LIMITS AND COSTS	522
VPC DEPLOYMENT SCENARIOS.....	522
VPC with a single public subnet.....	522
VPC with public and private subnets (NAT).....	523
VPC with public and private subnets and hardware VPN access	523
VPC with a private subnet only and hardware VPN access	523
GETTING STARTED WITH THE VPC WIZARD	523
FILL IN THE FOLLOWING DETAILS AS REQUIRED:	526
• IP CIDR block:.....	526
• VPC name:.....	526
• Public subnet:	526
• Availability Zone:.....	526
• Public subnet name:	526
• Private subnet, Availability zone, Private subnet name:.....	527
Next up, we specify the details of our NAT instance:	527

• Instance type:	527
• Key pair name:	528
• Subnet:.....	528
• Policy:.....	529
• Enable DNS hostnames:.....	529
• Hardware tenancy:	529
Viewing VPCs	530
Listing out subnets.....	531
Working with route tables.....	533
Listing Internet Gateways.....	534
Working with security groups and Network ACLs	535
Using the Create Security Group wizard, fill in the required information as described in the following:.....	536
• Name tag:.....	536
• Group name:	536
• Description:.....	537
• VPC :.....	537
QUESTION:	539
Explanation:	540
Availability Zones	540
Reference:.....	540
LAUNCHING INSTANCES IN YOUR VPC	540
CREATING THE WEB SERVERS.....	540
CREATING THE DATABASE SERVERS	542
QUESTIONS AND EXPLANATIONS:	543
The four options are:	547
<i>3 PLANNING NEXT STEPS</i>	<i>548</i>
<i>4 BEST PRACTICES AND RECOMMENDATIONS.....</i>	<i>550</i>
CHAPTER - AMAZON VIRTUAL PRIVATE CLOUD (AMAZON VPC).....	552
1 INTRODUCTION	552
2 AMAZON VIRTUAL PRIVATE CLOUD (AMAZON VPC)	552
An Amazon VPC consists of the following components:	552
An Amazon VPC has the following optional components:	552
3 SUBNETS.....	553
4 ROUTE TABLES	553
5 INTERNET GATEWAYS	554
6 DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP) OPTION SETS.....	555

You can configure the following values within a DHCP option set:.....	555
domain-name-servers—	555
domain-name—	556
ntp-servers—	556
netbios-name-servers—	556
netbios-node-type—	556
7 ELASTIC IP ADDRESSES (EIPS)	556
QUESTIONS AND EXPLANATIONS:	557
EC2-Classical platform , when you associate an Elastic IP Address (EIP).....	558
EC2-VPC platform , when you associate an EIP	558
8 ELASTIC NETWORK INTERFACES (ENIs)	559
QUESTIONS AND EXPLANATIONS:	559
Attaching multiple network interfaces (ENIs) to an EC2 instance is useful to:	561
Best Practices for Configuring Network Interfaces	562
9 ENDPOINTS	562
QUESTION	563
Explanation:	564
10 PEERING	564
QUESTION:.....	565
Explanation:	566
To create a VPC peering connection with another VPC, you need to be aware of the following limitations and rules:	566
Reference:.....	566
11 SECURITY GROUPS	567
TABLE 4.4 Security Group Rules for a Web Server	567
QUESTIONS AND EXPLANATIONS:	568
12 NETWORK ACCESS CONTROL LISTS (ACLs)	570
STATEFULNESS in conjunction with authorization info and return traffic.....	570
Stateful =	570
Stateless =.....	570
QUESTION:.....	571
Explanation:	572
A network access control list (ACL)	572
• Inbound SSH traffic. Port 22 Web servers in the public subnet to read and write to MS SQL servers in the private subnet.	572
• Port 1433 Inbound RDP traffic from the Microsoft Terminal Services gateway.....	572
• In the public private subnet. Port 3389	572
Reference:.....	572

13 NETWORK ADDRESS TRANSLATION (NAT) INSTANCES AND NAT GATEWAYS	572
14 NAT INSTANCE	572
15 NAT GATEWAY	573
QUESTION:	574
Explanation:	574
NAT devices , a NAT gateway or a NAT instance	574
Reference:.....	574
16 VIRTUAL PRIVATE GATEWAYS (VPGS), CUSTOMER GATEWAYS (CGWS), AND VIRTUAL PRIVATE NETWORKS (VPNS)	574
FIGURE 4.4 VPC with VPN connection to a customer network	575
17 AMAZON VPC SUMMARY.....	576
QUESTIONS AND EXPLANATIONS:	578
Amazon VPC provides two features that you can use to increase security for your VPC:	583
Security groups—	583
Network access control lists (ACLs)—	583
AWS Direct Connect	584
What is AWS Direct Connect?.....	584
Requirements.....	586
To use AWS Direct Connect, your network must meet one of the following conditions:.....	586
You are working with an independent service provider to connect to AWS Direct Connect. In addition, your network must meet the following conditions:.....	586
To connect to Amazon Virtual Private Cloud (Amazon VPC), you must first do the following:.....	586
To connect to public AWS products such as Amazon EC2 and Amazon S3, you need to provide the following:	586
18 EXAM ESSENTIALS.....	587
19 EXERCISES.....	589
Create Two Subnets for Your Custom Amazon VPC.....	589
Connect Your Custom Amazon VPC to the Internet and Establish Routing.....	589
Launch an Amazon EC2 Instance and Test the Connection to the Internet	590
CHAPTER - MONITORING YOUR AWS INFRASTRUCTURE.....	591
1 AN OVERVIEW OF AMAZON CLOUDWATCH	591
CONCEPTS AND TERMINOLOGIES	591
METRICS	591
NAMESPACES.....	592
DIMENSIONS.....	592
TIME STAMPS AND PERIODS	592
UNITS AND STATISTICS	593
ALARMS	594
CLOUDWATCH LIMITS AND COSTS	595

