Save 10%
on Exam
Voucher

See Inside

EXAM CRAM

CompTIA® Cloud+ CV0-003

Cram Sheet

Flash Cards

Practice Tests

WILLIAM "BO" ROTHWELL

FREE SAMPLE CHAPTER

SHARE WITH OTHERS

EXAM CRAM

CompTIA® Cloud+ CV0-003 Exam Cram

William "Bo" Rothwell

Pearson

CompTIA® Cloud+ CV0-003 Exam Cram

Copyright © 2022 by Pearson Education, Inc.

All rights reserved. This publication is protected by copyright, and permission must be obtained from the publisher prior to any prohibited reproduction, storage in a retrieval system, or transmission in any form or by any means, electronic, mechanical, photocopying, recording, or likewise. For information regarding permissions, request forms, and the appropriate contacts within the Pearson Education Global Rights & Permissions Department, please visit www.pearson.com/permissions.

No patent liability is assumed with respect to the use of the information contained herein. Although every precaution has been taken in the preparation of this book, the publisher and author assume no responsibility for errors or omissions. Nor is any liability assumed for damages resulting from the use of the information contained herein.

ISBN-13: 978-0-13-739325-1

ISBN-10: 0-13-739325-3

Library of Congress Control Number: 2021916057

ScoutAutomatedPrintCode

Trademarks

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Pearson IT Certification cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

Warning and Disclaimer

Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied. The information provided is on an “as is” basis. The author and the publisher shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the supplementary online content.

Special Sales

For information about buying this title in bulk quantities, or for special sales opportunities (which may include electronic versions; custom cover designs; and content particular to your business, training goals, marketing focus, or branding interests), please contact our corporate sales department at corpsales@pearsoned.com or (800) 382-3419.

For government sales inquiries, please contact governmentsales@pearsoned.com.

For questions about sales outside the U.S., please contact intlcs@pearson.com.

Editor-in-Chief
Mark Taub

Director,
ITP Product
Management
Brett Bartow

Executive Editor
Nancy Davis

Managing Editor
Sandra Schroeder

Project Editor
Mandie Frank

Copy Editor
Chuck Hutchinson

Indexer
Ken Johnson

Proofreader
Abigail Manheim

Technical Editor
Akhil Behl

Publishing
Coordinator
Cindy Teeters

Designer
Chuti Prasertsith

Compositor
codeMantra

Pearson's Commitment to Diversity, Equity, and Inclusion

Pearson is dedicated to creating bias-free content that reflects the diversity of all learners. We embrace the many dimensions of diversity, including but not limited to race, ethnicity, gender, socioeconomic status, ability, age, sexual orientation, and religious or political beliefs.

Education is a powerful force for equity and change in our world. It has the potential to deliver opportunities that improve lives and enable economic mobility. As we work with authors to create content for every product and service, we acknowledge our responsibility to demonstrate inclusivity and incorporate diverse scholarship so that everyone can achieve their potential through learning. As the world's leading learning company, we have a duty to help drive change and live up to our purpose to help more people create a better life for themselves and to create a better world.

Our ambition is to purposefully contribute to a world where:

- Everyone has an equitable and lifelong opportunity to succeed through learning.
- Our educational products and services are inclusive and represent the rich diversity of learners.
- Our educational content accurately reflects the histories and experiences of the learners we serve.
- Our educational content prompts deeper discussions with learners and motivates them to expand their own learning (and worldview).

While we work hard to present unbiased content, we want to hear from you about any concerns or needs with this Pearson product so that we can investigate and address them.

- Please contact us with concerns about any potential bias at https://www.pearson.com/report-bias.html.

Credits

Figure 3-1	Screenshot of CPU Compute Options © 2021, Amazon Web Services, Inc.
Figure 3-2	Screenshot of Database Class © 2021, Amazon Web Services, Inc.
Figure 3-3	Screenshot of Microsoft Azure Regions © Microsoft 2020
Figure 4-1	Screenshot of AWS EC2 Instance Types © 2021, Amazon Web Services, Inc.
Figure 5-1	Screenshot of Federation login example © Copyright 2021 Cisco DevNet
Figure 5-2	Screenshot of Invalid certificate warning © Google
Figure 5-3	Screenshot of List of CAs on a Google Chrome browser © Google
Figure 7-1	Screenshot of AWS Password Policy © 2021, Amazon Web Services, Inc.
Figure 7-2	Screenshot of Changing the permissions of a file in Windows © 2021, Amazon Web Services, Inc.
Figure 8-1	Screenshot of AWS Tags © 2021, Amazon Web Services, Inc.
Figure 10-1	© DZone, Inc.
Figure 10-2	© 1994 - 2018 Micro Focus
Figure 11-1	Screenshot of AWS instance details © 2021, Amazon Web Services, Inc.
Figure 12-1	© 2021, Amazon Web Services, Inc.
Figure 12-2	© 2021, Amazon Web Services, Inc.
Figure 14-3	Screenshot of Type 3 hypervisor © 2021, Amazon Web Services, Inc.
Figure 14-4	Screenshot of CPU Clock Speed value © 2021, Amazon Web Services, Inc.
Figure 15-1	Screenshot of Exporting a virtual machine in OVF format © 2021 Oracle
Figure 17-1	Screenshot of AWS Cloudwatch dashboard data representations © 2021, Amazon Web Services, Inc.
Figure 17-2	Screenshot of AWS Service Health Dashboard © 2021, Amazon Web Services, Inc.
Figure 17-3	Screenshot of AWS Personal Health Dashboard © 2021, Amazon Web Services, Inc.
Figure 18-1	Screenshot of AWS database instance bandwidth © 2021, Amazon Web Services, Inc.
Figure 21-1	Screenshot of Network diagram from Lucidchart tool © 2021 Lucid Software Inc
Figure 24-1	Screenshot of AWS Service Health Dashboard © 2021, Amazon Web Services, Inc.
Figure 25-1	Screenshot of The Wireshark command © Wireshark

Contents at a Glance

Introduction xxvi

CHAPTER 1 Different Types of Cloud Models 1

CHAPTER 2 Capacity Planning 15

CHAPTER 3 High Availability and Scaling in Cloud Environments 25

CHAPTER 4 Solution Design in Support of the Business Requirements 41

CHAPTER 5 Identity and Access Management 55

CHAPTER 6 Secure a Network in a Cloud Environment 71

CHAPTER 7 OS and Application Security Controls 87

CHAPTER 8 Data Security and Compliance Controls in Cloud Environments 103

CHAPTER 9 Security Requirements 115

CHAPTER 10 Incident Response Procedures 123

CHAPTER 11 Integrate Components into a Cloud Solution 135

CHAPTER 12 Storage in Cloud Environments 149

CHAPTER 13 Cloud Networking Solutions 165

CHAPTER 14 Compute Sizing for a Deployment 181

CHAPTER 15 Cloud Migrations 193

CHAPTER 16 Logging, Monitoring, and Alerting 205

CHAPTER 17 Operation of a Cloud Environment 217

CHAPTER 18 Optimize Cloud Environments 235

CHAPTER 19 Automation and Orchestration Techniques 247

CHAPTER 20 Backup and Restore Operations 259

CHAPTER 21 Disaster Recovery Tasks 273

CHAPTER 22 Troubleshooting Methodology 281

CHAPTER 23 Troubleshoot Security Issues 289

CHAPTER 24 Troubleshoot Deployment, Automation, and Orchestration Issues 301

CHAPTER 25 Troubleshoot Connectivity Issues and Common Performance Issues 317

Glossary of Essential Terms and Components 341

Index 361

Contents

Introduction . . . . **xxvi**

CHAPTER 1:
Different Types of Cloud Models **1**

Cloud Deployment Models 2

Public Cloud 3

Private Cloud 4

Hybrid Cloud 4

Community Cloud 5

Cloud Within a Cloud 5

Multicloud 6

Multitenancy 6

Cloud Service Models 6

Infrastructure as a Service (IaaS) 7

Platform as a Service (PaaS) 8

Software as a Service (SaaS) 8

Advanced Cloud Services 9

Internet of Things (IoT) 9

Serverless 9

Machine Learning/Artificial Intelligence (AI) 10

Cloud Shared Responsibility Model 11

What Next? 14

CHAPTER 2:
Capacity Planning **15**

Requirements 16

Hardware Requirements 16

Software Requirements 17

Budgetary Requirements 17

Business Need Analysis 17

Standard Templates 18

Licensing 18

Per-user 19

Socket-based 19

Volume-based 19

Core-based . . . 19
Subscription . . . 20
User Density . . . 20
System Load . . . 21
Trend Analysis . . . 21
Baselines . . . 21
Patterns . . . 22
Anomalies . . . 22
Performance Capacity Planning . . . 22
What Next? . . . 24

CHAPTER 3:
High Availability and Scaling in Cloud Environments . . . 25

Hypervisors . . . 26
Affinity . . . 27
Anti-affinity . . . 27
Oversubscription . . . 28
Compute . . . 28
Network . . . 29
Storage . . . 30
Regions and Zones . . . 30
Applications . . . 32
Containers . . . 32
Clusters . . . 33
High Availability of Network Functions . . . 33
Switches . . . 33
Routers . . . 33
Load Balancers . . . 34
Firewalls . . . 35
Avoid Single Points of Failure . . . 36
Scalability . . . 36
Auto-scaling . . . 36
Horizontal Scaling . . . 37
Vertical Scaling . . . 37
Cloud Bursting . . . 37
What Next? . . . 39

CHAPTER 4:
Solution Design in Support of the Business Requirements **41**
Requirement Analysis 42
Software 42
Hardware 43
Integration 45
Budgetary 45
Compliance 46
Service-Level Agreement (SLA) 46
User and Business Needs. 46
Security 46
Network Requirements 47
Environments 48
Development 48
Quality Assurance (QA). 48
Staging 49
Blue-Green 49
Production 49
Disaster Recovery (DR). 49
Testing Techniques 50
Vulnerability Testing. 50
Penetration Testing 50
Performance Testing. 51
Regression Testing 51
Functional Testing 51
Usability Testing 51
What Next? 53

CHAPTER 5:
Identity and Access Management **55**
Identification and Authorization 56
Privileged Access Management (PAM) 57
Logical Access Management 57
Account Lifecycle Management 58
Access Controls 59
Directory Services 60
Lightweight Directory Access Protocol (LDAP) 61
Federation 61
Certificate Management 63

Multifactor Authentication (MFA) 64
Single Sign-On (SSO) 65
Security Assertion Markup Language (SAML) 66
Public Key Infrastructure (PKI) 66
Secret Management 67
Key Management 67
What Next? 69

CHAPTER 6:
Secure a Network in a Cloud Environment 71

Network Segmentation 72
Virtual LAN (VLAN)/Virtual Extensible LAN (VxLAN)/ Generic Network Virtualization Encapsulation (GENEVE) 72
Microsegmentation 73
Tiering 73
Protocols 74
Domain Name Service (DNS) 74
Network Time Protocol (NTP) 75
Network Time Security (NTS) 75
Encryption 75
Tunneling 76
Network Services 77
Firewalls 78
Web Application Firewall (WAF) 78
Application Delivery Controller (ADC) 79
Intrusion Protection System (IPS)/Intrusion Detection System (IDS) 79
Data Loss Prevention (DLP) 79
Network Access Control (NAC) 79
Packet Brokers 80
Log and Event Monitoring 80
Network Flows 80
Hardening and Configuration Changes 81
Disabling Unnecessary Ports and Services 81
Disabling Weak Protocols and Ciphers 81
Firmware Upgrades 82
Control Ingress and Egress Traffic 82
Distributed Denial-of-Service (DDoS) Protection 84
What Next? 86

CHAPTER 7:
OS and Application Security Controls . . . 87

Policies . . . 88
Password Complexity . . . 88
Account Lockout . . . 89
Application Whitelisting . . . 89
Software Feature . . . 90
User/Group . . . 90
User Permissions . . . 90
Antivirus/Antimalware/Endpoint Detection and Response (EDR) . . . 93
Host-Based IDS (HIDS)/Host-Based IPS (HIPS) . . . 94
Hardened Baselines . . . 94
Single Function . . . 95
File Integrity . . . 96
Log and Event Monitoring . . . 96
Configuration Management . . . 96
Builds . . . 96
Stable . . . 96
Long-Term Support (LTS) . . . 97
Beta . . . 97
Canary . . . 97
Operating System (OS) Upgrades . . . 98
Encryption . . . 98
Application Programming Interface (API) Endpoint . . . 98
Application . . . 98
OS . . . 98
Storage . . . 98
Filesystem . . . 99
Mandatory Access Control . . . 99
Firewall Software . . . 100
What Next? . . . 101

CHAPTER 8:
Data Security and Compliance Controls in Cloud Environments . . . 103

Encryption . . . 104
Integrity . . . 105
Hashing Algorithms . . . 105
Digital Signatures . . . 106
File Integrity Monitoring (FIM) . . . 106

Classification 107
Segmentation 108
Access Control 108
Impact of Laws and Regulations 109
Legal Hold 109
Records Management 110
Versioning 110
Retention 110
Destruction 110
Write Once Read Many 110
Data Loss Prevention (DLP) 111
Cloud Access Security Broker (CASB) 111
What Next? 113

CHAPTER 9:
Security Requirements 115
Tools 116
Vulnerability Scanners 116
Port Scanners 116
Vulnerability Assessment 117
Default and Common Credential Scans 117
Credentialed Scans 118
Network-Based Scans 118
Agent-Based Scans 118
Service Availabilities Scans 118
Security Patches 118
Hot Fixes 119
Scheduled Updates 119
Virtual Patches 119
Signature Updates 119
Rollups 120
Risk Register 120
Prioritization of Patch Applications 120
Deactivate Default Accounts 120
Impacts of Security Tools on Systems and Services 121
What Next? 122

CHAPTER 10:
Incident Response Procedures **123**
Preparation 124
Documentation 124
Call Trees 125
Training 126
Tabletops 126
Documented Incident Types/Categories 127
Roles and Responsibilities 128
Incident Response Procedures 130
Identification 130
Containment, Eradication, and Recovery 131
Postincident and Lessons Learned 132
What Next? 134

CHAPTER 11:
Integrate Components into a Cloud Solution **135**
Subscription Services 136
File Subscriptions 137
Communications 137
Collaboration 138
Virtual Desktop Infrastructure (VDI) 138
Directory and Identity Services 139
Cloud Resources 139
IaaS 140
PaaS 140
SaaS 140
Provisioning Resources 140
Compute 141
Storage 141
Network 142
Application 142
Serverless 143
Deploying Virtual Machines (VMs) and Custom Images 143
Templates 143
OS Templates 143
Solution Templates 144
Identity Management 145

Containers . . . 145
Configure Variables . . . 145
Configure Secrets . . . 145
Persistent Storage . . . 146
Auto-scaling . . . 146
Postdeployment Validation . . . 146
What Next? . . . 148

CHAPTER 12:
Storage in Cloud Environments . . . 149
Types . . . 150
Block . . . 150
File . . . 151
Object . . . 151
Tiers . . . 152
Flash . . . 152
Hybrid . . . 152
Spinning Disks . . . 152
Long-Term . . . 152
Input/Output Operations per Second (IOPS) and Read/Write . . . 153
Protocols . . . 154
Network File System (NFS) . . . 154
Common Internet File System (CIFS) . . . 155
Internet Small Computer System Interface (iSCSI) . . . 155
Fibre Channel (FC) . . . 156
Non-Volatile Memory Express over Fabrics (NVMe-oF) . . . 156
Redundant Array of Inexpensive Disks (RAID) . . . 157
0 . . . 157
1 . . . 158
5 . . . 158
6 . . . 159
10 . . . 159
Storage System Features . . . 159
Compression . . . 160
Deduplication . . . 160
Thin Provisioning . . . 160
Thick Provisioning . . . 161
Replication . . . 161

