

Table of Contents

Module 1	16
Course Overview	16
Course Description	17
For whom is this learning path intended?	18
Prerequisites	19
What does the Cert Exam validate?	20
Course Outline	22
Take the Skill Checks to Test Your Knowledge	24
Explore Limitless Possibilities with OCI's Official Documentation	25
Get the Answers You Need: Use our "Ask Your Instructor" Form	26
Let's get started!	27
Module 2	28
Shared Security Model	28
Shared Security Model	29
Zero Trust Security	30
Zero Trust: Concept	31
Zero Trust: Principles	32
Security Services Introduction	33
Security Services	35
Object Storage Security	36
Security Services Use case	37
Security Questions	41
Security Design and Controls	52
Platform Security	54
Physical Security: Data Center Site	55

Physical Security Inside Data Center	56
Operational Security	57
Secure Connectivity	59
Data and Application Protection	62
Culture of Trust and Compliance	66
Module 3	67
Introduction	67
What is OCI IAM?	68
OCI IAM: Authentication (AuthN)	70
OCI IAM: Authorization (AuthZ)	72
OCI IAM Components	74
OCI IAM Identity Domains	79
What are □OCI IAM identity domains?	80
Identity Domains	81
Identity Domains: Use Cases	82
Identity Domains: Identity Lifecycle Management	83
OCI IDENTITY & ACCESS MANAGEMENT (IAM)	87
OCI IAM with Identity Domains	88
Identity Domain Types	89
Identity Domain Types	90
Default Identity Domain	95
Default Domain	96
Dos and Don'ts for the Administrator Users	98
Creating Identity Domains	99
Why do we need multiple identity domains?	100
Creating Identity Domains	101
Demo: Creating Identity Domains	102
Creating Identity Domains	103

Managing Groups	104
Groups	105
Default Groups in Identity Domains	107
Demo: Creating Groups	108
Creating Groups	109
Managing Users	111
Stages of the IAM User Life Cycle	112
User Lifecycle Management	113
Demo	114
Creating Groups	115
Demo: Creating Users	116
Creating Groups	117
Creating Users	118
Understanding the Administrator Role	119
Administrator Roles: Key Points	120
Types of Administrator Roles	121
Demo	122
Assigning Administrative Roles	123
Demo: Understanding Administrator Role	124
Policies	125
Policies	126
Subjects Clause	127
Actions Clause	130
Placement	132
Demo: Policies	133
Compartments	134
Compartment	135
Resource Compartments	137

Compartments□Access.....	138
Interaction of Resources	139
Movement of Resources	140
Multiple Regions	141
Nested Compartments	142
Demo: Compartments	143
Compartment Quotas	144
Scenario	145
Quota Syntax	146
Quota Examples	152
Types of Quota Policy Statement	153
Quota Examples	154
Budgets	155
Demo: Compartment Quotas	156
Module 4	157
Policy Inheritance and Attachment	157
Policy Inheritance	158
Policy Attachment	160
Demo: Policy Inheritance and Attachment	162
Conditional Policies	164
Conditional Policies	165
Conditions	167
Examples	169
Demo: Conditional Policies	170
Enforce Least Privileged: Advanced Policies	171
Permissions	172
Example	173
Network Sources	177

Network Sources	178
Demo: Network Sources	181
Scenario	182
Tag Based Access Control	183
Tag-based Access Control	184
Example	187
Demo: Tag Based Access Control	189
Dynamic Groups	190
Terms	191
Resource Principals Patterns	192
Infrastructure Principals	193
Stacked Principals	194
Ephemeral Principals	195
Dynamic Groups	196
Dynamic Groups	197
Policies	198
Demo: Dynamic Groups	199
Scenario: Dynamic Groups	200
Optimizing IAM Policies: Part 1	201
OCI IAM Policies	202
Eliminating Duplicate Policies	204
Removing Less-Permissive Policies	206
Policy Conditions and Inheritance	208
Removing Less-Permissive Policies	209
Consolidating Group Membership	210
Consolidating Group Membership: Same Members	211
Consolidating Group Membership: Different Members	212
Optimizing IAM Policies: Part 2	213