Here are a few important limits that you need to keep in mind when working with CloudWatch:	596
QUESTION	596
2 GETTING STARTED WITH CLOUDWATCH	597
MONITORING YOUR ACCOUNT'S ESTIMATE CHARGES USING CLOUDWATCH	597
From the Notification section, fill out the required details, as mentioned in the following:	600
• Whenever this alarm:	600
State is ALARM:.....	600
State is OK:.....	600
State is INSUFFICIENT:	600
• Send notification to:	601
QUESTION	602
Explanation:	603
MONITORING YOUR INSTANCE'S CPU UTILIZATION USING CLOUDWATCH	603
There are three basic action items that you can create for each of your EC2 alarms described as follows:.....	606
• Notification:	606
• AutoScaling Action:	606
• EC2 Action:	607
QUESTION	609
Explanation:	609
MONITORING YOUR INSTANCE'S MEMORY AND DISK UTILIZATION USING CLOUDWATCH SCRIPTS	610
CREATING CLOUDWATCH ACCESS ROLES	610
INSTALLING THE CLOUDWATCH MONITORING SCRIPTS	611
The following are some of the important files that the CloudWatch monitoring script ZIP contains:	612
• CloudWatchClient.pm:	612
• mon-put-instance-data.pl:	612
• mon-get-instance-stats.pl:	612
• awscreds.template:.....	613
VIEWING THE CUSTOM METRICS FROM CLOUDWATCH	614
MONITORING LOGS USING CLOUDWATCH LOGS.....	615
CLOUDWATCH LOG CONCEPTS AND TERMINOLOGIES	616
• Log events:	616
• Log stream:	616
• Log groups:	616
• Metric filters:	616
• Retention policies:	616
• Log agent:	616
GETTING STARTED WITH CLOUDWATCH LOGS	616

Here's a quick look at the awslogs.conf file's parameters:	618
• file:	618
• datetime_format:	618
• Initial_position:	619
• log_group_name:	619
• log_stream_name:	619
VIEWING THE LOGS	619
CREATING METRIC FILTERS AND ALARMS	620
QUESTIONS AND EXPLANATIONS:	622
Tools To Monitor The Performance Of Your Cluster	625
Hadoop Web Interfaces	626
CloudWatch Metrics	626
Ganglia	626
3 PLANNING YOUR NEXT STEPS	627
4 RECOMMENDATIONS AND BEST PRACTICES	627
CHAPTER - PROGRAMMING YOUR INFRASTRUCTURE: THE COMMAND LINE, SDKS, AND CLOUDFORMATION	628
Figure 1 Interacting with AWS by making calls to the REST AP	628
1 INFRASTRUCTURE AS CODE	629
1.1 Automation and the DevOps movement	630
1.2 Inventing an infrastructure language: JIML	630
Figure 2 From JIML blueprint to infrastructure: infrastructure automation	631
The infrastructure consists of the following:	631
Listing 1 Infrastructure description in JIML	631
Figure 3 The JIML interpreter figures out the order in which resources need to be created	635
2 USING THE COMMAND-LINE INTERFACE	636
2.1 Installing the CLI	636
LINUX AND MAC OS X	637
WINDOWS	637
2.2 Configuring the CLI	638
Figure 4 IAM users (empty)	638
Figure 5 Creating an IAM user	639
Figure 6 Creating an IAM user: showing credentials	640
Four pieces of information:	640
■ AWS access key ID—	640
■ AWS secret access key—	640
■ Default region name—	640

■Default output format—	641
Figure 7 IAM users.....	642
Figure 8 IAM user mycli without any permissions.....	643
Figure 9 Attaching a managed policy to an IAM user	644
Figure 10 IAM user mycli with admin permissions	645
2.3 Using the CLI.....	646
The limitations of this solution are as follows:	648
Nonetheless, the CLI solution solves the following use cases:	648
Where is the code located?.....	649
LINUX AND MAC OS X.....	649
WINDOWS	651
Listing 4 Creating and terminating a server from the CLI (PowerShell)	652
WHY SHOULD YOU SCRIPT?.....	654
3 PROGRAMMING WITH THE SDK	654
Installing and getting started with Node.js.....	655
3.1 Controlling virtual servers with SDK: nodecc.....	655
Figure 11 Node Control Center for AWS: start screen.....	656
3.2 How nodecc creates a server	656
Figure 12 nodecc: creating a server (step 1 of 2)	657
Listing 5 /lib/listAMIs.js	658
3.3 How nodecc lists servers and shows server details	659
Figure 13 nodecc: creating a server (step 2 of 2)	659
Figure 14 nodecc: listing servers	660
Figure 15 nodecc: showing server details.....	661
3.4 How nodecc terminates a server.....	661
Cleaning up.....	661
4 USING A BLUEPRINT TO START A VIRTUAL SERVER	662
The benefits of CloudFormation are as follows:.....	662
■It's a consistent way to describe infrastructure on AWS.....	662
■It can handle dependencies.....	662
■It's replicable.	662
■It's customizable.....	662
■It's testable.....	663
■It's updatable.	663
■It minimizes human failure.....	663
■It's the documentation for your infrastructure.....	663