User Quotas 161
Hyperconverged 161
Software-Defined Storage (SDS) 162
What Next? 163

CHAPTER 13:
Cloud Networking Solutions 165

Services 166
Dynamic Host Configuration Protocol (DHCP) 166
Network Time Protocol (NTP) 166
Domain Name Service (DNS) 167
Content Delivery Network (CDN) 169
IP Address Management (IPAM) 170
Virtual Private Networks (VPNs) 170
Site-to-site 170
Point-to-Point 171
Point-to-Site 171
IPsec 171
Multiprotocol Label Switching (MPLS) 171
Virtual Routing 171
Dynamic and Static Routing 172
Virtual Network Interface Controller (vNIC) 172
Subnetting 172
Network Appliances 176
Load Balancers 176
Firewalls 177
Virtual Private Cloud (VPC) 177
Hub and Spoke 178
Peering 178
VLAN/VxLAN/GENEVE 178
Single Root Input/Output Virtualization (SR-IOV) 179
Software-Defined Network (SDN) 179
What Next? 180

CHAPTER 14:
Compute Sizing for a Deployment 181

Virtualization 182
Hypervisors 182
Simultaneous Multithreading (SMT) 184

Dynamic Allocations 185
Oversubscription 185
Central Processing Unit (CPU)/ Virtual CPU (vCPU) 185
Graphics Processing Unit (GPU) 186
Virtual 186
Pass-through 186
Clock Speed/Instructions per Cycle (IPC) 187
Hyperconverged 188
Memory 188
Dynamic Allocation 189
Ballooning 189
What Next? 191

CHAPTER 15:
Cloud Migrations 193
Physical to Virtual (P2V) 194
Virtual to Virtual (V2V) 195
Cloud-to-Cloud Migrations 196
Vendor Lock-in 196
PaaS or SaaS Migrations 196
Storage Migrations 198
Block 199
File 199
Object 200
Database Migrations 200
Relational 201
Nonrelational 201
What Next? 203

CHAPTER 16:
Logging, Monitoring, and Alerting 205
Logging 206
Collectors 206
Analysis 207
Severity Categorization 207
Audits 208
Types 208

Automation 209
Trending 209
Monitoring 209
Baselines 210
Thresholds 210
Tagging 210
Log Scrubbing 211
Performance Monitoring 211
Resource Utilization 212
Availability 212
Verification of Continuous Monitoring Activities 213
Service Management Tool Integration 213
Alerting 214
Common Messaging Methods 214
Enable/Disable Alerts 214
Appropriate Responses 214
Policies for Categorizing and Communicating Alerts 215
What Next? 216

CHAPTER 17:
Operation of a Cloud Environment 217

Confirm Completion of Backups 218
Lifecycle Management 218
Roadmaps 218
Old/Current/New Versions 219
Upgrading and Migrating Systems 219
Deprecations or End of Life 220
Change Management 220
Asset Management 220
Configuration Management Database (CMDB) 221
Patching 221
Features or Enhancements 221
Fixes for Broken or Critical Infrastructure or Applications 222
Scope of Cloud Elements to Be Patched 222
Software 224
Policies 225
Rollbacks 225
Impacts of Process Improvements on Systems 226

Upgrade Methods . . . 226
Rolling Upgrades . . . 226
Blue-Green . . . 227
Canary . . . 227
Active-Passive . . . 227
Development/QA/Production/DR . . . 227
Dashboard and Reporting . . . 228
Tagging . . . 229
Costs . . . 229
Elasticity Usage . . . 231
Connectivity . . . 231
Latency . . . 231
Capacity . . . 232
Incidents . . . 232
Health . . . 232
Overall Utilization . . . 233
Availability . . . 233
What Next? . . . 234

CHAPTER 18:
Optimize Cloud Environments . . . 235

Right-sizing . . . 236
Compute and Storage . . . 236
Network . . . 237
Bandwidth . . . 237
Network Interface Controllers (NICs) . . . 239
Latency . . . 240
Software-Defined Networks (SDNs) . . . 241
Edge Computing . . . 241
Placement . . . 242
Geographical . . . 242
Cluster Placement . . . 242
Redundancy . . . 243
Colocation . . . 243
Device Drivers and Firmware . . . 243
Generic . . . 244
Vendor . . . 244
Open Source . . . 245
What Next? . . . 246

CHAPTER 19:
Automation and Orchestration Techniques . . . 247
- Infrastructure as Code (IaC) . . . 248
  - Infrastructure Components and Their Integration . . . 249
- Continuous Integration/Continuous Deployment (CI/CD) . . . 249
- Version Control . . . 250
- Configuration Management . . . 251
  - Playbook . . . 252
- Containers . . . 252
- Automation Activities . . . 252
  - Routine Operations . . . 253
  - Updates . . . 253
  - Scaling . . . 253
  - Shutdowns . . . 254
  - Restarts . . . 254
  - Create Internal APIs . . . 254
- Secure Scripting . . . 254
  - No Hardcoded Passwords . . . 255
  - Use of Individual Service Accounts . . . 255
  - Password Vaults . . . 255
  - Key-Based Authentication . . . 255
- Orchestration Sequencing . . . 255
- What Next? . . . 257

CHAPTER 20:
Backup and Restore Operations . . . 259
- Backup Types . . . 260
  - Incremental . . . 260
  - Differential . . . 261
  - Full . . . 261
  - Synthetic Full . . . 262
  - Snapshot . . . 262
- Backup Objects . . . 263
  - Application-Level Backup . . . 263
  - File-System Backup . . . 264
  - Database Dumps . . . 264
  - Configuration Files . . . 264

Backup Targets 265
- Tape 265
- Disk 265
- Object 266

Backup and Restore Policies 266
- Retention 266
- Schedules 267
- Location 267
- Service-Level Agreements (SLAs) 268
- Recovery Time Objective (RTO) 268
- Recovery Point Objective (RPO) 268
- Mean Time to Recovery (MTTR) 269
- 3-2-1 Rule 269

Restoration Methods 269
- In Place 269
- Alternate Location 270
- Restore Files 270
- Snapshot 270

What Next? 272

CHAPTER 21:
Disaster Recovery Tasks 273

Failovers 274

Failback 274

Restore Backups 275

Replication 275

On-Premises and Cloud Sites 275
- Hot 275
- Warm 276
- Cold 276

Requirements 277
- Corporate Guidelines 277

Documentation 277
- DR Kit 278
- Playbook 278
- Network Diagram 278

Geographical Data Center Requirements 279

What Next? 280

CHAPTER 22:
Troubleshooting Methodology **281**

Always Consider Corporate Policies, Procedures, and Impacts Before Implementing Changes 282
1. Identify the Problem 283
2. Establish a Theory of Probable Cause (Question the Obvious) 284
3. Test the Theory to Determine Cause 285
4. Establish a Plan of Action to Resolve the Problem and Implement the Solution. 285
5. Verify Full System Functionality and, if Applicable, Implement Preventive Measures 286
6. Document the Findings, Actions, and Outcomes Throughout the Process 286
What Next? 288

CHAPTER 23:
Troubleshoot Security Issues **289**

Privilege 290
Missing 290
Incomplete 290
Escalation 291
Keys 291
Authentication 291
Authorization 292
Security Groups 293
Network Security Groups 293
Directory Security Groups 294
Keys and Certificates 294
Expired 294
Revoked 295
Trust 295
Compromised 295
Misconfigured 295
Misconfigured or Misapplied Policies 295
Data Security Issues 296
Unencrypted Data 296
Data Breaches 296
Misclassification 296
Lack of Encryption in Protocols 296
Insecure Ciphers 297

Exposed Endpoints 297
Misconfigured or Failed Security Appliances 298
Unsupported Protocols 298
External/Internal Attacks 298
What Next? 300

CHAPTER 24:
Troubleshoot Deployment, Automation, and Orchestration Issues 301

Connectivity Issues 302
Cloud Service Provider (CSP) or Internet Service Provider (ISP) Outages 302
Performance Degradation 304
Latency 304
Configurations 305
Scripts 305
Applications in Containers 306
Misconfigured Templates 306
Missing or Incorrect Tags 306
Insufficient Capacity 307
Licensing Issues 307
Vendor-Related Issues 308
Migrations of Vendors or Platforms 308
Integration of Vendors or Platforms 308
API Request Limits 308
Cost or Billing Issues 309
Account Mismatches 310
Change Management Failures 310
Server Name Changes 311
IP Address Changes 311
Location Changes 312
Version/Feature Mismatch 312
Automation Tool Incompatibility 313
Deprecated Features 313
API Version Incompatibility 314
Job Validation Issue 314
Patching Failure 315
What Next? 316

CHAPTER 25:
Troubleshoot Connectivity Issues and Common Performance Issues 317
Network Security Group Misconfigurations 318
Access Control Lists (ACLs) 318
Inheritance 319
Common Networking Configuration Issues 319
Peering 320
Incorrect Subnet, IP Address, and IP Space 320
Routes 321
Firewall 322
Network Address Translation (NAT) 322
Load Balancers and DNS Records 323
VLAN/VxLAN/GENEVE and Proxy 324
Maximum Transmission Unit (MTU) 324
Quality of Service (QoS) 324
Time Synchronization Issues 324
Network Troubleshooting Tools 324
ping 325
tracert/traceroute 325
flushdns 326
ipconfig/ifconfig/ip 326
nslookup/dig 328
netstat/ss 330
route 332
arp 332
curl 333
Packet Capture 334
Packet Analyzer 335
OpenSSL Client 336
Resource Utilization 336
Application 337
Memory Management 337
Service Overload 337
Incorrectly Configured or Failed Load Balancing 338
What Next? 339

Glossary of Essential Terms and Components 341

Index 361

About the Author

At the impressionable age of 14, **William "Bo" Rothwell** crossed paths with a TRS-80 Micro Computer System (affectionately known as a "Trash 80"). Soon after, the adults responsible for Bo made the mistake of leaving him alone with the TSR-80. He immediately dismantled it and held his first computer class, showing his friends what made this "computer thing" work. Since that experience, Bo's passion for understanding how computers work and sharing this knowledge with others has resulted in a rewarding career in IT training. His experience includes cloud, Linux, UNIX, IT security, DevOps, and programming languages such as Perl, Python, Tcl, and BASH. He is the founder and lead instructor of One Course Source, an IT training organization.

Dedication

To my sister, Betsy, who I tormented so much growing up. I'm glad that now we are adults you have either forgotten or forgiven my misdeeds.

To my parents: 99.7 percent of the time Betsy confessed and got in trouble, it was really me.

To my childhood dog, Hansel, thank you for always being there, under the dining room table, when I needed vegetables to disappear from my plate. You learned to chew silently, and for that, I was grateful.

To my seventh-grade homeroom teacher, you know who you are. You said I was lazy and would never amount to anything. If you are reading this now, you have concrete proof in your hands that you were mistaken.

Acknowledgments

I always worry when I write this section that I will miss someone who has helped me with this book. It takes a team to write a book, but often the author gets all of the credit. For all of the editors and support staff who have helped make this book possible, thank you very much.

About the Technical Reviewer

Akhil Behl, CCIE Emeritus No. 19564, is a passionate IT executive with a key focus on the cloud and security. He has 18+ years of experience in the IT industry working across several leadership, advisory, consultancy, and business development profiles with various organizations. His technology and business specializations include cloud, security, infrastructure, data center, and business communication technologies. Currently, he leads business development for the cloud for a global systems integrator.

Akhil has written multiple titles on security and business communication technologies. In addition, he has contributed as technical editor for more than a dozen books on security, networking, and information technology. He also has published four books with Pearson Education/Cisco Press.

He has published several research papers in national and international journals, including *IEEE Xplore*, and presented at various IEEE conferences, as well as other prominent ICT, security, and telecom events. Writing and mentoring are his passion and a part of his life.

He holds CCIE Emeritus (Collaboration and Security), Azure Solutions Architect Expert, Google Professional Cloud Architect, Azure AI Certified Associate, Azure Data Fundamentals, CCSK, CHFI, PMP, ITIL, VCP, TOGAF, CEH, ISM, CCDP, and many other industry certifications. He has a bachelor's degree in technology and a master's of business administration degree.

We Want to Hear from You!

As the reader of this book, you are our most important critic and commentator. We value your opinion and want to know what we're doing right, what we could do better, what areas you'd like to see us publish in, and any other words of wisdom you're willing to pass our way.

We welcome your comments. You can email or write to let us know what you did or didn't like about this book—as well as what we can do to make our books better.

Please note that we cannot help you with technical problems related to the topic of this book.

When you write, please be sure to include this book's title and author as well as your name and email address. We will carefully review your comments and share them with the author and editors who worked on the book.

Email: community@informit.com

Introduction

Welcome to *CompTIA Cloud+ CV0-003 Exam Cram*. This book will help you get ready to take and pass the CompTIA Cloud+ exam CV0-003.

This book is designed to remind you of everything you need to know to pass the CV0-003 certification exam. Each chapter includes a number of practice questions that should give you a reasonably accurate assessment of your knowledge, and, yes, we've provided the answers and their explanations for these questions. Read this book, understand the material, and you'll stand a very good chance of passing the real test.

Exam Cram books help you understand and appreciate the subjects and materials you need to know to pass CompTIA certification exams. *Exam Cram* books are aimed strictly at test preparation and review. They do not teach you everything you need to know about a subject. Instead, the authors streamline and highlight the pertinent information by presenting and dissecting the questions and problems they've discovered that you're likely to encounter on a CompTIA test.

Let's begin by looking at preparation for the exam.

How to Prepare for the Exam

This text follows the official exam objectives closely to help ensure your success. The CompTIA exam covers 5 domains and 27 objectives, and this book is aligned with those domains and objectives. These official objectives from CompTIA can be found here:

> https://www.comptia.org/training/resources/exam-objectives

As you examine the numerous exam topics now covered in Cloud+, resist the urge to panic! This book you are holding will provide you with the knowledge (and confidence) that you need to succeed. You just need to make sure you read it and follow the guidance it provides throughout your Cloud+ journey.

Practice Tests

This book is filled with practice exam questions to get you ready!

- **CramSaver questions at the beginning of each chapter:** These difficult, open-ended questions ensure you really know the material. Some readers use these questions to "test out" of a particular topic.

- **CramQuizzes at the end of each chapter:** These quizzes provide another chance to demonstrate your knowledge after completing a chapter.

In addition, the book includes two full practice tests in the Pearson Test Prep software available to you either online or as an offline Windows application. To access the practice exams, please see the instructions in the card inserted in the sleeve in the back of the book. This card includes a unique access code that enables you to activate your exams in the Pearson Test Prep software.

If you are interested in more practice exams than are provided with this book, Pearson IT Certification publishes a Premium Edition eBook and Practice Test product. In addition to providing you with three eBook files (EPUB, PDF, and Kindle), this product provides you with two additional exams' worth of questions. The Premium Edition version also offers you a link to the specific section in the book that presents an overview of the topic covered in the question, allowing you to easily refresh your knowledge. The insert card in the back of the book includes a special offer for an 80 percent discount off this Premium Edition eBook and Practice Test product, which is an incredible deal.