Combining Policy Statements	214
Combining Policy Statements: Use case	217
Grouping Multiple Entities	218
Pattern-Based Optimization	220
Object-Level Granular Access Control for OCI Object Storage	222
OCI Object Storage	223
Object-Level Permissions	225
Object IAM	226
Object IAM Policy Examples	227
Organization Management	230
OCI Organization Management	231
Benefits of Sharing a Subscription	233
Governance Rules	234
Demo: Organization Management	235
Module 5	236
Securing Access using IAM	236
Securing Access using IAM	237
Password Policies	238
Password Policy	239
Types of Password Policies	240
Demo: Password Policies	241
MultiFactor Authentication (MFA)	242
Multifactor Authentication	243
Enable MFA	244
Demo: Multifactor Authentication	247
Adaptive Security	248
Adaptive Security	249

Risk Providers	253
Passwordless Authentication	254
OCI IAM Passwordless Authentication	257
How does OCI IAM Passwordless authentication work?	258
Network Perimeter	261
Network Perimeter	262
Demo	263
OCI IAM Reports	264
OCI Tenancy	265
Types of Reports	268
Accessing Reports: Administrator Roles	269
Notification	276
Notifications	277
Workflow for Customizing Notifications	280
Branding	281
Branding	283
Module 6	284
Course Overview	284
Oracle Access Governance - Course Overview	285
Introduction to Access Governance	286
Why Access Governance?	287
Oracle Access Governance	288
Oracle Access Governance Features	289
Oracle Access Governance Benefits	290
Introduction to Identity Governance and Administration	291
Challenges with Ungoverned Identities	292
Challenges with Access Control Measures	293
Evolving Requirements for Identity Governance and Administration	294

Identity Governance and Administration (IGA)	295
Identity Governance and Administration Capabilities	296
Access Governance Architecture	297
Oracle Access Governance Architecture: Functional View	298
Core Functional Areas	299
Oracle Access Governance: Key Capabilities	300
Oracle Access Governance Architecture: Physical View	301
Access Governance Roles	302
Access Governance Application Roles	303
User Access Model	304
Demo: Creating Access Governance Service Instance	305
Demo: Configuring Access Governance Roles	306
Module 7	307
Identity Orchestration	307
Access Governance: Core Functional Areas	308
Identity Orchestration in a Hybrid, Multicloud Environment	309
Identity Provisioning and Reconciliation	310
Identity Orchestration with Authoritative Source	311
Identity Orchestration: Key Capabilities	312
Connected Systems	313
Authoritative Sources and Target Systems	314
Connected Systems Integration Architecture	315
Example 1: Access Governance and OIG Integration	316
Example 2: Access Governance and OCI Integration	317
Codeless Integration	318
Codeless Integration: Design Goals	319
Example: OIG Codeless Integration	320
Integration of Oracle Access Governance with OCI IAM	321

Demo: Configuring Access Governance Roles	322
Custom Identity Attributes	323
Identity Attributes	324
Custom Attribute Support in Access Governance	325
Identity Marking	326
Access Governance User Classifications	327
Workforce & Consumer User Capabilities	328
Workforce & Consumer Users	329
Identity Marking in Access Governance	330
Access Control	331
Core Functional Area – Access Control	332
Access Control –Key Capabilities	333
Modern requirements for Access Control measures	334
Oracle Access Governance Access Model	335
Manual Provisioning to Automated Access	336
Access Requests and Approval Workflows	337
Access Requests as Access Control Mechanism	338
Approval Workflows	339
Access Requests flow in Access Governance	341
Identity Collections	342
Attribute-Based Access Control (ABAC)	343
ABAC as Access Control Mechanism	344
Identity Collections	345
Demo: Creating Identity Collection	346
Access Bundles	347
Access Bundles	348
Demo: Creating Access Bundle	349
Role-Based Access Control (RBAC)	350

Role-Based Access Control (RBAC)	351
Roles in Access Governance	352
Demo: Role Based Access Control	353
Policy-Based Access Control (PBAC)	354
Policy-Based Access Control (PBAC)	355
PBAC in Access Governance	356
Demo: Policy Based Access Control	357
Module 8	358
Governance and Compliance	358
Core Functional Areas – Governance and Compliance	359
Governance and Compliance in Modern Enterprises	360
Governance and Compliance: Key Capabilities	361
Enforcing Compliance Through Access Reviews	362
Campaigns and Access Reviews	363
Enforcing Compliance Through Access Reviews	364
Introduction to Access Reviews	365
Access Review Campaigns	366
Campaign Types and Selection Criteria	367
Policy Reviews	368
OCI Identity and Access Management	369
Policies	370
Policy Review in Access Governance	371
Policy Review Campaigns	372
Policy Review Selection Criteria	373
Event-Based Reviews	374
Need for Event-Based Access Reviews	375
Event-Based Review Types	376
Event-Based Access Review Flow	377