■ It's free	663
1 Anatomy of a CloudFormation template	663
A basic CloudFormation template is structured into five parts:	663
1 Format version—	663
2 Description—	663
3 Parameters—	664
4 Resources—	664
5 Outputs—	664
Listing 6 CloudFormation template structure.....	664
FORMAT VERSION AND DESCRIPTION.....	664
PARAMETERS.....	665
Listing 7 CloudFormation parameter structure	665
Table 1 CloudFormation parameter types.....	666
Table 2 CloudFormation parameter properties.....	667
RESOURCES.....	668
Listing 8 CloudFormation resources structure.....	669
Listing 9 CloudFormation EC2 server resource	670
OUTPUTS	670
Listing 10 CloudFormation outputs structure.....	670
Listing 11 CloudFormation outputs example.....	671
2 Creating your first template	671
Listing 12 Template to create an EC2 instance with CloudFormation	672
Where is the template located?	674
Figure 16 Overview of CloudFormation stacks	676
Figure 17 Creating a CloudFormation stack: selecting a template (step 1 of 4)	677
Figure 18 Creating a CloudFormation stack: defining parameters (step 2 of 4)	678
Figure 19 Creating a CloudFormation stack: summary (step 4 of 4).....	679
Figure 20 The CloudFormation stack has been created.	680
Figure 21 Updating the CloudFormation stack: summary (step 1 of 4).....	681
Alternatives to CloudFormation	682
Cleaning up.....	683
CHAPTER - AUTOMATING DEPLOYMENT: CLOUDFORMATION, ELASTIC BEANSTALK, AND OPSWORKS.....	684
1 DEPLOYING APPLICATIONS IN A FLEXIBLE CLOUD ENVIRONMENT.....	684
Figure 1 Deployment must be automated in a flexible and scalable cloud environment	685
2 RUNNING A SCRIPT ON SERVER STARTUP USING CLOUDFORMATION.....	685
2.1 Using user data to run a script on server startup	685

2.2 Deploying OpenSwan as a VPN server to a virtual server	686
Figure 2 Using OpenSwan on a virtual server to tunnel traffic from a personal computer	686
Listing 1 Deploying a VPN server to a virtual server: CloudFormation and a shell script	686
SHORTCUT FOR OS X AND LINUX.....	687
USING CLOUDFORMATION TO START A VIRTUAL SERVER WITH USER DATA	689
FN::JOIN AND FN::BASE64	689
Listing 2 Parts of a CloudFormation template to start a virtual server with user data.....	689
INSTALLING AND CONFIGURING A VPN SERVER WITH A SCRIPT.....	692
Cleaning up.....	694
2.3 Starting from scratch instead of updating	694
3 DEPLOYING A SIMPLE WEB APPLICATION WITH ELASTIC BEANSTALK.....	694
Elastic Beanstalk lets you handle the following recurring problems:	694
3.1 Components of Elastic Beanstalk	695
■ An application	695
■ A version.....	695
■ A configuration template	695
■ An environment	695
Figure 3 An Elastic Beanstalk application consists of versions, configurations, and environments.	696
3.2 Using Elastic Beanstalk to deploy Etherpad, a Node.js application	696
CREATING AN APPLICATION FOR AWS ELASTIC BEANSTALK	697
CREATING A VERSION FOR AWS ELASTIC BEANSTALK.....	697
CREATING AN ENVIRONMENT TO EXECUTE ETHERPAD WITH ELASTIC BEANSTALK	697
HAVING FUN WITH ETHERPAD	698
Listing 4 Describing the status of the Elastic Beanstalk environment	699
Figure 4 Online text editor Etherpad in action	700
EXPLORING ELASTIC BEANSTALK WITH THE MANAGEMENT CONSOLE	700
Figure 5 Overview of AWS Elastic Beanstalk environment running Etherpad.....	702
Cleaning up.....	702
Figure 6 Downloading logs from a Node.js application via AWS Elastic Beanstalk.....	704
4 DEPLOYING A MULTILAYER APPLICATION WITH OPSWORKS	704
The service offers some standard layers with the following runtimes:	705
About Chef	705
4.1 Components of OpsWorks	706
■ A stack	706
■ A layer	706
■ An instance.....	706

■ An app	707
Figure 7 Stacks, layers, instances, and apps are the main components of OpsWorks.	707
4.2 Using OpsWorks to deploy an IRC chat application	708
Figure 8 Building your own IRC infrastructure consisting of a web application and an IRC server.....	708
CREATING A NEW OPSWORKS STACK.....	708
Figure 9 Creating a new stack with OpsWorks	711
CREATING A NODE.JS LAYER FOR AN OPSWORKS STACK	711
Figure 10 Creating a layer with Node.js for kiwiIRC.....	712
CREATING A CUSTOM LAYER FOR AN OPSWORKS STACK	712
Figure 11 Creating a custom layer to deploy an IRC server	713
Shortcut for OS X and Linux.....	713
Listing 5 Creating a custom firewall with the help of CloudFormation	714
Figure 12 Adding a custom firewall configuration to the IRC server layer	715
Figure 13 Adding an IRC package to a custom layer	716
ADDING AN APP TO THE NODE.JS LAYER.....	716
Figure 14 Adding kiwiIRC, a Node.js app, to OpsWorks.....	717
ADDING INSTANCES TO RUN THE IRC CLIENT AND SERVER	718
Figure 15 Adding a new instance to the Node.js layer	719
Figure 16 Starting the instances for the IRC web client and server	720
HAVING FUN WITH KIWIRC	720
Figure 17 Waiting for deployment to open kiwiIRC in the browser	721
Figure 18 Using kiwiIRC to log in to your IRC server on channel #awsinaction	723
Cleaning up.....	724
5 COMPARING DEPLOYMENT TOOLS.....	724
1 Classifying the deployment tools	724
Figure 19 Comparing different ways to deploy applications on AWS	725
2 Comparing the deployment services.....	726
CHAPTER - DATABASE-AS-A-SERVICE USING AMAZON RDS	727
1 AN OVERVIEW OF AMAZON RDS	727
RDS INSTANCE TYPES.....	728
• Micro instances (db.t1.micro):	728
• Standard instances (db.m3):	729
• Memory optimized (db.r3):	729
• Burst capable (db.t2):	729
Here's a quick look at the different storage types provided with your RDS instances:	729
• Magnetic (standard):	729