Taking a Certification Exam

After you prepare for your exam, you need to register with a testing center. At the time of this writing, the cost to take the Cloud+ exam is $338 USD for individuals. Students in the United States are eligible for a significant discount. Additionally, check with your employer because many workplaces provide reimbursement programs for certification exams. For more information about these discounts, you can contact a local CompTIA sales representative, who can answer any questions you might have. If you don't pass, you can take the exam again for the same cost as the first attempt until you pass. The test is administered by Pearson VUE testing centers with locations globally. In addition, the CompTIA Cloud+ certification might fulfill requirements for many within the U.S. military, and testing centers are available on some military bases.

You will have 90 minutes to complete the exam. The exam consists of a maximum of 90 questions. If you have prepared, you should find that this is plenty of time to properly pace yourself and review the exam before submission.

Arriving at the Exam Location

As with any examination, arrive at the testing center early (at least 15 minutes). Be prepared! You need to bring two forms of identification (one with a picture). The testing center staff requires proof that you are who you say you are and that someone else is not taking the test for you. Arrive early, because if you are late, you will be barred from entry and will not receive a refund for the cost of the exam.

ExamAlert

You'll be spending a lot of time in the exam room. Plan on using the full 90 minutes allotted for your exam and surveys. Policies differ from location to location regarding bathroom breaks. Check with the testing center before beginning the exam.

In the Testing Center

You will not be allowed to take into the examination room study materials or anything else that could raise suspicion that you're cheating. This includes practice test material, books, exam prep guides, or other test aids. The Testing Center will provide you with scratch paper and a pen or pencil. These days, this often comes in the form of an erasable whiteboard.

Examination results are available after the exam. After submitting the exam, you will be notified whether you have passed or failed. The test administrator will also provide you with a printout of your results.

About This Book

The ideal reader for an *Exam Cram* book is someone seeking certification. However, it should be noted that an *Exam Cram* book is a very easily readable, rapid presentation of facts. Therefore, an *Exam Cram* book is also extremely useful as a quick reference manual.

You can read this book cover to cover, or you may jump across chapters as needed. Because the book chapters align with the exam objectives, some chapters may have overlap on topics. Where required, references to the other chapters are provided for you. If you need to brush up on a topic, you can use the index, table of contents, or Table I.1 to find the topics and go to the questions that you need to study. Beyond helping you prepare for the test, we think you'll find this book useful as a tightly focused reference on some of the most important aspects of the Cloud+ certification.

This book includes other helpful elements in addition to the actual logical, step-by-step learning progression of the chapters themselves. *Exam Cram* books use elements such as ExamAlerts, tips, notes, and practice questions to make information easier to read and absorb. This text also includes a very helpful glossary to assist you.

Note

Reading this book from start to finish is not necessary; this book is set up so that you can quickly jump back and forth to find sections you need to study.

Use the *CramSheet* found in the front of the book to remember last-minute facts immediately before the exam. Use the practice questions to test your knowledge. You can always brush up on specific topics in detail by referring to the table of contents and the index. Even after you achieve certification, you can use this book as a rapid-access reference manual.

Exam Objectives

Table I.1 lists the skills the CV0-003 exam measures and the chapter in which the objective is discussed.

TABLE I.1

Exam Domain	Objective	Chapter in Book That Covers It
1.0 Cloud Architecture and Design	1.1 Compare and contrast the different types of cloud models.	Chapter 1
1.0 Cloud Architecture and Design	1.2 Explain the factors that contribute to capacity planning.	Chapter 2
1.0 Cloud Architecture and Design	1.3 Explain the importance of high availability and scaling in cloud environments.	Chapter 3
1.0 Cloud Architecture and Design	1.4 Given a scenario, analyze the solution design in support of the business requirements.	Chapter 4
2.0 Security	2.1 Given a scenario, configure identity and access management.	Chapter 5
2.0 Security	2.2 Given a scenario, secure a network in a cloud environment.	Chapter 6

Exam Domain	Objective	Chapter in Book That Covers It
2.0 Security	2.3 Given a scenario, apply the appropriate OS and application security controls.	Chapter 7
2.0 Security	2.4 Given a scenario, apply data security and compliance controls in cloud environments.	Chapter 8
2.0 Security	2.5 Given a scenario, implement measures to meet security requirements.	Chapter 9
2.0 Security	2.6 Explain the importance of incident response procedures.	Chapter 10
3.0 Deployment	3.1 Given a scenario, integrate components into a cloud solution.	Chapter 11
3.0 Deployment	3.2 Given a scenario, provision storage in cloud environments.	Chapter 12
3.0 Deployment	3.3 Given a scenario, deploy cloud networking solutions.	Chapter 13
3.0 Deployment	3.4 Given a scenario, configure the appropriate compute sizing for a deployment.	Chapter 14
3.0 Deployment	3.5 Given a scenario, perform cloud migrations.	Chapter 15
4.0 Operations and Support	4.1 Given a scenario, configure logging, monitoring, and alerting to maintain operational status.	Chapter 16
4.0 Operations and Support	4.2 Given a scenario, maintain efficient operation of a cloud environment.	Chapter 17
4.0 Operations and Support	4.3 Given a scenario, optimize cloud environments.	Chapter 18
4.0 Operations and Support	4.4 Given a scenario, apply proper automation and orchestration techniques.	Chapter 19
4.0 Operations and Support	4.5 Given a scenario, perform appropriate backup and restore operations.	Chapter 20
4.0 Operations and Support	4.6 Given a scenario, perform disaster recovery tasks.	Chapter 21
5.0 Troubleshooting	5.1 Given a scenario, use the troubleshooting methodology to resolve cloud-related issues.	Chapter 22
5.0 Troubleshooting	5.2 Given a scenario, troubleshoot security issues.	Chapter 23

Exam Domain	Objective	Chapter in Book That Covers It
5.0 Troubleshooting	5.3 Given a scenario, troubleshoot deployment issues. 5.6 Given a scenario, troubleshoot automation or orchestration issues.	Chapter 24
5.0 Troubleshooting	5.4 Given a scenario, troubleshoot connectivity issues. 5.5 Given a scenario, troubleshoot common performance issues.	Chapter 25

The Chapter Elements

Each *Exam Cram* book has chapters that follow a predefined structure. This structure makes *Exam Cram* books easy to read and provides a familiar format for all *Exam Cram* books. The following elements typically are used:

- Chapter topics
- Essential Terms and Components
- CramSavers
- CramQuizzes
- Notes
- Available exam preparation software practice questions and answers

Note

Bulleted lists, numbered lists, tables, and graphics are also used where appropriate. A picture can paint a thousand words sometimes, and tables can help to associate different elements with each other visually.

Now let's look at each of the elements in detail.

- **Chapter topics**—Each chapter contains details of all subject matter listed in the table of contents for that particular chapter. The objective of an *Exam Cram* book is to cover all the important facts without giving too much detail; it is an exam cram.
- **CramSavers**—Each chapter kicks off with a short-answer quiz to help you assess your knowledge of the chapter topic. This chapter element is designed to help you determine whether you need to read the whole

chapter in detail or merely skim the material and skip ahead to the CramQuiz at the end of the chapter.

- **CramQuizzes**—Each chapter concludes with a multiple-choice quiz to help ensure that you have gained familiarity with the chapter content.
- **ExamAlerts**—ExamAlerts address exam-specific, exam-related information. An ExamAlert addresses content that is particularly important, tricky, or likely to appear on the exam. An ExamAlert looks like this:

ExamAlert

Make sure you remember the different ways in which you can access a router remotely. Know which methods are secure and which are not.

- **Notes**—Notes typically contain useful information that is not directly related to the current topic under consideration. To avoid breaking up the flow of the text, they are set off from the regular text.

Note

This is a note. You have already seen several notes.

Other Book Elements

Most of this *Exam Cram* book on Cloud+ follows the consistent chapter structure already described. However, various important elements are not part of the standard chapter format. These elements apply to the book as a whole.

- **Glossary**—The glossary contains a listing of important terms used in this book with explanations.
- **CramSheet**—The CramSheet is a quick-reference, tear-out cardboard sheet of important facts useful for last-minute preparation. CramSheets often include a simple summary of the facts that are most difficult to remember.
- **Companion website**—The companion website for your book allows you to access several digital assets that come with your book, including
  - Pearson Test Prep software (both online and Windows desktop versions)
  - Key Terms Flash Cards application
  - A PDF version of the CramSheet

To access the book's companion website, simply follow these steps:

1. Register your book by going to: PearsonITCertification.com/register and entering the ISBN: 9780137393251.
2. Respond to the challenge questions.
3. Go to your account page and select the **Registered Products** tab.
4. Click the **Access Bonus Content** link under the product listing.

Pearson Test Prep Practice Test Software

As noted previously, this book comes complete with the Pearson Test Prep practice test software containing two full exams. These practice tests are available to you either online or as an offline Windows application. To access the practice exams that were developed with this book, please see the instructions in the card inserted in the sleeve in the back of the book. This card includes a unique access code that enables you to activate your exams in the Pearson Test Prep software.

Accessing the Pearson Test Prep Software Online

The online version of this software can be used on any device with a browser and connectivity to the Internet, including desktop machines, tablets, and smartphones. To start using your practice exams online, simply follow these steps:

1. Go to http://www.PearsonTestPrep.com.
2. Select **Pearson IT Certification** as your product group.
3. Enter your email/password for your account. If you don't have an account on PearsonITCertification.com or CiscoPress.com, you will need to establish one by going to PearsonITCertification.com/join.
4. In the **My Products** tab, click the **Activate New Product** button.
5. Enter the access code printed on the insert card in the back of your book to activate your product.

6. The product will now be listed in your My Products page. Click the **Exams** button to launch the exam settings screen and start your exam.

Accessing the Pearson Test Prep Software Offline

If you wish to study offline, you can download and install the Windows version of the Pearson Test Prep software. There is a download link for this software on the book's companion website, or you can just enter this link in your browser:

http://www.pearsonitcertification.com/content/downloads/pcpt/engine.zip

To access the book's companion website and the software, simply follow these steps:

1. Register your book by going to PearsonITCertification.com/register and entering the ISBN: 9780137393251.
2. Respond to the challenge questions.
3. Go to your account page and select the **Registered Products** tab.
4. Click the **Access Bonus Content** link under the product listing.
5. Click the **Install Pearson Test Prep Desktop Version** link under the Practice Exams section of the page to download the software.
6. After the software finishes downloading, unzip all the files on your computer.
7. Double-click the application file to start the installation, and follow the on-screen instructions to complete the registration.
8. When the installation is complete, launch the application and select the **Activate Exam** button on the My Products tab.
9. Click the **Activate a Product** button in the Activate Product Wizard.
10. Enter the unique access code found on the card in the sleeve in the back of your book and click the **Activate** button.
11. Click **Next** and then the **Finish** button to download the exam data to your application.
12. You can now start using the practice exams by selecting the product and clicking the **Open Exam** button to open the exam settings screen.

Note that the offline and online versions will synch together, so saved exams and grade results recorded on one version will be available to you on the other as well.

Customizing Your Exams

Once you are in the exam settings screen, you can choose to take exams in one of three modes:

- Study Mode
- Practice Exam Mode
- Flash Card Mode

Study Mode allows you to fully customize your exams and review answers as you are taking the exam. This is typically the mode you would use first to assess your knowledge and identify information gaps. Practice Exam Mode locks certain customization options because it is presenting a realistic exam experience. Use this mode when you are preparing to test your exam readiness. Flash Card Mode strips out the answers and presents you with only the question stem. This mode is great for late stage preparation when you really want to challenge yourself to provide answers without the benefit of seeing multiple-choice options. This mode will not provide the detailed score reports that the other two modes will, so it should not be used if you are trying to identify knowledge gaps.

In addition to these three modes, you will be able to select the source of your questions. You can choose to take exams that cover all of the chapters, or you can narrow your selection to just a single chapter or the chapters that make up specific parts in the book. All chapters are selected by default. If you want to narrow your focus to individual chapters, simply deselect all the chapters and then select only those on which you wish to focus in the Objectives area.

There are several other customizations you can make to your exam from the exam settings screen, such as the time of the exam, the number of questions served up, whether to randomize questions and answers, whether to show the number of correct answers for multiple-answer questions, or whether to serve up only specific types of questions. You can also create custom test banks by selecting only questions that you have marked or questions on which you have added notes.

Updating Your Exams

If you are using the online version of the Pearson Test Prep software, you should always have access to the latest version of the software as well as the exam data. If you are using the Windows desktop version, every time you launch the software, it will check to see if there are any updates to your exam data and automatically download any changes that were made since the last time you used the software. This requires that you are connected to the Internet at the time you launch the software.

Sometimes, due to many factors, the exam data may not fully download when you activate your exam. If you find that figures or exhibits are missing, you may need to manually update your exams.

To update a particular exam you have already activated and downloaded, simply select the **Tools** tab and select the **Update Products** button. Again, this is an issue only with the Windows desktop application.

If you wish to check for updates to the Pearson Test Prep exam engine software, Windows desktop version, simply select the **Tools** tab and select the **Update Application** button. This will ensure you are running the latest version of the software engine.

Contacting the Author

Hopefully, this book provides you with the tools you need to pass the Cloud+ exam. Feedback is appreciated. You can follow and contact the author on LinkedIn: https://www.linkedin.com/in/bo-rothwell/.

CHAPTER 8

Data Security and Compliance Controls in Cloud Environments

This chapter covers the following official CompTIA Cloud+ exam objective:

- ▶ 2.4 Given a scenario, apply data security and compliance controls in cloud environments.

(For more information on the official CompTIA Cloud+ exam topics, see the Introduction.)

In this chapter you will learn about different data security and compliance controls that are available in cloud environments. You will learn about how encryption and integrity affect an organization's data. You will also learn how to secure data by classifying and segmenting the data, as well as controlling access to the data.

Also discussed in this chapter is how laws and regulations impact data security, including the concept of a legal host. Lastly, you will learn about records management, a process in which rules are put in place to determine how long data is maintained and how to properly destroy the data when it is no longer needed.

CramSaver

If you can correctly answer these questions before going through this section, save time by skimming the ExamAlerts in this section and then completing the CramQuiz at the end of the section.

1. Data at rest and data in transit are two forms of data encryption. What is the third?
2. A _____ algorithm is a mathematical function that is applied to data that should return a unique result.

3. True or false: Data classification may be dependent on who can view the data.
4. In relation to data security, data _____ is the process of placing data into different locations based on who should be able to access the data.

Answers

1. Data in use
2. Hashing
3. True
4. Segmentation

Encryption

Encryption is the process of transforming data from its original form to a form that, when viewed, does not reveal the original data. There are three different forms of encryption:

- **Data at rest:** Data is encrypted when it is stored. This method can either be performed by you prior to uploading the data to storage, or in some cases, it can be performed by a function that is provided by the cloud provider. When you perform the data encryption, it is your responsibility to decrypt the data when the original data is needed. When the cloud provider encrypts the data, the decryption process must be performed by the cloud provider.
- **Data in transit:** Data is encrypted before it is sent and decrypted when received. This form of encryption could involve several different techniques, but in most cases for cloud computing environments it means that the data is encrypted by a network device that then sends the data across the network.
- **Data in use:** Data is encrypted when being actively used, which typically means while it is stored in random-access memory (RAM). Because some exploits may make data in RAM vulnerable, this form of encryption may be very important to ensuring data integrity.