Delegation	378
Delegation in Access Governance	379
Delegation Preferences in AG	380
Demo: Creating Review Campaigns	381
Identity Intelligence	382
Core Functional Areas – Identity Intelligence	383
Identity Intelligence –Key Capabilities	384
Prescriptive Analytics and Insights	385
Prescriptive Analytics for Informed Decisions	386
Intelligent Insights in Oracle Access Governance	387
Intelligent Dashboard	388
Who has Access to what?	389
My Access and My Directs’ Access	390
Enterprise-wide Access	391
Application Details	392
Identity Access Details	393
Connected Systems (DB and Flat File)	394
Access Reviews	395
Access Control - Policy Reviews	396
Event-Based Access Review Report	397
Identity Correlation	398
Identity Correlation	399
Unmatched Account Management	400
Recommendations and Remediation	401
Remediation	402
Remediation: Example	403
Remediation: Perform Access Review Tasks for Identity Collection	404
Remediation: Perform Policy Review Tasks	405

Demo: Reviews and Identity Insights	406
Module 9	407
Introduction to Virtual Cloud Network	407
Objectives	408
Oracle Cloud Infrastructure Architecture	409
Virtual Cloud Network (VCN)	410
CIDR Notation	411
CIDR: Example	412
IP Address Range for Your VCN	413
IP Address Range for Your VCN	414
Subnet	415
IAM Policies for Networking □Admins/Users	417
Objectives	418
Compartments and Your Cloud Network	419
Network Security Group (NSG)	420
IAM Policies for Networking	421
Nuances of Different Verbs	423
Demo: Public and Private Subnets	424
VCN Security	425
Objectives	426
Security List (SL)	427
Network Security Group (NSG)	428
SL + NSG	429
Stateful Security Rules	430
Stateless Security Rules	431
Bastion Host	432
Demo: Security List	433
Demo: Network Security Group	434

Zero Trust Packet Routing (ZPR)	435
Network Architecture Is Not the Same as Network Security	436
Simple Scenario	438
Network Configuration Is Complicated by Security	444
OCI Zero Trust Packet Routing (ZPR)	445
ZPR Separates Security from Network Configuration	446
OCI Zero Trust Packet Routing (OCI ZPR)	447
Benefits of OCI Zero Trust Packet Routing (ZPR)	449
How to Set Up OCI ZPR	450
OCI ZPR: How It Works	451
OCI ZPR: Use Case	455
Introducing CarCo	456
CarCo Scales Up and Makes Network Changes	457
CarCo Network Update Introduces a Security Issue	458
Protecting CarCo with OCI Zero Trust Packet Routing	459
VCN Connectivity	460
Objectives	461
Connectivity Options	462
Site-to-Site VPN	463
Site-to-Site VPN (IPSec)	464
Site-to-Site VPN (IPSec): Configuration Workflow	465
Fast Connect	466
FastConnect	467
FastConnect – Use cases	468
FastConnect Connectivity Providers	469
IPsec VPN and FastConnect	470

Table of Contents

Module 10	17
Load Balancer Concepts	17
Primer	18
OCI Load Balancing Service	19
OCI Flexible Load Balancer	20
Fixed to Flexible Load Balancer	21
HTTP/2 Support on Flexible Load Balancer	22
Public and Private Load Balancer	23
Public Load Balancer	24
Public Load Balancer (Regional Subnets)	26
Public Load Balancer (AD-Specific Subnets)	27
Private Load Balancer	28
Private Load Balancer (Using Regional Subnets)	30
Public Load Balancer (AD-Specific Subnets)	31
Load Balancer Policies and <input type="checkbox"/> Health Checks	32
Load Balancing Policies	33
Health Check	34
SSL Handling	35
SSL Handling	36
Concepts	37
LB with SSL Not Enabled	38
Generate Private Key and CSR	39
Generate a Self-Signed Certificate	40
Add Certificate to the LB	41
Create a Listener to Listen on Port 443	42