• General purpose (SSD):	729
• Provisioned IOPs:	730
MULTI-AZ DEPLOYMENTS AND READ REPLICAS	730
2 WORKING WITH AMAZON RDS	733
GETTING STARTED WITH MYSQL ON AMAZON RDS	734
CREATING A MYSQL DB INSTANCE	735
Step 1: Select Engine	736
Step 2: Production?	736
Step 3: Specify DB Details	737
• License Model:	737
• DB Engine Version:	737
• DB Instance Class:	738
• Multi-AZ Deployment:	738
• Storage type:	738
• Allocate storage:	738
Settings panel:	739
• DB Instance Identifier:	739
• Master Username:	739
• Master Password:	739
Step 4: Configure Advanced Settings	739
• VPC:	739
• Subnet Group:	739
• Publicly Accessible:	740
• Security Group(s):	740
Database Options:	740
• Database Name:	740
• Database Port:	741
• DB Parameter Group:	741
• Option Group:	741
• Enable Encryption:	742
Some of the states that a DB instance goes through during its lifecycle:	744
• Creating:	744
• Modifying:	744
• Backing-up:	744
• Available:	744
QUESTIONS AND EXPLANATIONS:	745
Server-side encryption	746

In client-side encryption,	746
CONNECTING REMOTELY TO YOUR DB INSTANCE	747
TESTING YOUR DATABASE	748
MODIFYING YOUR DB INSTANCES	749
BACKING UP DB INSTANCES	750
CREATING READ REPLICAS AND PROMOTING THEM	752
LOGGING AND MONITORING YOUR DB INSTANCE	755
CLEANING UP YOUR DB INSTANCES	757
QUESTIONS AND EXPLANATIONS:	758
SQL Server authentication.....	764
A DB instance reboot occurs immediately when one of the following occurs:.....	765
A DB instance reboot occurs during the maintenance window when one of the following occurs:.....	766
The data model of DynamoDB is:.....	766
"Table",	766
"Items",	766
"Attribute",.....	767
Amazon RDS Multi-AZ Deployments.....	768
Enhanced Durability	769
Amazon Aurora Enhanced Durability	769
Increased Availability	769
Multi-AZ deployments Increased Availability.....	770
Amazon Aurora Increased Availability	770
ElastiCache for Memcached.....	771
Having your caching layer handle these queries has several advantages.	771
Architecture with ElastiCache for Memcached.....	772
A simplified deployment for a web application looks something like this:	773
Here is an example architecture that uses Amazon DynamoDB instead of Amazon RDS and MySQL:.....	777
What can I do with Amazon SQS?	779
Load Balancer Layer:	781
Cache Layer:	782
Database Layer: A few options:	782
Use RDS to run MySQL/ Postgres.....	782
App Layer:	782
Saving money:	783
RDS Multi-AZ deployments.....	785
Benefits.....	785
Enhanced Durability.....	785

Increased Availability	786
No Administrative Intervention	786
Failover conditions.....	786
Amazon RDS automatically performs a failover in the event of any of the following:.....	787
• Loss of availability in primary Availability Zone	787
• Loss of network connectivity to primary	787
• Compute unit failure on primary.....	787
• Storage failure on primary.....	787
Note:	787
3 PLANNING YOUR NEXT STEPS	788
4 RECOMMENDATIONS AND BEST PRACTICES.....	788
CHAPTER - EXTENDED AWS SERVICES FOR YOUR APPLICATIONS	789
1 INTRODUCING AMAZON ROUTE53	789
WORKING WITH ROUTE53	789
CREATING HOSTED ZONES	790
Here are some of the commonly used record set types provided by Route53:	792
• A record:	792
• AAAA record:	792
• CNAME records:	792
A Canonical Name (CNAME)	792
• MX records:	792
They are as follows:	793
• Simple routing:.....	793
• Weighted routing:.....	793
• Latency-based routing:	793
• Geolocation routing:	793
• Failover routing:.....	794
QUESTIONS AND EXPLANATIONS:	796
Active-active failover:	796
Active-passive failover:	796
Active-active-passive and other mixed configurations:	797
With DNS Failover,	797
GETTING STARTED WITH TRAFFIC FLOW.....	798
Use the following DNS types if you wish to route traffic to the following AWS resources:	798
• ELB:	798
• Amazon S3 bucket:	798

• CloudFront distribution:	798
CONFIGURING HEALTH CHECKS	799
QUESTIONS:	802
How Health Checks Work.....	803
For example,.....	803
Here's how Amazon EC2 and Amazon Route 53 are configured:	804
Sequence of events:.....	807
What Happens When You Associate a Health Check with an Alias Resource Record Set?	807
For example, suppose the following configuration:	807
What Happens When You Omit Health Checks?.....	808
Here's what happens when you omit a health check on a non-alias resource record set in this configuration:	810
What Happens When You Set Evaluate Target Health to No?	810
Here's what happens when you set Evaluate Target Health to No for an alias resource record set in this configuration:	812
2 CONTENT DELIVERY USING AMAZON CLOUDFRONT	813
GETTING STARTED WITH DISTRIBUTIONS	814
CloudFront supports two modes of delivering content; they are as follows:.....	814
• Web:	814
• RTMP:	814
The following variants of the RTMP protocol are supported by CloudFront:	815
• RTMP:.....	815
• RTMPT.....	815
• RTMPE.....	815
• RTMPTE.....	815
Next, fill out the following details to create your very own RTMP distribution:.....	815
• Origin Domain Name:.....	815
• Restrict Bucket Access:.....	815
• Origin Access Identity:.....	815
• <i>Grant Read Permissions on Bucket:</i>	816
• <i>Restrict Viewer Access:</i>	816
• <i>Price Class:</i>	816
• <i>Alternate Domain Names (CNAMEs):</i>	817
• <i>Logging:</i>	817
• <i>Distribution State:</i>	817
CLOUDFRONT RECOMMENDATIONS AND BEST PRACTICES	818
QUESTIONS AND EXPLANATIONS:	819
Before you can delete an SSL certificate, you need to	819