Many different technologies can be used to encrypt data, and which technology you use will depend on several factors, including which cloud provider you utilize. These technologies fall into one of two methods of encryption:

- **Symmetric encryption:** With this method you use the same key (a unique value of some sort) to both encrypt and decrypt the data.
- **Asymmetric encryption:** With this method you use a different key to encrypt and decrypt the data. One key is referred to as the *public key*, and the other is called the *private key*. An example of using this encryption method would be if you wanted someone to send data to you across the network. You provide the public key to this person, and this person then encrypts the data. The only way to decrypt the data is to use the private key, which you would never share with anyone else.

Integrity

While data encryption is focused on keeping prying eyes from seeing the original data, data *integrity* is focused on assuring the data is accurate and consistent. Doing so requires ensuring data integrity through all stages of the data lifecycle, which includes transporting, storing, retrieving, and processing data.

Several tools can be used to ensure data integrity, including hashing algorithms, digital signatures, and file integrity monitoring (FIM).

Hashing Algorithms

A *hashing algorithm* is a mathematical function that is applied to data that should return a unique result. Unlike encryption, in which the result of the encryption process is data that could be decrypted back to the original format, hash data is one-way, making it impossible to return the original data. The purpose of a hash isn't to hide or encrypt the data, but rather to ensure that the data you have received matches up with the original.

Consider a situation in which you receive a database with sensitive information. Your organization is going to use this information to help make some critical decisions on future products. You received this data from a trusted third-party source, but how can you be certain that a "bad actor" didn't intercept the data and inject false information?

Your third-party source could use a hashing algorithm and send the resulting hash separately. Then you could take the data that you have received, perform the same hashing algorithm, and then compare the results with the hash from the third-party. If they match, you know you have unaltered data.

There are many different types of hashing algorithms. Each has specific advantages and disadvantages, but for the CompTIA Cloud+ certification exam, you should be familiar with the names of these algorithms:

- MD5
- SHA-1
- SHA-2
- SHA-3
- RIPEMD-160

Digital Signatures

Suppose a friend sends you a letter. How would you know that it really came from that person? One method is to have your friend add a signature to the bottom of the letter. If you recognize the signature, you can be more certain that it came from your friend.

Digital signatures are used in the same way but are a bit more complicated in how they are implemented. Digital signatures make use of asymmetric cryptography in which the signature is encrypted using the private key of an individual or organization. The public key is made well known through another means. The signature that has been encrypted with the private key can only be decrypted by the public key. Successful decryption verifies the data came from the correct source.

File Integrity Monitoring (FIM)

In some cases, it is important to determine if data within a file has changed. The process that handles this determination is called *file integrity monitoring*. With FIM a checksum is created when the file is in a known state called a *baseline*. This checksum is a value that is based on the current contents and, in some cases, additional file attributes, such as the file owner and permissions.

To determine if a file or a file attribute has been changed, you can take another checksum sometime in the future. When you're comparing the original checksum to the new checksum, if they match, the current file is the same as the original. This technique can be used to determine if someone has tampered with a key operating system file or a file that has been downloaded from a remote server.

Classification

Consider how you would treat data that contains credit card information compared to how you would treat data that contains comments that have been made regarding your company website. The data that contains credit card information is much more sensitive than the data that contains customer comments, so you would want to treat the data differently.

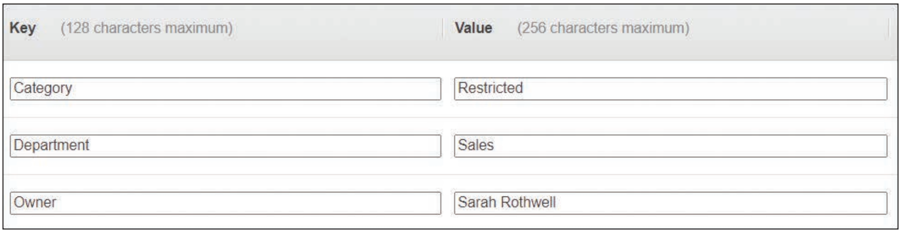
In this situation data classification becomes important. With data classification, you place data into different categories depending on how you want to treat the data. These categories can be based on rules related to how sensitive the data is, who should be able to read the data, who should be able to modify the data, and how long the data should be available. Unless you are storing data that is related to compliance regulations (like SOC 2, GDPR, PCI-DSS, or HIPAA), the data classification criteria are up to you. See the "Impact of Laws and Regulations" section in this chapter for more details on compliance regulations.

For example, you may consider classifying data based on who is permitted to access the data. In this case you may use the following commonly used categories:

- **Public:** This data is available to anyone, including those who are not a part of your organization. This typically includes information found on your public website, announcements made on social media sites, and data found in your company press releases.
- **Internal:** This data should be available only to members of your organization. An example of this data would be upcoming enhancements to a software product that your organization creates.
- **Confidential:** This data should be available only to select individuals who have the need to access this information. This could include personally identifiable information (PII), such as an employee Social Security number. Often the rules for handling this data are also governed by compliance regulations.
- **Restricted:** This data may seem similar to confidential data, but it is normally more related to proprietary information, company secrets, and in some cases, data that is regarded by the government as secret.

In the cloud there are different techniques to handle different types of data. These techniques could include placing different types of data into different storage locations. Chapter 12, "Storage in Cloud Environments," will discuss different storage solutions that are typically found in a cloud environment.

You can also make use of metadata. *Metadata* is data that is associated with the "real data," and it is used to describe or classify the "real data." In cloud environments, metadata is normally created by using a feature called *tags*. Tags are flexible in that you can create a key-value pair that describes components of the data. Figure 8.1 demonstrates applying tags to data in AWS.



Key (128 characters maximum)	**Value** (256 characters maximum)
Category	Restricted
Department	Sales
Owner	Sarah Rothwell

FIGURE 8.1 **AWS Tags**

Segmentation

In relation to data security, data *segmentation* is the process of placing data into different locations based on who should be able to access the data. For example, it would be a good practice to place employee PII in a different location (like a different database) from the data contained in press releases.

Data segmentation may also be a requirement for compliance regulations. For example, a regulation may require that specific data never leave a country. The reason is typically that laws govern the use of this data, and once the data leaves the country, those laws no longer have effect. In this case, data segmentation may be related to the region in which you store the data. See the "Impact of Laws and Regulations" section in this chapter for further details.

Access Control

Access control is the technique that determines who can access a resource. In terms of data access control, accessing the resource can include viewing, modifying, and destroying the data.

In most cloud environments, the definition of "who" can include both people and other resources. For example, you may have a payroll application that needs to access secure data about employees that is stored in a database. There must be access control rules in place that permit or block access for both people and resources.

People are given user accounts to access cloud resources. These user accounts are granted access to resources by using permissions.

Applications are assigned to roles, which are similar to user accounts in that permissions can be applied to roles just as they are applied to user accounts. However, applications can never be assigned to user accounts (in some cases a user may be assigned to a role, depending on the cloud environment that you are working in).

To learn more about how user accounts and roles impact access to resources, see Chapter 5, "Identity and Access Management."

Impact of Laws and Regulations

As previously mentioned, many laws and regulations govern how data is treated in an organization. They will vary depending on where your data is located. For example, the laws that govern data in the United States are different from the laws that govern data in the European Union (EU).

The laws and rules are numerous and vary based on the industry of your organization. For example, if your company is a retailer and you accept credit card payments, you will likely need to follow PCI Security Standards when dealing with credit card data. If your organization is a hospital, you will need to follow HIPAA regulations when dealing with patient data.

For the certification exam, it likely is not worthwhile to memorize a bunch of laws and regulations. Many organizations have full-time staff devoted to ensuring these laws are followed. Being aware of the impact of these laws is most critical for the exam.

Legal Hold

Organizations cannot just delete information whenever they want. Some information, such as employee records, must be maintained for specific periods of time in the event of investigations or litigation. The term *legal hold* is used by an organization's legal department to indicate how long specific data must be stored and how it should be made available in the event it is needed.

Records Management

Organizations often end up creating, gathering, and accumulating a lot of data. The volumes of information stored by an organization can result in high costs because storing data is not free. While cloud vendors provide many ways of storing data, they will charge to store data, so organizations typically do not want to keep data for longer than necessary.

Records management is the process of determining how and for how long to store data. This large topic includes data classification and encryption, as well as versioning, retention policies, and destruction policies.

Versioning

Versioning is the process of keeping track of file content changes over time. Many cloud technologies provide versioning as a feature that can be enabled, so the versioning happens automatically whenever a data record is changed.

Retention

Retention refers to a policy that determines how long data should be stored. A retention schedule is created that will determine when data is destroyed and how older data is stored until it is to be destroyed.

Destruction

The destruction of data must be clearly defined when developing a records management plan. When the data is to be destroyed is one key element to define, but also how the data is to be destroyed should be clearly stated in the plan. Data can be destroyed by physical destruction of records, degaussing, or zeroizing.

Write Once Read Many

Write once read many, also referred to as WORM, is a form of write protection in which the data can be written only once and then it cannot be modified. This is a critical feature when you need to ensure that data has not been tampered with after it was created.

Data Loss Prevention (DLP)

Data loss prevention is the process of ensuring that sensitive data is not misused, accessed, or lost. It is designed to prevent a data breach that may include accessing, modifying, or destroying data. In some cases, the DLP process must be clearly defined because the data is regulated by laws and regulations. In other cases, the DLP may be the result of wanting to keep classified information secure.

Some cloud providers will include DLP as a software tool. For example, Google Cloud has a product called Cloud DLP, which enables you to view how data is stored and processed, configure data inspection and monitoring, and reduce the risk of data loss. In other cases, the features of DLP may be associated with a specific data-based product. For example, there are techniques that you can use for DLP when storing data in AWS S3 buckets.

Cloud Access Security Broker (CASB)

CASB is a software tool that can be located either on-premises or in the cloud. It is designed to provide an interface between cloud resources (applications) and cloud users. It monitors access to cloud resources including data, issues warnings when a cloud resource may have been compromised, and enforces security policies.

CASBs also provide the means to perform audits, so access to data resources in the past can be analyzed. They are also often used for compliance reporting because they provide insights to data access over time.

CramQuiz

Answer these questions. The answers follow the last question. If you cannot answer these questions correctly, consider reading this section again until you can.

1. Which is not a form of data encryption?

❍ **A.** Data in use

❍ **B.** Data at rest

❍ **C.** Data in transit

❍ **D.** Data in the cloud

2. With this method you use a key (a unique value of some sort) to both encrypt and decrypt the data.

   ❍ **A.** Antisymmetric encryption

   ❍ **B.** Asymmetric encryption

   ❍ **C.** Symmetric encryption

   ❍ **D.** None of these answers are correct

3. Digital signatures make use of _____ cryptography in which the signature is encrypted using the private key of an individual or organization.

   ❍ **A.** Asymmetric

   ❍ **B.** Symmetric

   ❍ **C.** Antisymmetric

   ❍ **D.** Hashing

4. With ____ a checksum is created when the file is in a known state called a baseline.

   ❍ **A.** Digital signatures

   ❍ **B.** Hashing algorithms

   ❍ **C.** File integrity monitoring

   ❍ **D.** Data classification

5. The term _____ is used by an organization's legal department to indicate how long specific data must be stored and how it should be made available in the event it is needed.

   ❍ **A.** Records management

   ❍ **B.** Retention

   ❍ **C.** WORM

   ❍ **D.** Legal hold

CramQuiz Answers

1. Data in the cloud
2. Symmetric encryption
3. Asymmetric
4. File integrity monitoring
5. Legal hold

What Next?

If you want more practice on this chapter's exam objectives before you move on, remember that you can access all of the CramQuiz questions on the companion website. You can also create a custom exam by objectives with the practice exam software. Note any objectives you struggle with and go to that objective's material in this chapter.

Index

Numbers

3–2-1 rule, 269

A

access logs, 208–209

access management, 56

- ACL
  - cloud-to-cloud migrations, 197–198
  - NACL, 318
  - troubleshooting, 318–319
- CASB, 111
- certificate management, 63–64
- DAC, 59–60
- data access control, 108–109
- directory services, 60
- FID, 61–63
- groups, 57
- LAM, 57–58
- LDAP, 61
- life-cycle management, 58
- MAC, 60, 99–100
- MFA, 64–65
- NAC, 60, 79–80
- NACL, security groups versus, 318
- PAM, 57
- PKI, 66–67
- role-based access control, 59
- roles, 57
- SSO, 65–66
- user accounts, 56–57

accounts

- creating, 58
- deactivating, 58
- default accounts, deactivating, 120
- deleting, 58
- life-cycle management, 58
- lockout policies, 89

mismatches, 310
missing accounts/roles, 290
provisionng/deprovisioning, 58
service accounts, automation, 255
troubleshooting
mismatches, 310
missing accounts/roles, 290
updating, 58
user accounts, 56–57
certificate management, 63–64
DAC, 59–60
directory services, 60
FID, 61–63
groups, 57
LAM, 57–58
LDAP, 61
life-cycle management, 58
MAC, 60, 99–100
MFA, 64–65
NAC, 60
PAM, 57
PKI, 66–67
role-based access control, 59
roles, 57
SSO, 65–66
ACL (Access Control Lists)
cloud-to-cloud migrations, 197–198
NACL
inheritance, 319
security groups versus, 318
troubleshooting, 318–319
action plans, troubleshooting methodologies, 285–286
actions/findings/outcomes (troubleshooting), documenting, 286
active-passive upgrades, 227
advanced cloud services, 9
AI, 10–11
IoT, 9
machine learning, 11
serverless applications, 9–10
affinity, 27
agent-based scans, 118
AI (Artificial Intelligence), 10–11
alarms, 229
alerting, 214, 229
categorizing alerts, 215
common messaging methods, 214
communicating alerts, 215
enabling/disabling, 214
responding to alerts, 214–215
algorithms, hashing, 105–106
allocations, dynamic
CPU, 185
memory, 189
alternate location restorations, 270
analysis
capacity planning
business need analysis, 17–18
trend analysis, 21
logging analysis tools, 207
packet analyzers, 335–336
requirement analysis, solution design, 42
root cause analysis, 132, 274
analysis phase, vulnerability assessments, 117
anomalies, capacity planning, 22
anti-affinity, 27–28
antimalware, 93–94
antivirus software, 93–94
APC (Application Delivery Controller), 79
API (Application Programming Interface)
endpoints, 98
internal API, automation, 254
troubleshooting
request limits, 308–309
version incompatibility, 314
APM (Application Performance Monitoring), 212
appliances, virtual patches, 223
application logs, 209
applications
backups, 263