SSL Termination Enabled for LB	43
Demo: SSL Certificate	44
Troubleshoot: High Availability with IP Hash Load Balancing	45
Ensuring High Availability with Load Balancer	46
IP Hash Algorithm and Workflow	47
Troubleshoot: Load Balancer Critical Health Check Error	48
Load Balancer Health Check – Critical Error	49
Certificates Overview	50
Certificate Creation	51
TLS Connection	52
Mutual TLS Connection	53
Certificate Authority (CA)	54
Certificate Authorities: Examples	57
Chain of Trust	58
Types of Certificates	59
Certificate Pain Points	60
OCI Certificates Service	61
OCI Certificates Service	62
OCI Certificates	63
OCI Certificates: Concepts	64
Certificate Authority	65
Certificates	66
Certificates: Modes of Operation	68
Certificate Rules	72
Certificate Profile	73
Integrations	74
OCI Certificates: <input type="checkbox"/> Lifecycle Management Features	75
OCI Certificates – Use cases	76

Use Case 1: Public Certificate	77
Use Case 2: Private Certificate	78
Use Case 3: Private Certificate - mTLS	79
Use Case 4: Code Signing	80
Demo: OCI Certificates	81
OCI Certificates - Scenario	82
Module 11	84
OCI Network Firewall	84
Why we need Firewall?	85
OCI Network Firewall	86
OCI Network Firewall-Deployment	88
OCI Network Firewall-Workflow	90
OCI Network Firewall – Use Cases	91
Use Case 1: Perimeter Security	92
Use Case 2: Intrusion Detection and Prevention	93
Use Case 3: Selective Access to Oracle Services Network (OSN)	94
Use Case 4: Application Segmentation and Zero-Trust	95
Network Firewall Policy	96
Network Firewall Policies	97
Building Rules -Create Policy Workflow	99
Network Firewall Policy Components	100
Rules	103
Demo: OCI Certificates	104
OCI Certificates - Scenario	105
Module 12	107
Securing Applications in the Cloud – Part 1	107
Objectives	108
Multiple Layers of Defense	109

Web Application Firewall	110
OCI Web Application Firewall	111
OCI WAF Architecture	112
WAF Point of Presences (PoPs)	113
OCI WAF Use Cases	114
OWASP Rules in OCI WAF	115
Securing Applications in the Cloud – Part 2	116
Objectives	117
WAF Service Components	118
Origin Management	119
Protection Rules	120
Access Control	121
Bot Management	122
Caching Rules	123
Threat Intelligence	124
Shared Responsibility Model for WAF	125
Benefits of Oracle Cloud Infrastructure WAF	126
Required IAM Policies	127
Getting Started with WAF - Prerequisites	128
Getting Started with WAF - Workflow	129
Demo: Load Balancer and WAF Policy	130
Demo: Creating a WAF Policy	131
Demo: Enabling Protection Rules □and XSS	132
Demo: Creating a WAF Bot Management	133
Demo: Adding Access Control Rules	134
Module 13	135
Compute Best Practices	135
Security Recommendations	136

Shielded Instances	138
Shielded instances	139
OCI Bastion Service	140
Scenario	141
OCI Bastion Service	143
OCI Bastion	144
Session Types	145
Managed SSH Session	146
SSH Port Forward Session	147
Dynamic Port Forward Session	148
OCI Bastion Details	149
Required IAM Policies for using OCI Bastion service	150
Demo: Manage Bastion	151
Demo: Bastion Port Forwarding	152
Oracle OS Management Hub (OSMH)	153
Understanding Challenges of IT Administrator	154
Managing the OS: Challenges	159
Oracle OS Management Hub	160
OSMH Service Architecture	162
OSMH Dashboard	164
OSMH: Simplify and Automate Patch Updates	166
OSMH: Benefits	167
Oracle OS Management Hub (OSMH) Components	168
OSMH Components	169
OSMH: OCI IAM Policies	170
Supported OS Platforms	175
Oracle OS Management Hub (OSMH) for OCI Instances	176
OSMH Example: OCI Instances	177