An Internal Elastic Load Balancer In A VPC	821
The header X-Forwarded-For in header	822
Example	822
The Forwarded-For request header takes the following form:	822
3 WHAT'S NEW IN AWS?.....	823
ELASTIC CONTAINER SERVICE.....	823
Here are a few key benefits and features of using ECS:	823
• Automated Clustering:.....	823
• Container Scheduling:.....	824
• Portability and extensibility:	824
• AWS integration:.....	824
ELASTIC FILE SYSTEM.....	824
DATABASE MIGRATION MADE EASY WITH DATABASE MIGRATION SERVICE	826
GO SERVERLESS WITH AWS LAMBDA.....	826
CHAPTER - AWS SECURITY	827
<i>CLOUDS CAN HAVE BOUNDARIES, TOO</i>	827
Figure 1: The AWS computing environment architecture.....	828
The placement of the trust boundary at the instance means that Amazon takes responsibility for the security of these parts of the computing environment:	829
✓ The physical facility:.....	829
✓ The computing hardware:	829
✓ The hypervisor:.....	829
✓ The surrounding software infrastructure:	829
✓ The Application Programming Interface (API):	829
Security is a shared responsibility, and some security elements remain with you. Here's a brief list:	829
✓ Your application's software packages:	829
✓ Your application's configuration:.....	829
✓ Your application's operating system (possibly):	830
<i>THE DEPERIMETERIZATION OF SECURITY</i>	830
The Jericho Forum recommends that everyone recognize the successful deperimeterization of security and acknowledge that, consequently:.....	830
Amazon doesn't let you install an IDS/IPS device in its network, because:.....	831
The concept of deperimeterization provides the context for what's going on, but doesn't truly change the fundamental nature of your partnership with Amazon, because	831
✓ Amazon is still responsible for all security of the computing environment, up to and including the hypervisor.	831
✓ You're still responsible for the security of the running instance and the overall application.	832
<i>AWS SECURITY GROUPS</i>	832

Security group rules control the following elements of network traffic access:	832
✓ Traffic protocol:	832
✓ Traffic source:	833
✓ Traffic port:	833
Security groups.....	833
Security group rules.....	833
Figure 2: Setting security group rules.....	834
Figure 3: The port range field.....	835
Security group traffic sources.....	835
<i>USING SECURITY GROUPS TO PARTITION APPLICATIONS</i>	836
Figure 4: Using security groups to partition applications.....	837
Steps you'd use to define how security groups can implement application partitioning:.....	838
Security group scope	839
Security group cost.....	839
<i>SECURITY GROUP BEST PRACTICES</i>	840
✓ Avoid using the Default security group.	840
✓ Use meaningful names.	840
✓ Open only the ports you need to open.	840
✓ Partition applications.	840
✓ Restrict system administrator access.	840
<i>AWS VIRTUAL PRIVATE CLOUD (VPC)</i>	841
VPC overview.....	841
How VPC works	842
Figure 5: The AWS virtual private cloud	842
Every VPC can have one or more subnets, which can then be used in these four VPC scenarios, based on the types of subnets the VPC contains:	843
✓ VPC with public subnet:	843
✓ VPC with public and private subnet:	843
✓ VPC with public and private subnet and hardware VPN access:.....	843
✓ VPC with only private subnet and hardware VPN access:	843
VPC subnets.....	844
Communication from instances within subnets	844
VPC routing tables	845
Internet gateway	845
NAT servers.....	845
Figure 6: A more complex VPC configuration.....	848
VPC Network Access Control Lists (ACLs)	848

Elastic Network Interfaces	848
VPC scope	849
VPC cost.....	849
Using VPC	849
AWS APPLICATION SECURITY.....	849
Recommendations to increase your AWS application security:	849
✓ Use security groups appropriately.	849
Limiting traffic to appropriate IP address ranges is a good practice to follow as well	850
✓ Implement data encryption in transit.	850
✓ Implement data encryption at rest.	850
✓ Manage security keys carefully.	850
✓ Install and configure your software packages correctly.	850
✓ Implement on-instance security.	850
✓ Manage your instance code properly.	851
CHAPTER – COMMAND LINE INTERFACE	852
1 GETTING STARTED WITH AWS CLI.....	852
Run the following commands from your Linux terminal:	852
Run the following commands from your Linux terminal to install the Python pip package:.....	853
2 MANAGING ACCESS AND SECURITY USING THE AWS CLI	854
QUESTION	859
3 THE AWS CLI.....	860
GETTING HELP WITH THE AWS CLI	860
AWS CLI API DOCUMENTATION	866
• Actions	867
• Data Types	867
• Common Parameters	867
• Common Errors.....	867
SERVICE-SPECIFIC CLIS	867
COMMAND STRUCTURE IN THE AWS CLI	867
SPECIFYING PARAMETER VALUES FOR THE AWS CLI.....	868
COMMON PARAMETER TYPES.....	869
USING JSON FOR PARAMETERS.....	872
USING QUOTATION MARKS WITH STRINGS	875
Linux, macOS, or Unix.....	875
PowerShell	875
Windows Command Prompt	875

LOADING PARAMETERS FROM A FILE.....	876
BINARY FILES.....	877
REMOTE FILES.....	879
GENERATE THE CLI SKELETON AND INPUT PARAMETERS FROM A JSON INPUT FILE	880
CONTROLLING COMMAND OUTPUT FROM THE AWS CLI	887
HOW TO SELECT THE OUTPUT FORMAT.....	887
JSON OUTPUT FORMAT	888
TEXT OUTPUT FORMAT	888
TABLE OUTPUT FORMAT	889
HOW TO FILTER THE OUTPUT WITH THE --QUERY OPTION.....	891
USING SHORTHAND SYNTAX WITH THE AWS COMMAND LINE INTERFACE	899
STRUCTURE PARAMETERS.....	899
Linux, macOS, or Unix.....	899
PowerShell.....	899
LIST PARAMETERS	900
USING AWS CLI PAGINATION OPTIONS.....	902
UNDERSTANDING RETURN CODES FROM THE AWS CLI.....	903
4 USING THE AWS CLI TO WORK WITH AWS SERVICES.....	907
USING AMAZON DYNAMODB WITH THE AWS CLI	907
USING AMAZON EC2 WITH THE AWS CLI	911
CREATE, DISPLAY, AND DELETE AMAZON EC2 KEY PAIRS.....	911
CREATING A KEY PAIR	911
DISPLAYING YOUR KEY PAIR	913
DELETING YOUR KEY PAIR.....	913
CREATE, CONFIGURE, AND DELETE SECURITY GROUPS FOR AMAZON EC2	913
CREATING A SECURITY GROUP	914
EC2-VPC	914
EC2-CLASSIC.....	915
ADDING RULES TO YOUR SECURITY GROUP	916
EC2-VPC	917
EC2-CLASSIC.....	919
DELETING YOUR SECURITY GROUP.....	920
EC2-VPC	920
EC2-CLASSIC.....	920
LAUNCH, LIST, AND TERMINATE AMAZON EC2 INSTANCES	920
LAUNCHING AN INSTANCE	921
EC2-VPC	921