- broken/critical infrastructures/applications, fixes, 222
- encryption, 98
- HA, 32
- patches, 223–224
- provisioning resources, 142–143
- security
  - account lockout policies, 89
  - antimalware, 93–94
  - antivirus software, 93–94
  - builds, 96–97
  - EDR, 93–94
  - encryption, 98
  - hardened baselines, 94–95
  - HIDS, 94
  - HIPS, 94
  - password complexity policies, 88–89
  - single function methodology, 95
  - software feature policies, 90
  - user permissions policies, 90–93
  - user/group policies, 90
  - whitelisting, 89
- serverless applications, 9–10
- troubleshooting, 337
  - memory management, 337
  - service overloads, 337

architectures, database migrations, 200

arp command, 332–333

assessing
- risk, 117
- vulnerabilities, 117

asset management, 220–221

asymmetric encryption, 105

attacks, security
- external attacks, 298
- internal attacks, 299

audits, logging, 208

authentication
- logs, 208–209
- MFA, MFA, 64–65
- troubleshooting, 291–292

authoritative name servers, DNS, 169

authorization, 56
- certificate management, 63–64
- DAC, 59–60
- directory services, 60
- FID, 61–63
- groups, 57
- LAM, 57–58
- LDAP, 61
- life-cycle management, 58
- MAC, 60, 99–100
- MFA, 64–65
- NAC, 60
- PAM, 57
- PKI, 66–67
- role-based access control, 59
- roles, 57
- SSO, 65–66
- troubleshooting, 292–293
- user accounts, 56–57

automation, 252–253
- CD, 250
- CI, 250
- configuration management, 251–252
- continuous delivery, 250
- IaC, 248
  - declarative IaC, 249
  - imperative IaC, 249
  - orchestration sequencing, 255–256
- internal API, 254
- logging, 209
- passwords
  - hardcoded passwords, 255
  - vaults, 255
- routine operations, 253
- secure scripting, 254
- service accounts, 255
- shutdowns, 254
- troubleshooting
  - API version incompatibility, 314
  - deprecated features, 313–314
  - job validation, 314–315
  - patch failures, 315
  - tool incompatibility, 313

updates, 253
version control, 250–251
auto-scaling, 36–37
availability, resources, 212
availability zones, 31
AWS (Amazon Web Services)
Cloudwatch dashboard, 228
database instance bandwidth, 237–238
EC2 instances, 44–45
HDD storage options, 153
health dashboards, 232–233
instances, 144
metadata, 108
SDD storage options, 153–154
Service Health dashboard, 302–303
Azure Regions, Microsoft, 30–31

B

backporting, 219
backups, 260, 266
3–2-1 rule, 269
application-level backups, 263
configuration files, 263–264
confirming completions, 218
data objects, 263
database dumps, 264
differential backups, 261
disk backups, 265–266
file-system backups, 263–264
full backups, 261
incremental backups, 260
locations, 267
MTTR, 269
object-based backups, 266
retention policies, 266–267
RPO, 268, 275
RTO, 268
scheduling, 267
SLA, 268
snapshots, 262–263
synthetic full backups, 262
tape backups, 265
targets, 265
balancers, load, 176–177
geographic-based load balancing, 35
HA, 34–35
network optimization, 239
round robin load balancing, 35
weighted load balancing, 35
ballooning memory, 189
bandwidth
AWS database instance bandwidth, 237–238
network optimization, 237–239
storage migrations, 198
bare metal hypervisors. *See* Type 1 hypervisors
baselines
capacity planning, 21
hardened baselines, 94–95
monitoring, 210
beta builds, 96
billing issues, troubleshooting, 309–310
binary numeric values, IPv4 addresses, 172–173
blacklisting, 82
block storage, 141
migrations, 199
SAN, 150
blue-green deployments, business-based design solutions, 49
branches, version control, 251
breaches, data, 296
broken/critical infrastructures/applications, fixes, 222
buckets, object storage, 151
budgets
capacity planning, 17
requirements, business-based design solutions, 45–46
bug fixes, 222
builds, 96
beta builds, 96
canary builds, 97
LTS builds, 97

stable builds, 96

business need analysis, capacity planning, 17–18

business-based design solutions

blue-green deployments, 49
budgetary requirements, 45–46
compliance, 46
development environments, 48
DR environments, 49–50
functional testing, 51
hardware, 43–45
integration, 45
network requirements, 47–48
penetration testing, 50–51
performance testing, 51
production environments, 49
QA environments, 48
regression testing, 51
requirement analysis, 42
routing, 48
security, 46–47
SLA, 46
software, 42–43
staging environments, 49
subnetting, 47
usability testing, 51–52
user needs, 46
vulnerability testing, 50

C

CA (Certificate Authorities), 63–64, 66

caching, DNS

name servers, 169
poisoning, 74

call trees, incident response, 125

canary builds, 97

capacities

monitoring, 232
planning, 15, 16
anomalies, 22
baselines, 21
budgetary requirements, 17
business need analysis, 17–18
GPU, 16
hardware requirements, 16–17
licensing, 18–20
network performance, 17
patterns, 22
performance, 22–23
RAM, 16
software requirements, 17
storage, 16
system load, 21
templates, 18
trend analysis, 21
troubleshooting, 307
user density, 20
vCPU, 16

capex (capital expense), 4

CASB (Cloud Access Security Broker), 111

categorizing alerts, 215

causes (troubleshooting), testing, 285

CD (Continuous Deployment), 250

CDN (Content Delivery Networks), 169–170

certificates, digital, 66

CRL, 67
CSR, 67
managing, 63–64
troubleshooting, 294
compromised certificates, 295
expired certificates, 294
misconfigured certificates, 295
revoked certificates, 295
trusted certificates, 295

chain of custody documents, incident response containment procedures, 132

changes

implementation, corporate policies/procedures, 282–283
management, troubleshooting, 310–311
feature/version mismatches, 312

locations, 312
server name changes, 311
chargebacks, 230
checkouts, version control, 251
chmod command, 92–93
CI (Continuous Integration), 250
CIFS (Common Internet File Systems), 155
ciphers
disabling, 81–82
security, 297
Class C networks, 174–175
classes, databases, 29
classifying data, 107
confidential data, 107
internal data, 107
metadata, 108
public data, 107
restricted data, 107
client/server interactions, NTP, 167
clock speeds, virtualization, 187–188
clones, version control, 251
closed source vendor software, 245
cloud bursting, 37–38
cloud computer resources, 141
cloud resources, cloud deployments
IaaS, 140
PaaS, 140
SaaS, 140
cloud service models, 6–7
advanced cloud services, 9–11
AI, 10–11
IaaS, 7
business-based design solutions, 43
cloud deployments, 140
IoT, 9
machine learning, 11
PaaS, 8
business-based design solutions, 43
cloud deployments, 140
cloud-to-cloud migrations, 196–198
SaaS, 8
business-based design solutions, 43
cloud deployments, 140
serverless applications, 9–10
shared responsibility models, 11–12
"clouds within clouds", 5
cloud-to-cloud migrations, 196
ACL, 197–198
firewalls, 198
PaaS, 196–198
proprietary lock-in migrations, 196
vendor lock-in migrations, 196
Cloudwatch dashboard, AWS, 228
clusters, 33. *See also* instances
HA, 242
redundancy, 242
resiliency, 243
resource placement, 242–243
CMDB (Configuration Management Database), 221
cold standby sites, 276–277
collaboration services, cloud deployments, 138
collectors, 206
SNMP, 206, 207
Syslog, 206–207
colocation, network optimization, 243
columnar databases, 201
common messaging methods, 214
communications
alerts, 215
cloud deployments, 137
email services, 138
messaging services, 138
VoIP, 137
community clouds, 5
compiling code, 245
completing backups, confirming, 218
complexity, passwords, 88–89
compliance
business-based design solutions, 46
control
access control, 108–109

CASB, 111
data classification, 107–108
data destruction, 110
data integrity, 105
data retention, 110
data segmentation, 108
digital signatures, 106
DLP, 111
encryption, 104–105
FIM, 106
hashing algorithms, 105–106
laws/regulations, 109
legal holds, 109
records management, 110
versioning, 110
WORM, 110

compression, storage systems, 160

compromised keys/certificates, troubleshooting, 295

compute power, oversubscription, 28–29

compute resources, 141

confidential data, 107

configuration files, backups, 263–264

configurations
management, 251–252
security, 81, 82
ciphers, disabling, 81–82
firmware, upgrading, 82
unnecessary ports/services, disabling, 81
weak protocols, disabling, 81–82
troubleshooting, 305–306, 319–320

confirming backup completions, 218

connectivity
monitoring, 231
troubleshooting, 302
capacity planning, 307
CSP outages, 302–304
ISP outages, 304
latency, 304–305
licensing, 307
metadata tags, 306–307
performance degradation, 304
scripts, 305–306

containers, 32, 145. *See also* instances

containment procedures, incident response, 131
chain of custody documents, 132
evidence acquisition, 132
isolation, 132

continuous delivery, 226–227, 250

continuous monitoring, verifying, 213

core-based licenses, 19–20

corporate policies/procedures
change implementation, 282–283
disaster recovery, 277

costs
database migrations, 200
operating costs, 229–230
chargebacks, 229–230
showbacks, 230
savings, storage system features, 159
storage migrations, 199
troubleshooting, 309–310

CPU (Central Processing Units), 185–186
clock speeds, 187–188
IPC, 188
sockets, socket-based licenses, 19

credential scans, 117–118

credentialed scans, 118

critical/broken infrastructures/ applications, 222

CRL (Certificate Revocation Lists), 67

CSP (Cloud Service Providers), troubleshooting, 302–304

CSR (Certificate Signing Requests), 67

curl command, 333–334

current versions, lifecycle management, 219

customizing, templates, 145

D

DAC (Discretionary Access Control), 59–60

daemons, 154–155

DAS (Direct-Attached Storage), 188
dashboards, 228–229
- capacity, 232
- connectivity, 231
- health dashboards, 232–233
- incidents, 232
- latency, 231
- overall utilization, 233
- Service Health dashboard, AWS, 302–303

data at rest, 104
data centers, disaster recovery requirements, 279
data deduplication, storage systems, 160
data in transit, 104
data in use, 104
data integrity, 105, 198
data objects, backups, 263
data replication, storage systems, 161
data security, breaches, 296
database instance bandwidth, AWS, 237–238
databases
- classes, 29
- columnar databases, 201
- document databases, 201
- dumps, 264
- graph databases, 201
- instances, 29–30
- key-value databases, 201
- migrations, 200
- nonrelational databases, migrations, 201–202
- RDBMS, 264
- relational databases, migrations, 201

DDoS (Distributed Denial-of-Service), security, 84–85
deactivating
- accounts, 58
- default accounts, 120

declarative IaC, 249
dedicated hosting, public clouds, 4
deduplication, storage systems, 160
default accounts, deactivating, 120
default routing, troubleshooting, 321
degrading performance, troubleshooting, 304
delays
- processing delays, 240
- queuing delays, 240
- transmission delays, 240

deleting accounts, 58
density, user, 20
deployments
- blue-green deployments, business-based design solutions, 49
- CD, 250
- cloud resources
  - IaaS, 140
  - PaaS, 140
  - SaaS, 140
- collaboration services, 138
- communications, 137
  - email services, 138
  - messaging services, 138
  - VoIP, 137
- file subscriptions, 137
- models, 2–3
  - “clouds within clouds”, 5
  - community clouds, 5
  - hybrid clouds, 4–5
  - multiclouds, 6
  - private clouds, 4
  - public clouds, 3–4
  - VPC, 5
- provisioning resources, 140–141
  - application resources, 142–143
  - compute resources, 141
  - network resources, 142
  - storage resources, 141–142
- sizing, virtualization, 182
  - clock speeds, 187–188
  - dynamic allocations, 185, 189
  - GPU, 186–187

guest OS, 183
HCI, 188
hypervisors, 182–184
IPC, 188
memory, 188–189
SMT, 184
vCPU, 185–186
subscription services, 136–137
VDI, 138–139
VM, 143
containers, 145
instances, 143
persistent storage, 146
postdeployment validation, 146
templates, 143–144
variables, template customization, 145

deprecations
features, troubleshooting, 313–314
lifecycle management, 220

deprovisioning accounts, 58

design solutions, business-based
blue-green deployments, 49
budgetary requirements, 45–46
compliance, 46
development environments, 48
DR environments, 49–50
functional testing, 51
hardware, 43–45
integration, 45
network requirements, 47–48
penetration testing, 50–51
performance testing, 51
production environments, 49
QA environments, 48
regression testing, 51
requirement analysis, 42
routing, 48
security, 46–47
SLA, 46
software, 42–43
staging environments, 49
subnetting, 47
usability testing, 51–52
user needs, 46
vulnerability testing, 50

desktops, VDI, 138–139

destroying data, 110

development environments
business-based design solutions, 48
upgrading, 227

device drivers
generic device drivers, 244
network optimization, 244–245
vendor device drivers, 244–245

DHCP (Dynamic Host Configuration Protocol), 166

differential backups, 261

dig command, 329–330

digital certificates, 66
CRL, 67
CSR, 67

digital signatures, 106

directly connected networks, latency, 240

directory security groups, 294

directory services, 60–61

disabling
alerts, 214
ciphers, 81–82
ports, 81
protocols, 81–82
services, 81

disaster recovery
cold standby sites, 276–277
corporate guidelines, 277
documentation, 277
DR kits, 278
failbacks, 274
failovers, 274
geographical data center requirements, 279
hot standby sites, 275–276
network diagrams, 278
playbooks, 278

redundant resources, 275
RPO, 275
warm sites, 276

disk backups, 265–266

DLP (Data Loss Prevention), 79, 111, 159

DNAT (Destination NAT), 323

DNS (Domain Name Service), 60, 74, 167–168
authoritative name servers, 169
cache poisoning, 74
caching name servers, 169
dig command, 329–330
domain names, 168
flushdns command, 326
forwarder, 169
FQDN, 168
hosts, 168
lookups
forward lookups, 169
reverse lookups, 169
name servers, 168–169
authoritative name servers, 169
caching name servers, 169
nslookup command, 328–329
records, 169
spoofing, 74
subdomains, 168
top-level domains, 168
TTL, 169
zone files, 168–169

DNSSEC (DNS Security), 74–75

document databases, 201

documentation
chain of custody documents, incident response containment procedures, 132
disaster recovery, 277
findings/actions/outcomes, troubleshooting, 286
incident response plans, 124–125
incident types/categories, 127–128