Oracle OS Management Hub (OSMH) □Management Station	188
OSMH: Management Station	189
Management Station	190
Oracle OS Management Hub (OSMH) □Lifecycle Environments	192
Scenario	193
Lifecycle Environments	194
Lifecycle Environments Benefits	195
Dedicated Virtual Machine Hosts	196
Dedicated Virtual Machine Hosts	197
Example Scenarios	198
Available shapes defined by host type	199
Limitations	200
Module 14	201
OCI Vulnerability Scanning Service	201
OCI Vulnerability Scanning□Service	202
Setting up VSS	206
Scanning Reports	209
Cloud Guard integration	210
Demo: OCI Vulnerability Scanning Service	211
Scenario	212
Demo: Cloud Guard Integration with Vulnerability Scanning Service	213
Demo: Scanning Container Image □for Vulnerabilities	214
Demo: Scan and Verify Container Image for Security	215
Module 15	216
OCI Key Management Service (KMS)	216
OCI Encryption Options	217
OCI KMS encryption portfolio	220

Choosing the right OCI KMS offering	221
OCI KMS offers	222
Encryption Basics	223
Encryption at rest and in-transit	225
Symmetric Encryption	226
Asymmetric Encryption	227
Encryption Concepts	228
Hardware Security Module (HSM)	229
Vault Introduction	230
OCI Vault	231
Vaults	232
Keys	233
Master and Data Encryption Keys	234
Master Encryption Keys: Protection Modes	235
Wrapping Keys	236
Rotating Keys	237
Demo: Encryption and Decryption of Data with Vault	238
Import and Export Keys	239
Cryptographic and Management Endpoints	240
Crypto Operations	242
Importing Keys or Key Versions	243
Exporting Keys or Key Versions	244
OCI Services Integration with Vault	245
Encryption Using Oracle-Managed Keys	247
Encryption Using Customer-Managed Keys	248
OCI Object Storage Integration with Vault	249
Back up and Replicate Vaults and Keys	250
Backing Up Vaults and Keys	251

Restoring Vaults and Keys	253
Cross-Region Replication	254
Secrets	255
What's a Secret?	256
Secrets	257
Secrets Rules	259
Demo: Automate Secret Generation and Audit	260
Demo: Retrieve Secret from Vault Using Instance Principal	261
OCI Dedicated Key Management Service (KMS)	262
What is OCI Dedicated KMS?	263
Dedicated KMS – Architecture	265
Workflow for setting up HSM Cluster	266
OCI Dedicated KMS – Use cases and Benefits	267
Dedicated KMS – Use Cases	268
Dedicated KMS versus Private Vault	271
Key benefits of Dedicated KMS	272
OCI External KMS - Overview	273
OCI KMS	274
External KMS	275
How External KMS works?	276
OCI External KMS - Onboarding	278
Onboarding External KMS	279
External KMS - Vault	280
External KMS – Key Reference	281
External KMS – Using Key References	282
External KMS – When to use?	283
External KMS – Use cases	284
External KMS - Details	285

Module 16	286
Oracle Database Security	286
Objectives	287
Take a Guess!	288
Data Vulnerability	289
Database Security in OCI	290
Controlled Access	291
Safeguarding Your Database	293
Data Encryption	294
Database Patching	295
Security Assessment	296
Autonomous Database Security	297
Security in Autonomous Database (ADB)	298
Oracle Data Safe	302
Objectives	303
Introduction – Data Security	304
Data – The Critical Asset	305
Data Protection Consideration	306
Overview – Oracle Data Safe in OCI	307
Oracle Data Safe in OCI	308
Oracle Data Safe: Features	309
Oracle Data Safe – Security Assessment	310
Oracle Data Safe: Security Assessment	313
Oracle Data Safe – User Assessment	314
Oracle Data Safe: User Assessment	315
Oracle Data Safe – Activity Auditing	317
Oracle Data Safe: Activity Auditing	318
Oracle Data Safe: Activity Auditing (Features)	319

Oracle Data Safe – Data Discovery	323
Oracle Data Safe: Data Discovery	324
Oracle Data Safe – Data Masking	327
Oracle Data Safe: Data Masking	328
Oracle Data Safe – Architecture	331
Oracle Data Safe: Architecture	332
Oracle Data Safe: Administration in OCI	334
Oracle Data Safe – Targets DB Connectivity	335
Oracle Data Safe: Target Database Connectivity	336
Oracle Data Safe: Public Endpoint Connectivity	337
Oracle Data Safe: Private Endpoint Connectivity	338
Oracle Data Safe: Using on-premises Connectors	339
Module 17	340
What is Cloud Security Posture Management?	340
Problem with Cloud Security	341
Cloud Security Posture Management (CSPM) capabilities	342
DevSecOps	343
Cloud Security Posture Management Outcomes	344
Cloud Security Posture Management Benefits	345
Cloud Guard Introduction	346
Cloud Guard	347
Supported Services	349
CIS OCI Foundations Benchmark	350
Reporting Region	351
Demo: Enable Cloud Guard	352
Cloud Guard Concepts	353
Cloud Guard: Overview	354