EC2-CLASSIC	924
ADDING A BLOCK DEVICE TO YOUR INSTANCE	926
ADDING A TAG TO YOUR INSTANCE	927
LISTING YOUR INSTANCES	927
TERMINATING AN INSTANCE	927
USING AMAZON S3 GLACIER WITH THE AWS CLI	928
CREATING AN AMAZON S3 GLACIER VAULT	928
PREPARING A FILE FOR UPLOADING	929
INITIATING A MULTIPART UPLOAD AND UPLOAD FILES	930
COMPLETING THE UPLOAD	932
To Calculate A Tree Hash	933
QUESTION:	936
Explanation:	936
Using multipart upload provides the following advantages:	936
Improved throughput—	936
Quick recovery from any network issues—	936
Pause and resume object uploads—	936
Begin an upload before you know the final object size—	937
Reference:	937
USING AWS IDENTITY AND ACCESS MANAGEMENT FROM THE AWS CLI	937
CREATING IAM USERS AND GROUPS	937
ATTACH AN IAM MANAGED POLICY TO AN IAM USER	939
SET AN INITIAL PASSWORD FOR AN IAM USER	940
QUESTIONS AND EXPLANATIONS:	941
CREATE AN ACCESS KEY FOR AN IAM USER	943
QUESTION:	944
Explanation:	945
Granting Cross-account Permission to objects It Does Not Own	945
There are two core issues:	945
Background: Cross-Account Permissions and Using IAM Roles	945
Each IAM role you create has two policies attached to it:	945
A trust policy identifying another AWS account that can assume the role.	945
An access policy defining what permissions-for example, s3:GetObject-are allowed when someone assumes the role.	945
The user can then do the following to access objects:	946
The following is a summary of the walkthrough steps:	946
USING AMAZON S3 WITH THE AWS CLI	948
USING HIGH-LEVEL (S3) COMMANDS WITH THE AWS CLI	949

MANAGING BUCKETS	949
CREATING A BUCKET	949
LISTING YOUR BUCKETS	949
DELETING A BUCKET	950
MANAGING OBJECTS	950
USING API-LEVEL (S3API) COMMANDS WITH THE AWS CLI	957
APPLYING A CUSTOM ACL	957
CONFIGURING A LOGGING POLICY	957
USING AMAZON SNS WITH THE AWS CLI	958
CREATE A TOPIC	959
SUBSCRIBE TO A TOPIC	959
PUBLISH TO A TOPIC	960
UNSUBSCRIBE FROM A TOPIC	960
DELETE A TOPIC	960
USING AMAZON SWF WITH THE AWS CLI	961
LIST OF AMAZON SWF COMMANDS BY CATEGORY	961
COMMANDS RELATED TO ACTIVITIES	961
COMMANDS RELATED TO DECIDERS	962
COMMANDS RELATED TO WORKFLOW EXECUTIONS	962
COMMANDS RELATED TO ADMINISTRATION	962
Activity Management	962
Workflow Management	962
Domain Management	962
Workflow Execution Management	963
VISIBILITY COMMANDS	963
Activity Visibility	963
Workflow Visibility	963
Workflow Execution Visibility	963
Domain Visibility	963
Task List Visibility	963
WORKING WITH AMAZON SWF DOMAINS USING THE AWS CLI	964
LIST YOUR DOMAINS	964
GET INFORMATION ABOUT A DOMAIN	965
REGISTER A DOMAIN	965
DEPRECATING A DOMAIN	966
<i>5 TROUBLESHOOTING AWS CLI ERRORS</i>	<i>967</i>
PERMISSIONS ISSUES	967

MAIN CLI PROGRAM MUST HAVE 'RUN' PERMISSION	967
YOU MUST USE VALID CREDENTIALS.....	967
YOUR IAM USER MUST BE ABLE TO RUN THE COMMAND.....	968
QUESTIONS AND EXPLANATIONS:	969
To access your AWS account resources, users must have credentials.....	972
Web Identity Federation.....	973
Using Amazon Cognito.....	974
Using Amazon Cognito for Mobile Apps.....	974
Sample workflow using Amazon Cognito to federate users for a mobile application	976
Use the following process to configure your app to use Amazon Cognito to authenticate users and give your app access to AWS resources.	977
Working with volumes.....	979
Launching instances (Run Instances)	981
a). AMI.....	981
Alternatively, the following policy allows users to launch instances using only the specified AMIs,	982
Alternatively, the following policy allows users to launch instances from all AMs owned by Amazon.	983
b). Instance type	984
Alternatively, you can create a policy that denies users permission to launch any instances except t2.micro and t2.small instance types.....	986
c). Subnet	987
Alternatively, you could create a policy that denies users permission to launch an instance into any other subnet.....	988
6 NEXT STEPS	990
AWS has also services as well that help with your account's easy administration and management.	990
• AWS CloudTrail:	990
• AWS Config:	990
• AWS Key Management Service:	991
7 RECOMMENDATIONS AND BEST PRACTICES	991
CHAPTER – DESIGNING FOR FAULT-TOLERANCE	992
Differentiate among services that guarantee the following:.....	992
■ Nothing (single point of failure)—	992
■ High availability—.....	992
■ Fault-tolerance—.....	992
<i>Single point of failure</i> (SPOF) means this service will fail if, for example, a hardware failure occurs:.....	992
■ Amazon Elastic Compute Cloud (EC2) instance—	992
■ Amazon Relational Database Service (RDS) single instance—.....	993
<i>Highly available</i> (HA) means that when a failure occurs the service won't be available for a short time but will come back automatically:	993
■ Elastic Network Interface (ENI)—	993
■ Amazon Virtual Private Cloud (VPC) subnet—	993