DoH (DNS over HTTPS), 74

domain names, DNS, 168

DoT (DNS over TLS), 74

DR (Disaster Recovery)
business-based design solutions, 49–50
DR kits, 278
upgrading, 228

dynamic allocations
CPU, 185
memory, 189

dynamic routing, 172, 322

E

EC2 instances, AWS, 44–45

edge computing, network optimization, 241–242

EDR (Endpoint Detection and Response), 93–94

egress/ingress traffic control, 82
blacklisting, 82
proxy servers, 82–84
whitelisting, 82, 89

elasticity, 36–37, 231. *See also* scalability

email services, cloud deployments, 138

enabling/disabling, alerts, 214

encryption, 75
API endpoints, 98
applications, 98
asymmetric encryption, 105
data, 104–105
filesystems, 99
HTTPS, 74, 76
IPsec, 75
MAC, 60
OS, 98
protocols, 296–297
storage, 98
symmetric encryption, 105
TLS, 76

end of life, lifecycle management, 220

endpoints
API endpoints, 98
EDR, 93–94
security, 297–298
VPC, 178

environments, 48
- blue-green deployments, 49
- development environments, 48
- DR environments, 49–50
- production environments, 49
- QA environments, 48
- staging environments, 49

eradication procedures, incident response, 131

error codes, REST, 292–293

escalating privileges, troubleshooting, 291

ethical hacking. *See* penetration testing

evidence acquisition, incident response containment procedures, 132

expired keys/certificates, troubleshooting, 294

exposed endpoints, 297–298

external attacks, security, 298

F

failbacks, 274

failovers, 274

failure, single points of, 36

FC (Fibre Channel), 156

feature policies, software, 90

features roadmaps, 218

feature/version mismatches, troubleshooting, 312

FID (Federation Identity Management), 61–63

file searches, NTP, 167

file storage, 141
- migrations, 199
- NAS, 151

file subscriptions, 137

file-system backups, 263–264

filesystems
- CIFS, 155
- encryption, 99
- mounting, 154–155
- NFS, 154–155

FIM (File Integrity Monitoring), 106

findings/actions/outcomes (troubleshooting), documenting, 286

firewalls, 100, 177
- APC, 79
- cloud-to-cloud migrations, 198
- HA, 35–36
- stateful firewalls, 78
- stateless firewalls, 78
- troubleshooting, 322
- WAF, 78

firmware
- generic firmware, 244
- network optimization, 244–245
- patches, 224
- upgrading, 82
- vendor firmware, 244–245

fixes
- bug fixes, 222
- hot fixes, 119, 120

Flash storage, 152

flows, networks, 80

flushdns command, 326

forward lookups, DNS, 169

forward proxies, 83

forwarder, DNS, 169

forwarding ports, 76

FQDN (Fully Qualified Domain Names), 168

full backups, 261

full system functionality (troubleshooting), verifying, 286

fully automated P2V migrations, 194–195

functional testing, business-based design solutions, 51

functions, single function methodology, 95

G

gateways, VPC, 178

generic device drivers/firmware, network optimization, 244

GENEVE, 73

geographic locations, resource placement, 242
geographical data centers, disaster recovery requirements, 279
geographic-based load balancing, 35
GPU (Graphics Processing Units)
- capacity planning, 16
- pass-through GPU, 186–187
- virtual GPU, 186
- virtualization, 186

graph databases, 201
GRE (Generic Routing Encapsulation), 77
groups
- directory security groups, 294
- identity/access management, 57
- NSG, 293–294
- security groups versus, NACL versus, 318
- user/group policies, 90

guest OS, 183
guidelines, disaster recovery, 277

H

HA (High Availability), 25
- affinity, 27
- anti-affinity, 27–28
- applications, 32
- clusters, 33, 242
- containers, 32
- firewalls, 35–36
- hypervisors, 26–27
- load balancers, 34–35
- oversubscription, 28
  - compute power, 28–29
  - monitoring hardware, 30
  - networks, 28–29
  - storage, 30
- regions, 30–31
- routers, 33–34
- single points of failure, 36
- switches, 33
- zones, 31

hacking, ethical hacking. *See* penetration testing
hardcoded passwords, 255
hardened baselines, 94–95
hardening networks, 81
- ciphers, disabling, 81–82
- firmware, upgrading, 82
- unnecessary ports/services, disabling, 81
- weak protocols, disabling, 81–82

hardware
- business-based design solutions, 43–45
- capacity planning, 16–17
- instances, 43–45
- monitoring, oversubscription, 30

hashing algorithms, 105–106
HCI (Hyperconverged Infrastructures), virtualization, 188
HDD (Hard Disk Drives), 152, 153
health dashboards, 232–233
HIDS (Host-Based IDS), 94
HIPS (Host-based IPS), 94
holds, legal, 109
horizontal scaling, 37
hosts, DNS, 168
hot fixes, 119, 120
hot standby sites, disaster recovery, 275–276
HTTPS (HTTP Secure), 74, 76
hub-and-spoke VPC, 178
hybrid clouds, 4–5
hybrid storage, 152
hyperconverged, 188
hyperjacking, 183
hypervisors, 26–27, 182
- bare metal hypervisors. *See* Type 1 hypervisors
- patches, 222
- Type 1 hypervisors, 183
- Type 2 hypervisors, 183–184
- Type 3 hypervisors, 184

I

IaaS (Infrastructure as a Service), 7
- business-based design solutions, 43
- cloud deployments, 140

IaC (Infrastructure as Code), 248
- declarative IaC, 249
- imperative IaC, 249
- orchestration sequencing, 255–256

identification phase, vulnerability assessments, 117

identification procedures, incident response, 130
- investigation phase, 131
- scope of incidents, 131

identifying problems, troubleshooting methodologies, 283–284

identity management, 56
- certificate management, 63–64
- DAC, 59–60
- directory services, 60
- FID, 61–63
- groups, 57
- LAM, 57–58
- LDAP, 61
- life-cycle management, 58
- MAC, 60, 99–100
- MFA, 64–65
- NAC, 60
- PAM, 57
- PKI, 66–67
- role-based access control, 59
- roles, 57
- SSO, 65–66
- user accounts, 56–57

IDS (Intrusion Detection Systems), HIDS, 94

ifconfig/ipconfig command, 326–327

imperative IaC, 249

incident response, 123
- call trees, 125
- containment procedures, 131
  - chain of custody documents, 132
  - evidence acquisition, 132
  - isolation, 132
- documentation, 124–125
- eradication procedures, 131
- identification procedures, 130–131
  - investigation phase, 131
  - scope of incidents, 131
- incident types/categories, documentation, 127–128
- postmortems/lessons learned, 132
- preparation, 124
- RACI matrix, 129
- recovery procedures, 131
- roles/responsibilities, 128–129
- root cause analysis, 132
- tabletops, 126
- training, 126

incident types/categories, documentation, 127–128

incidents, dashboards, 232

incomplete privileges, troubleshooting, 290

incremental backups, 260

infrastructure components, performance monitoring, 212

ingress/egress traffic control, 82
- blacklisting, 82
- proxy servers, 82–84
- whitelisting, 82, 89

inheritance, NACL, 319

initiators, iSCSI, 156

in-place restorations, 269

insecure ciphers, 297

instances, 7, 143. *See also* clusters; containers
- AWS instances, 144
- databases, 29–30
- EC2 instances, AWS, 44–45
- hardware instances, 43–45
- orchestration sequencing, 255–256

integration
- business-based design solutions, 45
- CI, 250

integrity, data, 105, 198

internal API, automation, 254

internal attacks, security, 299

internal data, 107

Internet gateways, VPC, 178

invalid certificate warnings, 63

investigation phase, identification procedures, 131

IOPS (Input/Output Operations Per Second), 153–154

IoT (Internet of Things), 9

IP addresses, troubleshooting, 320–321

ip command, 327–328, 332

IP spaces, troubleshooting, 320–321

IPAM (IP Address Management), 170

IPC (Instructions Per Cycle), virtualization, 188

ipconfig command, 326–327

IPS (Intrusion Protection Systems), HIPS, 94

IPsec (IP Security), 75, 171

IPv4 addresses
- binary numeric values, 172–173
- classes, 173

iSCSI (Internet Small Computer System Interface), 155–156

isolation, incident response containment procedures, 132

ISP (Internet Service Providers), troubleshooting, 304

ITSM (Information Technology Service Management), 213

J

jitter, latency, 305

job validation, troubleshooting, 314–315

JSON (JavaScript Object Notation), templates, 18

jumbo packets, NIC, 239

K

key management
- private keys, 66
- public keys, 66
- troubleshooting, 294
  - compromised keys, 295
  - expired keys, 294
  - misconfigured keys, 295
  - revoked keys, 295

key-value databases, 201

L

L2TP (Layer 2 Tunneling Protocol), 77

LAM (Local Access Management), 57–58

latency, 231
- directly connected networks, 240
- jitter, 305
- MPLS, 240
- network optimization, 240–241
- networks, troubleshooting, 304–305
- processing delays, 240
- queuing delays, 240
- round-trip times, 304–305
- server response times, 305
- transmission delays, 240

laws/regulations
- data security, 109
- database migrations, 200

LDAP (Lightweight Directory Access Control), 61

learning models, 11

legal holds, 109

lessons learned/postmortems, incident response, 132

licensing, 18–19
- core-based licenses, 19–20
- per-user licenses, 19
- socket-based licenses, 19
- subscriptions, 20
- troubleshooting, 307
- volume-based licenses, 19

life-cycle management, accounts, 58

lifecycle management
- backporting, 219
- current versions, 219
- deprecations, 220
- end of life, 220
- new versions, 219
- old versions, 219

roadmaps, 218–219
systems
migrations, 219–220
upgrading, 219–220
versioning, 219
load balancers, 176–177
geographic-based load balancing, 35
HA, 34–35
network optimization, 239
round robin load balancing, 35
weighted load balancing, 35
locations, changes, troubleshooting, 312
lockout policies, accounts, 89
log files, NTP, 166
logging
access logs, 208–209
analysis tools, 207
application logs, 209
audits, 208
authentication logs, 208–209
automation, 209
collectors, 206
SNMP, 206, 207
Syslog, 206–207
scrubbing, 211
severity categorization, 207–208
system logs, 209
trails, 208
trending, 209
types (overview), 208
logins, FID, 61–63
logs, 229
long-term storage, 152–153
lookups, DNS
forward lookups, 169
reverse lookups, 169
LTS (Long-Term Support) builds, 97

M

MAC (Mandatory Access Control), 60, 99–100
machine learning, 11
magnetic drives, 152
malware, antimalware, 93–94
managing
access, 56
ACL, cloud-to-cloud migrations, 197–198
ACL, troubleshooting, 318–319
CASB, 111
certificate management, 63–64
DAC, 59–60
data access control, 108–109
directory services, 60
FID, 61–63
groups, 57
LAM, 57–58
LDAP, 61
life-cycle management, 58
MAC, 60, 99–100
MFA, 64–65
NAC, 60
NACL versus security groups, 318
PAM, 57
PKI, 66–67
role-based access control, 59
roles, 57
SSO, 65–66
user accounts, 56–57
assets, 220–221
CMDB, 221
certificates, 63–64
change
feature/version mismatches, 312
location changes, 312
server names, 311
troubleshooting, 310–312
configurations, 251–252
playbooks, 252
identity, 56
certificate management, 63–64
DAC, 59–60
directory services, 60
FID, 61–63

    - groups, 57
    - LAM, 57–58
    - LDAP, 61
    - life-cycle management, 58
    - MAC, 60, 99–100
    - MFA, 64–65
    - NAC, 60
    - PAM, 57
    - PKI, 66–67
    - role-based access control, 59
    - roles, 57
    - SSO, 65–66
    - user accounts, 56–57
- IPAM, 170
- keys
    - compromised keys, 295
    - expired keys, 294
    - misconfigured keys, 295
    - private keys, 66
    - public keys, 66
    - troubleshooting, 294–295
- life-cycle management, accounts, 58
- lifecycles
    - backporting, 219
    - current versions, 219
    - deprecations, 220
    - end of life, 220
    - new versions, 219
    - old versions, 219
    - roadmaps, 218–219
    - systems, migrations, 219–220
    - systems, upgrading, 219–220
    - versioning, 219
- memory, 337
- records, 110
    - destroying data, 110
    - DNS, 169
    - retention, 110
    - versioning, 110
- secret management, 67
- services, 213

manual P2V migrations, 194

MASQUERADE, 323

memory

- ballooning, 189
- dynamic allocations, 189
- managing, 337
- RAM, capacity planning, 16
- troubleshooting, 337
- virtualization, 188–189

merges, version control, 251

messaging, common methods, 214

messaging services, cloud deployments, 138

metadata, 108, 306–307

metrics, reporting, 229

MFA (Multifactor Authentication), 64–65

microsegmentation, 73

Microsoft Azure Regions, 30–31

migrations

- cloud-to-cloud migrations, 196
    - ACL, 197–198
    - firewalls, 198
    - PaaS, 196–198
    - proprietary lock-in migrations, 196
    - vendor lock-in migrations, 196
- databases, 200
- P2V, 194
    - fully automated migrations, 194–195
    - manual migrations, 194
    - semi-automated migrations, 194
- storage migrations, 198
    - bandwidth, 198
    - block storage, 199
    - cost, 199
    - data integrity, 198
    - databases, nonrelational, 201–202
    - databases, relational, 201
    - file storage, 199
    - monitoring, 198
    - object storage, 200
    - security, 198
- systems, 219–220
- V2V migrations, 195

vendor lock-in migrations, 196
vendor migrations, troubleshooting, 308
mirroring, 158
misconfigured keys/certificates, troubleshooting, 295
missing accounts/roles, troubleshooting, 290
monitoring, 209–210
baselines, 210
capacity, 232
connectivity, 231
continuous monitoring, verifying, 213
hardware, oversubscription, 30
log scrubbing, 211
performance, 211
APM, 212
infrastructure components, 212
resource availability, 212
resource utilization, 212
service management tools, 213
storage migrations, 198
tagging, 210–211
thresholds, 210
mounting, filesystems, 154–155
MPLS (Multiprotocol Label Switching)
latency, 240
VPN, 171
MTTR (Mean Time To Recovery), 269
MTU (Maximum Transmission Units), troubleshooting, 324
multiclouds, 6
multitenant object storage, 151
multitenant, public clouds, 3–4
multithreading
SMT, 184
temporal hyperthreading, 184

N

N-1 releases, patches, 225
NAC (Network Access Control), 79–80
NAC (Nondiscretionary Access Control), 60
NACL (Network Access Control Lists)
inheritance, 319
security groups versus, 318
troubleshooting, 318–319
name servers, DNS, 168–169
authoritative name servers, 169
caching name servers, 169
NAS (Network-Attached Storage), 151
NAT (Network Address Translation)
DNAT, 323
MASQUERADE, 323
SNAT, 323
troubleshooting, 322–323
netstat command, 330–331
network-based scans, 118
networks
business-based design solutions, 47–48
CDN, 169–170
Class C networks, 174–175
configurations, troubleshooting, 319–324
deployments, virtualization, 182
clock speeds, 187–188
dynamic allocations, 185, 189
GPU, 186–187
guest OS, 183
HCI, 188
hypervisors, 182–184
IPC, 188
memory, 188–189
SMT, 184
vCPU, 185–186
diagrams, disaster recovery, 278
directly connected networks, latency, 240
DLP, 79
DNS, 74
DNSSEC, 74–75
DoH, 74
DoT, 74
firewalls, 177
APC, 79
stateful firewalls, 78

stateless firewalls, 78
WAF, 78
flows, 80
GENEVE, 73
hardening, 81
ciphers, disabling, 81–82
firmware, upgrading, 82
unnecessary ports/services, disabling, 81
weak protocols, disabling, 81–82
HTTPS, 76
IPsec, 75
latency, 231, 240–241, 304–305
load balancers, 34–35, 176–177
NAC, 79–80
NTP, 75
NTS, 75
optimization, 237, 243–244
colocation, 243
device drivers, 244–245
edge computing, 241–242
firmware, 244–245
latency, 240–241
load balancers, 239
NIC, 239–240
open source software, 243
placement of resources, 242–243
redundancy, 243
SDN, 241
shaping networks, 238–239
oversubscription, 28–29
packet brokers, 80
performance, capacity planning, 17
provisioning resources, 142
routing
business-based design solutions, 48
dynamic routing, 172
HA, 33–34
static routing, 172
virtual routing (VRF), 171–172
SAN, 150
SDN, network optimization, 241
security
configuration changes, 81–85
DNS, 74
DNSSEC, 74–75
DoH, 74
DoT, 74
encryption, 75–76
firewalls, 177
hardening changes, 81–85
HTTPS, 76
IPsec, 75
network services, 77–80
NTP, 75
NTS, 75
protocols, 74–75
segmentation, 72–74
TLS, 76
tunneling, 76–77
segmentation, 72
GENEVE, 73
microsegmentation, 73
tiering, 73–74
VLAN, 72–73
VxLAN, 72–73
services, 166
CDN, 169–170
DHCP, 166
DNS, 167–169
IPAM, 170
NTP, 166–167
shaping, 238–239
sizing deployments, virtualization, 182
clock speeds, 187–188
dynamic allocations, 185, 189
GPU, 186–187
guest OS, 183
HCI, 188
hypervisors, 182–184
IPC, 188
memory, 188–189
SMT, 184
vCPU, 185–186
SR-IOV, 179