Cloud Guard Concepts: Targets and Detectors	355
Cloud Guard Concepts: Detector Rules and Recipes	356
Cloud Guard Concepts: Problems and Responders	357
Cloud Guard Concepts: Responder Rules and Recipes	358
Cloud Guard Problems	359
Scenario: Public Bucket	360
Cloud Guard Concepts: Problems	361
Processing Reported Problems	362
Cloud Guard – Manage Detector Recipes	364
Detector Rules and Recipes	365
Configuration Detector Rules (Oracle-Managed)	366
Activity Detector Rules (Oracle-managed)	367
Compartment Inheritance	368
Cloud Guard Responder Recipes	369
Managing Responder Recipes	370
Managed Lists	372
Cloud Guard Notifications	374
Cloud Guard Notifications	375
Integration with Events and Notification Services	376
Demo: Cloud Guard	377
Demo: Cloud Guard Notifications	378
Module 18	379
OCI Threat Intelligence Service	379
What is Threat Intelligence?	380
Two Pillars of Threat Detection	382
OCI Threat Intelligence Service	383
Threat Intelligence Concepts	384
Demo: Threat Indicator Database	385

Cloud Guard Threat Detector	386
Threat Intelligence Integration with Cloud Guard	387
Sighting Type Reference	388
Cloud Guard Threat Detector	389
Threat Detection	390
Benefits	391
Demo: Cloud Guard Threat Detector	392
Security Zones and Security Advisor	393
Security Zones	394
Security Zone Concepts	396
Security Zone Policies	397
Security Advisor	398
Demo: Security Zones and Advisor	399
Demo: Custom Security Zones	400
Module 19	401
Managing Security Operations	401
Your Top Priorities Within Security	402
Observability and Management: Introduction	403
Key Services	404
Monitoring Service ~ Getting Started	405
OCI Monitoring Service: Overview	406
Monitoring Capabilities	407
Monitoring Service Workflow	408
Demo: Monitoring	409
Logging Service	410
OCI Logging Service	411
Log Groups	412

Logging Concepts	413
Types of Logs	414
Searching Logs	415
Viewing Audit Log Events	416
IAM Policies Required	417
Service Flow	418
Demo: Logging Service and Audit Events	419
Ingesting Logs for Analytics	420
Ingesting Logs from Sources	421
Ingesting Logs from Sources: Compute Instance	422
Ingesting Logs from Sources: Object Storage	423
Ingesting Logs from Sources: OCI Cloud Services	424
Ingesting Logs from Sources: On-Demand Upload	425
What is a management agent?	426
Management Agent Installation: Workflow	427
Management Agent Installation: Verify OCI Environment	428
Management Agent Installation: Prerequisites	429
Management Agent Installation: Agent Install Key	430
Management Agent Installation: Installing Agent	431
How Does Service Connector Help with Ingestion?	432
Configuration Parameters	433
Ingestion with Object Storage	434
Insights with Logging Analytics	436
An Overview of Logging Analytics	437
Logging Analytics Answers Security Posture Questions	438
Architecture □ Concepts & Terms	439
Storage and Log Archiving	440
Log Explorer to Filter, Query, and Visualize	441

Dashboards	442
OCI Audit Analysis Dashboard	443
Advanced Analysis with Log Clustering	444
Audit Service	445
OCI Audit Service	446
Audit Log	447
Viewing Audit Log Events	448
Reasons to use Audit logs	449
Required IAM policies	450
Demo: Logging Analytics with Management Agent Log Ingestion	451
Notifications Service - Observability and Management – Monitoring	452
Notifications Service - Overview	453
Notifications Service: Creating a Topic	454
Rule Action Type: Notifications	455
Events Service	456
Overview	457
OCI Events Service Concepts	461
What is an Event?	462
What does an Event look like?	463
Services That Produce Events	464
OCI Service Event Types	465
What are Rules?	466
Creating Rules	467
Events Metrics	468
An Example of OCI Events Service in Action	469
Demo: Notifications and Events Service	470