■ Amazon Elastic Block Store (EBS) volume—	993
■ Amazon Relational Database Service (RDS) Multi-AZ instance—	993
<i>Fault-tolerant</i> means that if a failure occurs, you won't notice it:	993
1 USING REDUNDANT EC2 INSTANCES TO INCREASE AVAILABILITY	994
A few reasons your virtual server might suffer from a crash caused by the host system:	994
The software running on top of the virtual server may also cause a crash:	994
1.1 Redundancy can remove a single point of failure	994
1.2 Redundancy requires decoupling	995
Figure 3 Fault-tolerant EC2 servers with an auto-scaling group and ELB	995
Figure 3 See What Parts Are Redundant:	995
■ Availability zones—	995
■ Subnets—	996
■ EC2 instances—	996
Figure 4 Fault-tolerant EC2 servers with an auto scaling group and SQS	996
2 CONSIDERATIONS FOR MAKING YOUR CODE FAULT-TOLERANT	997
2.1 Let it crash, but also retry	997
2.2 Idempotent retry makes fault-tolerance possible	997
3 ARCHITECTING A FAULT-TOLERANT WEB APPLICATION: IMAGERY	997
Figure 7 The user uploads an image to Imagery, where a filter is applied.	998
Figure 8 Producers send messages to a message queue, and consumers read messages.	999
Figure 9 The user asynchronously uploads an image to Imagery, where a filter is applied.	1002
Figure 10 Combining AWS services to implement the asynchronous Imagery process	1003
AWS Lambda and Amazon API Gateway	1003
3.1 The idempotent image-state machine	1003
THE FINITE STATE MACHINE	1003
IDEMPOTENT STATE TRANSITIONS	1004
3.2 Implementing a fault-tolerant web service	1005
The server will support the following routes:	1005
SETTING UP THE SERVER PROJECT	1006
Listing 1 Initializing the Imagery server (server/server.js)	1006
CREATING A NEW IMAGERY PROCESS	1007
Figure 11 Creating a new image process in Imagery	1007
Optimistic locking	1008
Figure 12 Looking up an image process in Imagery to return its state	1010
LOOKING UP AN IMAGERY PROCESS	1010
Listing 3 Imagery server: GET /image/:id looks up an image process	1011

Figure 13 Uploading a raw image to Imagery and triggering image processing	1013
3.3 Implementing a fault-tolerant worker to consume SQS messages	1017
SETTING UP THE SERVER PROJECT	1018
Listing 5 Initializing the Imagery worker (worker/worker.js).....	1018
HANDLING SQS MESSAGES AND PROCESSING THE IMAGE	1019
Figure 14 Processing a raw image to upload a sepia image to S3	1019
Listing 6 Imagery worker: POST /sqs handles SQS messages	1020
3.4 Deploying the application.....	1023
CloudFormation does a bit more than deploy two Elastic Beanstalk applications. It defines the following:	1023
DEPLOYING S3, DYNAMODB, AND SQS	1024
Listing 7 Imagery CloudFormation template: S3, DynamoDB, and SQS	1024
IAM ROLES FOR SERVER AND WORKER EC2 INSTANCES	1027
All server instances must be able to do the following:	1027
All worker instances must be able to do the following:.....	1027
ELASTIC BEANSTALK FOR THE SERVER.....	1028
An Elastic Beanstalk consists of these elements:.....	1028
■ An application.....	1028
■ A version.....	1028
■ A configuration template.....	1028
■ An environment.....	1028
Figure 15 An AWS Elastic Beanstalk application consists of versions, configurations, and environments.	1029
Listing 8 Imagery CloudFormation template: Elastic Beanstalk for the server	1030
ELASTIC BEANSTALK FOR THE WORKER	1032
ELASTIC BEANSTALK FOR THE WORKER	1032
Listing 9 Imagery CloudFormation template: Elastic Beanstalk for the worker.....	1033
Figure 16 The Imagery application in action.....	1037
Cleaning up.....	1037
CHAPTER – BABYLONJS BASICS	1038
<i>Introduction</i>	1038
Prerequisites	1038
WebGL.....	1039
TypeScript.....	1039
<i>Environment Setup</i>	1039
<i>Overview</i>	1040
BabylonJs offers following features which help to create different types of 3D-scenes:.....	1041
Blender	1041

FBX.....	1042
MAX.....	1042
<i>Basic Elements</i>	1042
Sample Demo 1	1042
Step 1.....	1048
Step 2.....	1049
Step 3.....	1051
Step 4.....	1054
Rendering Loop.....	1054
Step 5.....	1057
Adding Camera and Light.....	1057
code:	1058
Step 6.....	1058
Adding of shapes	1058
code:	1058
code looks as follows:	1059
Output	1062
output:.....	1063
<i>Summary of all the shapes and the syntax:</i>	1069
<i>Basic Element-Box</i>	1072
Syntax.....	1072
Parameters	1072
Demo – Box	1073
Output	1077
<i>Basic Element-Sphere</i>	1077
Syntax.....	1077
Parameters.....	1077
Demo – Sphere	1079
Output	1081
<i>Sphere can also be created using the meshbuilder</i>	1081
Syntax to create a sphere using the meshbuilder:	1081
The Properties for a Sphere	1081
CHAPTER – PENETRATION TESTING	1083
<i>AWS Customer Support Policy for Penetration Testing</i>	1083
<i>Customer Service Policy for Penetration Testing</i>	1083
Permitted Services	1083