- subnet masks, 175
- subnetting, 47, 172–175
- switches, HA, 33
- TLS, 76
- traffic control, 82
    - blacklisting, 82
    - proxy servers, 82–84
    - whitelisting, 82, 89
- virtualization, 182
    - clock speeds, 187–188
    - dynamic allocations, 185, 189
    - GPU, 186–187
    - guest OS, 183
    - HCI, 188
    - hyperjacking, 183
    - hypervisors, 182–184
    - IPC, 188
    - memory, 188–189
    - SMT, 184
    - vCPU, 185–186
- VLAN, 72–73
- vNIC, 172
- VPC, 177–178
- VPN, 170
    - IPsec, 171
    - MPLS VPN, 171
    - point-to-point VPN, 171
    - point-to-site VPN, 171
    - site-to-site VPN, 170
- VxLAN, 72–73

new versions, lifecycle management, 219

NFS (Network File Systems), 154–155

NIC (Network Interface Controllers)
- jumbo packets, 239
- network optimization, 239–240
- receiver buffers, 239
- vNIC, 172

nonrelational databases, migrations, 201–202

NSG (Network Security Groups), 293–294, 318

nslookup command, 328–329

NTP (Network Time Protocol), 166–167

NTP (Network Trunk Protocol), 75

NTS (Network Time Security), 75

NVMe-oF (Non-Volatile Memory Express over Fabrics), 156–157

O

object storage, 141–142
- buckets, 151
- migrations, 200
- tenants, 151

object-based backups, 266

octal permissions, 93

off-peak hours, scheduling updates during, 239

old versions, lifecycle management, 219

open source software, network optimization, 245

openssl client command, 336

operating costs, 229–230
- chargebacks, 229–230
- showbacks, 230

optimization
- networks, 237, 243–244
    - colocation, 243
    - device drivers, 244–245
    - edge computing, 241–242
    - firmware, 244–245
    - latency, 240–241
    - load balancers, 239
    - NIC, 239–240
    - open source software, 243
    - placement of resources, 242–243
    - redundancy, 243
    - SDN, 241
    - shaping networks, 238–239
- right-sizing, 236

orchestration sequencing, 255–256

OS (Operating Systems)
- encryption, 98
- guest OS, 183
- instances, 143

security
account lockout policies, 89
antimalware, 93–94
antivirus software, 93–94
builds, 96–97
EDR, 93–94
encryption, 98
hardened baselines, 94–95
HIDS, 94
HIPS, 94
password complexity policies, 88–89
single function methodology, 95
software feature policies, 90
user permissions policies, 90–93
user/group policies, 90
templates, 143–144
outcomes/findings/actions (troubleshooting), documenting, 286
overall utilization, dashboards, 233
oversubscription, 28
compute power, 28–29
hardware, monitoring, 30
networks, 28–29
storage, 30

P

P2V (Physical to Virtual) migrations, 194
fully automated migrations, 194–195
manual migrations, 194
semi-automated migrations, 194
PaaS (Platform as a Service), 8
business-based design solutions, 43
cloud deployments, 140
cloud-to-cloud migrations, 196–198
packet analyzers, 335–336
packet brokers, 80
packet captures, 334
PAM (Private Access Management), 57
pass-through GPU, virtualization, 186–187
passwords
complexity policies, 88–89
hardcoded passwords, 255
vaults, 255
patches, 221
applications, 223–224
features/enhancements, 221–222
firmware, 224
fixes, broken/critical infrastructures/applications, 222
hypervisors, 222
N-1 releases, 225
networking components, 223
policies, 225
prioritizing patch applications, 120
rollbacks, 225–226
security patches, 118–119
software, 224
storage components, 224
troubleshooting, 315
virtual appliances, 223
virtual patches, 119
VM, 222–223
patterns, capacity planning, 22
peering
troubleshooting, 320
VPC, 178
penetration testing, business-based design solutions, 50–51
performance
capacity planning, 22–23
degradation, troubleshooting, 304
monitoring, 211
APM, 212
infrastructure components, 212
networks, capacity planning, 17
testing, business-based design solutions, 51
permissions
chmod command, 92–93
octal permissions, 93
user permissions policies, 90–93
persistent storage, 146
per-user licenses, 19
ping command, 325

PKI (Public Key Infrastructure), 66–67

placement of resources, network optimization, 242
- clusters, 242–243
- colocation, 243
- geographic locations, 242
- redundancy, 243

planning, capacity, 15, 16
- anomalies, 22
- baselines, 21
- budgetary requirements, 17
- business need analysis, 17–18
- GPU, 16
- hardware requirements, 16–17
- licensing, 18–20
- network performance, 17
- patterns, 22
- performance, 22–23
- RAM, 16
- software requirements, 17
- storage, 16
- system load, 21
- templates, 18
- trend analysis, 21
- troubleshooting, 307
- user density, 20
- vCPU, 16

plans of action, troubleshooting methodologies, 285–286

platforms, troubleshooting integrations, 308

playbooks
- configuration management, 252
- disaster recovery, 278

point-to-point VPN, 171

point-to-site VPN, 171

policies, 88
- account lockout policies, 89
- password complexity policies, 88–89
- patches, 225
- software feature policies, 90
- user permissions policies, 90–93
- user/group policies, 90
- whitelisting policies, 89

portfolio roadmaps, 219

ports
- disabling, 81
- forwarding, 76
- scanning, 116–117
- unnecessary ports, disabling, 81

postdeployment validation, 146

postmortems/lessons learned, incident response, 132

PPTP (Point-to-Point Tunneling Protocol), 77

preparation procedures, incident response, 124

preventive measures, troubleshooting methodologies, 286

prioritizing, patch applications, 120

private clouds, 4

private keys, 66

privileges, troubleshooting, 290
- escalating privileges, 291
- incomplete privileges, 290
- missing accounts/roles, 290

probable cause, theory of, 284–285

problems (troubleshooting), identifying, 283–284

process improvements, systems, 226

processing delays, 240

production environments
- business-based design solutions, 49
- upgrading, 228

proprietary lock-in migrations, 196

protocols
- encryption, 296–297
- unsupported protocols, 298
- weak protocols, disabling, 81–82

provisioning
- accounts, 58
- resources, 140–141
  - application resources, 142–143
  - compute resources, 141
  - network resources, 142
  - storage resources, 141–142
- thin/thick, storage systems, 160–161

proxy servers, 82
forward proxies, 83
reverse proxies, 83–84
tunneling proxies, 82–83
public clouds, 3
dedicated hosting, 4
multitenancy, 3–4
public data, 107
public keys, 66

Q

QA (Quality Assurance)
business-based design solutions, 48
upgrading, 227–228
QoS (Quality of Service), troubleshooting, 324
queuing delays, 240
quick fixes, 119, 120
quotas, user, 161

R

RACI matrix, 129
RAID (Redundant Array of Inexpensive Disks), 157
RAID 0, 157
RAID 1, 158
RAID 5, 158
RAID 6, 159
RAID 10, 159
RAM (Random Access Memory), capacity planning, 16
RDBMS (Relational Database Management System), 264
read/write operations, storage, 154
receiver buffers, NIC, 239
records management, 110
destroying data, 110
DNS, 169
retention, 110
versioning, 110
recovery, disaster
cold standby sites, 276–277
corporate guidelines, 277
documentation, 277
DR kits, 278
failbacks, 274
failovers, 274
geographical data center requirements, 279
hot standby sites, 275–276
network diagrams, 278
playbooks, 278
redundant resources, 275
RPO, 275
warm sites, 276
recovery procedures, incident response, 131
redundancy
clusters, 242
disaster recovery, 275
network optimization, 243
regions
HA, 30–31
Microsoft Azure Regions, 30–31
regression testing, business-based design solutions, 51
regulations/laws
data security, 109
database migrations, 200
relational databases, migrations, 201
release roadmaps, 219
remediation phase, vulnerability assessments, 117
replicating data, storage systems, 161
reporting methods
alerts, 229
logs, 229
metrics, 229
tagging, 229
request limits, API, troubleshooting, 308–309
requirements
analysis, solution design, 42
business-based design solutions, budgets, 45–46
capacity planning

budgets, 17
hardware, 16–17
software, 17
network requirements, business-based design solutions, 47–48

resiliency, clusters, 243

resources
availability
elasticity usage, 231
monitoring, 212
capacity planning, 307
placement of, 242
clusters, 242–243
colocation, 243
geographic locations, 242
redundancy, 212, 243
utilization, 336–337

responding to alerts, 214–215

response times (servers), latency, 305

responsibilities/roles
access control, 59
identity/access management, 57
incident response, 128–129
shared responsibility models, 7, 11–12
troubleshooting, 290

rest, data at, 104

REST error codes, 292–293

restores, 266, 269
3–2-1 rule, 269
alternate location restorations, 270
files, 270
in-place restorations, 269
MTTR, 269
retention policies, 266–267
snapshots, 270

restricted data, 107

retention

data, 110
policies, 266–267

reverse lookups, DNS, 169

reverse proxies, 83–84

revoked keys/certificates, troubleshooting, 295

right-sizing, 236

risk assessments, 117

risk registers, 120

roadmaps, 218–219

roles/responsibilities
access control, 59
identity/access management, 57
incident response, 128–129
shared responsibility models, 7, 11–12
troubleshooting, 290

rollbacks, patches, 225–226

rolling upgrades, 226–227

rollups, 120

root cause analysis, 132, 274

round robin load balancing, 35

round-trip times, latency, 304–305

route command, 332

routine operations, automation, 253

routing
business-based design solutions, 48
default routing, troubleshooting, 321
dynamic routing, 172, 322
GRE, 77
HA, 33–34
static routing, 172, 321
troubleshooting, 321
default routing, 321
dynamic routing, 322
static routing, 321
virtual routing (VRF), 171–172

routing tables, VPC, 178

RPO (Recovery Point Objectives), 268, 275

RTO (Recovery Time Objectives), 268

S

SaaS (Software as a Service), 8
business-based design solutions, 43
cloud deployments, 140

SAML (Security Assertion Markup Language), 66

SAN (Storage-Area Networks), 150

scalability, 25, 36. *See also* elasticity
auto-scaling, 36–37
cloud bursting, 37–38
containers, 32
database migrations, 200
horizontal scaling, 37
vertical scaling, 37
scanners
agent-based scans, 118
credential scans, 117–118
credentialed scans, 118
network-based scans, 118
port scanners, 116–117
service availabilities scans, 118
vulnerability scanners, 116
scheduling
backups, 267
updates, 119, 239
scope of incidents, 131
scripting
security, 254
troubleshooting, 305–306
scrubbing, log, 211
SDD, AWS storage options, 153–154
SDN (Software-Defined Networks), network optimization, 241
SDS (Software-Defined Storage), 162
searching files, NTP, 167
secret management, 67
security
agent-based scans, 118
applications
account lockout policies, 89
antimalware, 93–94
antivirus software, 93–94
builds, 96–97
EDR, 93–94
encryption, 98
hardened baselines, 94–95
HIDS, 94
HIPS, 94
password complexity policies, 88–89
single function methodology, 95
software feature policies, 90
user permissions policies, 90–93
user/group policies, 90
whitelisting, 89
attacks, 298–299
business-based design solutions, 46–47
CASB, 111
ciphers, 297
classifying data, 107
confidential data, 107
internal data, 107
metadata, 108
public data, 107
restricted data, 107
configuration changes
ciphers, disabling, 81–82
firmware, upgrading, 82
unnecessary ports/services, disabling, 81
weak protocols, disabling, 81–82
credential scans, 117–118
credentialed scans, 118
data breaches, 296
data security
access control, 108–109
CASB, 111
data classification, 107–108
data destruction, 110
data integrity, 105
data retention, 110
data segmentation, 108
digital signatures, 106
DLP, 111
encryption, 104–105
FIM, 106
hashing algorithms, 105–106
laws/regulations, 109
legal holds, 109
records management, 110
versioning, 110
WORM, 110
database migrations, 200

DDoS, 84–85
default accounts, deactivating, 120
destroying data, 110
digital signatures, 106
directory security groups, 294
DLP, 79
DNSSEC, 74–75
encryption, 75, 104
  API endpoints, 98
  applications, 98
  asymmetric encryption, 105
  filesystems, 99
  HTTPS, 76
  IPsec, 75
  MAC, 60
  protocols, 296–297
  storage, 98
  symmetric encryption, 105
  TLS, 76
exposed endpoints, 297–298
external attacks, 298
FIM, 106
firewalls, 100, 177
  APC, 79
  cloud-to-cloud migrations, 198
  HA, 35–36
  stateful firewalls, 78
  stateless firewalls, 78
  troubleshooting, 322
  WAF, 78
groups, NACL versus, 318
hardening networks, 81
  ciphers, disabling, 81–82
  firmware, upgrading, 82
  unnecessary ports/services, disabling, 81
  weak protocols, disabling, 81–82
hashing algorithms, 105–106
hot fixes, 119, 120
HTTPS, DoH, 74
insecure ciphers, 297
internal attacks, 299
IPsec, 75
legal holds, 109
NAC, 79–80
networks
  configuration changes, 81–85
  DNS, 74
  DNSSEC, 74–75
  DoH, 74
  DoT, 74
  encryption, 75–76
  flows, 80
  hardening changes, 81–85
  HTTPS, 76
  IPsec, 75
  network services, 77–80
  NTP, 75
  NTS, 75
  protocols, 74–75
  scans, 118
  segmentation, 72–74
  TLS, 76
  tunneling, 76–77
NSG, 293–294
NTS, 75
OS
  account lockout policies, 89
  antimalware, 93–94
  antivirus software, 93–94
  builds, 96–97
  EDR, 93–94
  encryption, 98
  hardened baselines, 94–95
  HIDS, 94
  HIPS, 94
  password complexity policies, 88–89
  single function methodology, 95
  software feature policies, 90
  user permissions policies, 90–93
  user/group policies, 90
packet brokers, 80
passwords
  hardcoded passwords, 255
  vaults, 255

patches
prioritizing patch applications, 120
security patches, 118–119
virtual patches, 119
port scanners, 116–117
privileges, 290
escalating privileges, 291
incomplete privileges, 290
missing accounts/roles, 290
protocols
encryption, 296–297
unsupported protocols, 298
quick fixes, 119, 120
records management, 110
destroying data, 110
retention, 110
versioning, 110
retaining data, 110
risk registers, 120
rollups, 120
scheduled updates, 119
scripting, 254
segmenting data, 108
service availabilities scans, 118
signature updates, 119
storage migrations, 198
TLS, 76
tools, impact on systems/services, 121
traffic control, 82
blacklisting, 82
proxy servers, 82–84
whitelisting, 82, 89
tunneling, 76
GRE, 77
L2TP, 77
PPTP, 77
SSH, 76–77
unsupported protocols, 298
user privileges, 290
escalating privileges, 291
incomplete privileges, 290
missing accounts/roles, 290
versioning, 110
virtual patches, 119
vulnerability scanners, 116
segmentation
data, 108
networks, 72
GENEVE, 73
microsegmentation, 73
tiering, 73–74
VLAN, 72–73
VxLAN, 72–73
semi-automated P2V migrations, 194
serverless applications, 9–10
servers
authoritative name servers, DNS, 169
caching name servers, DNS, 169
client interactions, NTP, 167
name changes, 311
name servers, DNS, 168–169
authoritative name servers, 169
caching name servers, 169
proxy servers, 82–84
response times, latency, 305
service accounts, automation, 255
service availabilities scans, 118
Service Health dashboard, AWS, 302–303
service models, 6–7
advanced cloud services, 9–11
AI, 10–11
IaaS, 7
business-based design solutions, 43
cloud deployments, 140
IoT, 9
machine learning, 11
PaaS, 8
business-based design solutions, 43
cloud deployments, 140
cloud-to-cloud migrations, 196–198
SaaS, 8
business-based design solutions, 43
cloud deployments, 140

serverless applications, 9–10
shared responsibility models, 11–12
services
collaboration services, cloud deployments, 138
directory services, 60–61
DNS, 74
email services, cloud deployments, 138
managing, 213
messaging services, cloud deployments, 138
network services, 166
CDN, 169–170
DHCP, 166
DNS, 167–169
IPAM, 170
NTP, 166–167
overloads, troubleshooting, 337
subscription services, 136–137
unnecessary services, disabling, 81
severity categorization, logging, 207–208
shaping networks, 238–239
shared responsibility models, 7, 11–12
showbacks, 230
shutdowns, automation, 254
signature updates, 119
signatures, digital, 106
single function methodology, 95
single points of failure, HA, 36
single-tenant object storage, 151
site-to-site VPN, 170
sizing deployments, virtualization, 182
clock speeds, 187–188
dynamic allocations, 185, 189
GPU, 186–187
guest OS, 183
HCI, 188
hypervisors, 182–184
IPC, 188
memory, 188–189
SMT, 184
vCPU, 185–186
SLA (Service-Level Agreements), 46, 268
SMT (Simultaneous Multithreading), 184
snapshots, 262–263, 270
SNAT (Source NAT), 323
SNMP (Simple Network Management Protocol), 206, 207
socket-based licenses, 19
software
antimalware, 93–94
antivirus software, 93–94
builds, 96
beta builds, 96
canary builds, 97
LTS builds, 97
stable builds, 96
business-based design solutions, 42–43
capacity planning, 17
closed source vendor software, 245
feature policies, 90
open source software, network optimization, 245
patches, 224
SaaS, 8, 43
SDS, 162
solution design, business-based
blue-green deployments, 49
budgetary requirements, 45–46
compliance, 46
development environments, 48
DR environments, 49–50
functional testing, 51
hardware, 43–45
integration, 45
network requirements, 47–48
penetration testing, 50–51
performance testing, 51
production environments, 49
QA environments, 48
regression testing, 51
requirement analysis, 42
routing, 48
security, 46–47
SLA, 46
software, 42–43

staging environments, 49
subnetting, 47
usability testing, 51–52
user needs, 46
vulnerability testing, 50

solution templates, 144

spinning disk storage, 152

spoofing, DNS, 74

SR-IOV (Single Root Input/Output Virtualization), 179

ss command, 331

SSH (Secure Shell), 76–77

SSO (Single Sign-On), 65–66

stable builds, 96

staging environments, business-based design solutions, 49

stateful firewalls, 78

stateless firewalls, 78

static routing, 172, 321

storage

block storage, 141
migrations, 199
SAN, 150
capacity planning, 16
CIFS, 155
DAS, 188
encryption, 98
FC, 156
file storage, 141
migrations, 199
NAS, 151
Flash storage, 152
HDD, 152, 153
hybrid storage, 152
IOPS, 153–154
iSCSI, 155–156
long-term storage, 152–153
magnetic drives, 152
migrations, 198
bandwidth, 198
block storage, 199
cost, 199
data integrity, 198
file storage, 199
monitoring, 198
nonrelational databases, 201–202
object storage, 200
relational databases, 201
security, 198
mirroring, 158
NAS, 151
NFS, 154–155
NVMe-oF, 156–157
object storage, 141–142
buckets, 151
migrations, 200
tenants, 151
oversubscription, 30
patches, 224
persistent storage, 146
provisioning resources, 141–142
RAID, 157
RAID 0, 157
RAID 1, 158
RAID 5, 158
RAID 6, 159
RAID 10, 159
read/write operations, 154
replicating data, 161
SAN, 150
SDD, 153–154
SDS, 162
spinning disk storage, 152
system features
compression, 160
cost savings, 159
deduplication, 160
DLP, 159
tenants, 151
thin/thick provisioning, 160–161
tiers, 152
user quotas, 161

strategy roadmaps, 219

subdomains, DNS, 168

subnet masks, 175

subnetting, 172–175
business-based design solutions, 47
troubleshooting, 320–321
VPC, 177
subscriptions, 20
files, 137
services, 136–137
switches, HA, 33
symmetric encryption, 105
synthetic full backups, 262
Syslog, 206–207
system load, capacity planning, 21
system logs, 209
systems
migrations, 219–220
process improvements, 226
upgrading, 219–220

T

tabletops, incident response, 126
tagging, 210–211, 229
tags, metadata, 108, 306–307
tape backups, 265
targets
backups, 265
iSCSI, 156
tcpdump command, 334
templates, 18, 143
customizing, 145
OS templates, 143–144
solution templates, 144
variables, template customization, 145
temporal hyperthreading, 184
tenants, object storage, 151
testing, 50
functional testing, 51
penetration testing, 50–51
performance testing, 51
probable causes, troubleshooting methodologies, 285
QA environments, 48
regression testing, 51
usability testing, 51–52
vulnerability testing, 50
theory of probable cause, 284–285
thick provisioning, storage systems, 160–161
thin provisioning, storage systems, 160–161
thresholds, monitoring, 210
tiering, 73–74
tiers, storage, 152
timestamps, NTP
file searches, 167
transaction logs, 167
TLS (Transport Layer Security), 74, 76
tools
collaboration tools, 138
security tools
agent-based scans, 118
credential scans, 117–118
credentialed scans, 118
default accounts, deactivating, 120
hot fixes, 119, 120
impact on systems/services, 121
network-based scans, 118
patches, 118–119, 120
port scanners, 116–117
quick fixes, 119, 120
risk registers, 120
rollups, 120
scheduled updates, 119
service availabilities scans, 118
signature updates, 119
vulnerability scanners, 116
troubleshooting tools
arp command, 332–333
curl command, 333–334
dig command, 329–330
flushdns command, 326
ifconfig/ipconfig command, 326–327
ip command, 327–328, 332
netstat command, 330–331

nslookup command, 328–329
openssl client command, 336
packet analyzers, 335–336
packet captures, 334
ping command, 325
resource utilization, 336–337
route command, 332
ss command, 331
tcpdump command, 334
tracert/traceroute command, 325–326
tstark command, 335–336
wireshark command, 335

top-level domains, DNS, 168

tracert/traceroute command, 325–326

traffic control, 82
blacklisting, 82
proxy servers, 82–84
whitelisting, 82, 89

traffic flows, network optimization, 238

trails, logging, 208

training, incident response, 126

transaction logs, NTP, 167

transit, data in, 104

transmission delays, 240

traps, 207

trend analysis, capacity planning, 21

trending, logging, 209

troubleshooting
accounts, mismatches, 310
ACL, 318–319
action plans, 285–286
API, request limits, 308–309
applications, 337
memory management, 337
service overloads, 337
arp command, 332–333
authentication, 291–292
authorization, 292–293
automation
API version incompatibility, 314
deprecated features, 313–314
job validation, 314–315
patch failures, 315
tool incompatibility, 313
billing issues, 309–310
capacity planning, 307
change implementation, 282–283
change management, 310–311
feature/version mismatches, 312
locations, 312
server name changes, 311
compromised keys/certificates, 295
configurations, 305–306, 319–320
connectivity, 302
capacity planning, 307
CSP outages, 302–304
ISP outages, 304
latency, 304–305
licensing, 307
metadata tags, 306–307
performance degradation, 304
scripts, 305–306
corporate policies/procedures, 282–283
costs, 309–310
CSP, 302–304
curl command, 333–334
deprecated features, 313–314
dig command, 329–330
digital certificates, 294
compromised certificates, 295
expired certificates, 294
misconfigured certificates, 295
revoked certificates, 295
trusted certificates, 295
expired keys/certificates, 294
findings/actions/outcomes, documenting, 286
firewalls, 322
flushdns command, 326
full system functionality, 286
identifying problems, 283–284
ifconfig/ipconfig command, 326–327
IP addresses, 320–321
ip command, 327–328, 332

IP spaces, 320–321
ISP, 304
job validation, 314–315
keys, 294
  compromised keys, 295
  expired keys, 294
  misconfigured keys, 295
  revoked keys, 295
latency, networks, 304–305
licensing, 307
memory management, 337
methodologies
  action plans, 285–286
  change implementation, 282–283
  corporate policies/procedures, 282–283
  findings/actions/outcomes, documenting, 286
  full system functionality, 286
  identifying problems, 283–284
  preventive measures, 286
  testing probable causes, 285
  theory of probable cause, 284–285
misconfigured keys/certificates, 295
missing accounts/roles, 290
MTU, 324
NACL, 318–319
NAT, 322–323
netstat command, 330–331
network latency, 304–305
networks, configurations, 319–324
NSG, NACL, 318
nslookup command, 328–329
openssl client command, 336
packet analyzers, 335–336
packet captures, 334
patches, 315
peering, 320
ping command, 325
platforms, integrations, 308
preventive measures, 286
privileges, 290
  escalating privileges, 291
  incomplete privileges, 290
  missing accounts/roles, 290
QoS, 324
request limits, API, 308–309
resource utilization, 336–337
REST error codes, 292–293
revoked keys/certificates, 295
roles/responsibilities, 290
route command, 332
routing, 321
  default routing, 321
  dynamic routing, 322
  static routing, 321
scripts, 305–306
service overloads, 337
ss command, 331
subnetting, 320–321
tags, metadata, 306–307
tcpdump command, 334
testing probable causes, 285
theory of probable cause, 284–285
tracert/traceroute command, 325–326
trusted certificates, 295
tstark command, 335–336
user privileges, 290
  escalating privileges, 291
  incomplete privileges, 290
  missing accounts/roles, 290
vendors, 308
  account mismatches, 310
  API request limits, 308–309
  costs/billing issues, 309–310
  integrations, 308
  migrations, 308
wireshark command, 335

trusted certificates, troubleshooting, 295

TSIG (Transaction Signatures), 74–75

tstark command, 335–336

TTL (Time To Live), 169

tunneling, 76
  GRE, 77
  L2TP, 77
  PPTP, 77

proxies, 82–83
SSH, 76–77
Type 1 hypervisors, 26, 183
Type 2 hypervisors, 27, 183–184
Type 3 hypervisors, 184

U

unnecessary ports/services, disabling, 81
unsupported protocols, 298
updating
accounts, 58
automating updates, 253
scheduled updates, 119, 239
signature updates, 119
upgrading
active-passive upgrades, 227
continuous delivery, 226–227
development environments, 227
DR environments, 228
firmware, 82
production environments, 228
QA environments, 227–228
rolling upgrades, 226–227
systems, 219–220
usability testing, business-based design solutions, 51–52
use, data in, 104
users
accounts, 56–57
certificate management, 63–64
DAC, 59–60
default accounts, deactivating, 120
directory services, 60
FID, 61–63
groups, 57
LAM, 57–58
LDAP, 61
life-cycle management, 58
lockout policies, 89
MAC, 60, 99–100
MFA, 64–65
missing accounts/roles, troubleshooting, 290
NAC, 60
PAM, 57
PKI, 66–67
role-based access control, 59
roles, 57
SSO, 65–66
business-based design solutions, 46
density, 20
permissions policies, 90–93
policies, 90
privileges, troubleshooting, 290
escalating privileges, 291
incomplete privileges, 290
missing accounts/roles, 290
quotas, storage systems, 161

V

V2V (Virtual to Virtual) migrations, 195
validation
job validation, troubleshooting, 314–315
postdeployment validation, 146
variables, template customization, 145
vaults, passwords, 255
vCPU (Virtual CPU), 16, 185–186
VDI (Virtual Desktop Infrastructure), 138–139
vendors
device drivers/firmware, 244–245
integrations, troubleshooting, 308
migrations
lock-in migrations, 196
troubleshooting, 308
troubleshooting, 308
account mismatches, 310
API request limits, 308–309
costs/billing issues, 309–310
integrations, 308
migrations, 308

verification
- continuous monitoring, 213
- full system functionality (troubleshooting), 286

version control, 250–251
- branches, 251
- checkouts, 251
- clones, 251
- merges, 251

versioning
- API version incompatibility, troubleshooting, 314
- data, 110
- deprecated features, troubleshooting, 313–314
- feature/version mismatches, troubleshooting, 312
- lifecycle management, 219

vertical scaling, 37

virtual appliances, patches, 223

virtual GPU, 186

virtual patches, 119

virtual routing (VRF), 171–172

virtualization, 182
- clock speeds, 187–188
- dynamic allocations
  - CPU, 185
  - memory, 189
- GPU, 186
  - pass-through GPU, 186–187
  - virtual GPU, 186
- guest OS, 183
- HCI, 188
- hypervisors, 182
  - bare metal hypervisors. *See* Type 1 hypervisors
  - patches, 222
  - Type 1 hypervisors, 183
  - Type 2 hypervisors, 183–184
  - Type 3 hypervisors, 184
- IPC, 188
- memory, 188–189
- SR-IOV, 179
- vCPU, 185–186

viruses, antivirus software, 93–94

VLAN (Virtual LAN), 72–73

VM (Virtual Machines)
- affinity, 27
- anti-affinity, 27–28
- containers, 145
- deployments, 143
  - containers, 145
  - instances, 143
  - persistent storage, 146
  - postdeployment validation, 146
  - templates, 143–144
  - variables, template customization, 145
  - virtualization, 182
  - virtualization, clock speeds, 187–188
  - virtualization, dynamic allocations, 185, 189
  - virtualization, GPU, 186–187
  - virtualization, guest OS, 183
  - virtualization, HCI, 188
  - virtualization, hypervisors, 182–184
  - virtualization, IPC, 188
  - virtualization, memory, 188–189
  - virtualization, SMT, 184
  - virtualization, vCPU, 185–186
- hyperjacking, 183
- hypervisors, 26–27
- instances, 7, 143
- patches, 222–223
- templates, 143–144
- variables, template customization, 145

vNIC (Virtual Network Interface Controllers), 172

VoIP (Voice over IP), cloud deployments, 137

volume-based licenses, 19

VPC (Virtual Private Clouds), 5, 177
- endpoints, 178
- gateways, 178

hub-and-spoke VPC, 178
peering VPC, 178
routing tables, 178
subnetting, 177

VPN (Virtual Private Networks), 170
IPsec, 171
MPLS VPN, 171
point-to-point VPN, 171
point-to-site VPN, 171
site-to-site VPN, 170

VRF (Virtual Route Forwarding), 171–172

vulnerabilities
assesments, 117
scanners, 116

testing, business-based design solutions, 50

VxLAN (Virtual Extensible LAN), 72–73

W

WAF (Web Application Firewall), 78

warm sites, disaster recovery, 276

weak protocols, disabling, 81–82

weighted load balancing, 35

whitelisting, 82, 89

wireshark command, 335

workloads, performance testing, 51

X - Y

YAML (YAML Ain't Markup Language), templates, 18

Z

zone files, DNS, 168–169

zones, 31

zoning, SAN, 150