Prohibited Activities	1084
Requesting Authorization for Other Simulated Events	1084
<i>TERMS AND CONDITIONS</i>	1084
<i>AWS POLICY REGARDING THE USE OF SECURITY ASSESSMENT TOOLS AND SERVICES</i>	1085
CHAPTER - TEN WAYS TO DEPLOY AWS QUICKLY	1087
1 RESEARCHING AWS INTERACTIVITY WITH THIRD-PARTY PRODUCTS	1087
QUESTION:	1087
Explanation:	1087
Third-party software support.....	1087
Reference:	1088
2 DEVELOPING A PLAN FOR SENSITIVE DATA	1088
3 USE TOOLS TO ENHANCE PRODUCTIVITY.....	1088
» Built-in:	1088
» Third party:	1088
» Developer:	1088
4 CHOOSING THE RIGHT SERVICE	1090
5 ENSURING THAT YOUR PLAN CONSIDERS LOSS OF CONTROL	1090
6 LOOKING FOR ALL-IN-ONE SOLUTIONS.....	1090
7 SPENDING FREE TIME WHERE YOU NEED IT MOST	1091
8 WORKING WITH TEMPLATES	1091
QUESTION	1091
Explanation:	1092
9 DISCOVERING IMPLIED THIRD-PARTY USE	1092
QUESTION:	1093
Explanation:	1094
For example,	1094
Explanation of the Cloud Solution/Pattern	1094
Implementation	1095
Benefits	1097
Cautions	1097
CHAPTER - SERVICE CONTROL POLICIES (SCPS)	1098
Topics	1098
<i>Testing effects of SCPs</i>	1099
<i>Maximum size of SCPs</i>	1099
<i>Inheritance of SCPs in the OU hierarchy</i>	1099

SCP effects on permissions.....	1100
Using access data to improve SCPs.....	1101
Tasks and entities not restricted by SCPs.....	1102
You can't use SCPs to restrict the following tasks:.....	1102
Exceptions for only member accounts created before September 15, 2017.....	1102
CHAPTER - SIX STRATEGIES FOR MIGRATING APPLICATIONS TO THE CLOUD.....	1104
Formulating a Migration Strategy.....	1104
Portfolio Discovery and Planning.....	1104
6 APPLICATION MIGRATION STRATEGIES: "THE 6 R'S".....	1104
1 Rehosting—Otherwise known as "lift-and-shift.".....	1105
2. Replatforming—I sometimes call this "lift-tinker-and-shift.".....	1106
3. Repurchasing—Moving to a different product.....	1106
4. Refactoring / Re-architecting—Re-imagining how the application is architected and developed, typically using cloud-native features.....	1106
5. Retire—Get rid of.....	1107
6. Retain—Usually this means "revisit" or do nothing (for now).....	1107
CHAPTER - TEN MUST-HAVE AWS SOFTWARE PACKAGES.....	1108
1 USING THE CONSOLE INTERNET TOOLS.....	1108
2 USING THE COMMAND LINE INTERFACE (CLI)TO INSTALL PACKAGES.....	1108
3 CHANGING CONFIGURATION USING COMMAND LINE EDITORS.....	1110
4 CHECKING SYSTEM PERFORMANCE.....	1110
5 WORKING AT THE SYSTEM LEVEL.....	1111
6 MAKING CLOUD MANAGEMENT EASIER WITH CLOUDMGR.....	1114
AWS supports three levels of CloudMGR:.....	1114
» CloudMGR Business:	1114
» CloudMGR for Autotask:	1114
» CloudMGR for cPanel Web Host Manager Complete Solution (WHMCS):	1114
7 GOING OUTSIDE THE MARKETPLACE WITH ENSTRATIUS.....	1115
8 MANAGING AND SCALING YOUR APPS USING HEROKU.....	1115
The product defines three phases of custom app management:.....	1115
The supported Linux distributions are.....	1115
You can use these languages directly with Heroku:.....	1115
9 PERFORMING BROWSER-BASED MANAGEMENT USING HYBRIDFOX.....	1116
Use Hybridfox to perform these kinds of tasks:.....	1116
9 GETTING A COMPLETE MANAGEMENT PACKAGE WITH RIGHTSCALE.....	1116
10 EMPLOYING POLICY-BASED MANAGEMENT WITH SCALR.....	1117

QUESTIONS AND EXPLANATIONS:	1117
AWS CloudHSM.....	1118
AWS CloudHSM requires the following environment before an HSM appliance can be provisioned.	1119
CHAPTER – AWS SUPPORT PLANS.....	1120
<i>Compare AWS Support Plans</i>	1120
Basic Support is included for all AWS customers and includes:	1120
Customer Service and Communities -	1120
AWS Trusted Advisor -.....	1120
AWS Personal Health Dashboard -	1120
Developer, Business and Enterprise includes:.....	1121
CHAPTER - PLANNING YOUR NEXT STEPS	1124
1 RESOURCES, RECOMMENDATIONS, AND BEST PRACTICES.....	1125
2 AMAZON WEB SERVICES SCREEN SHOTS	1126
3 ALTERNATIVE WEB SERVICES PROVIDERS.....	1127
Below are some common features of cloud providers:	1127
4 THE DIFFERENCE BETWEEN AWS, AZURE, GOOGLE CLOUD AND OPENSTACK TABLE	1128
5 A FEW EXAMPLE OF COMPANIES AND ORGANIZATIONS RUNNING WEB SERVICES	1130
AWS.....	1130
GOOGLE CLOUD PLATFORM	1131
MICROSOFT AZURE	1131
6 CLOUD SERVICES COMPARISON TABLE	1132
INDEX.....	1138
REFERENCES	1147