CENGAGE

NETWORKING

CompTIA Cloud+ Guide to Cloud Computing

Jill West

CompTIA Cloud+

Guide to Cloud Computing

JILL WEST

NETWORKING

CENGAGE

Australia • Brazil • Canada • Mexico • Singapore • United Kingdom • United States

CENGAGE

CompTIA Cloud+
Guide to Cloud Computing
Jill West

Higher Education Product Management: Erin Joyner SVP

Product Management: Mike Schenk VP

Product Director: Lauren Murphy

Product Team Manager: Kristin McNary

Product Manager: Amy Savino

Product Assistant: Tom Benedetto

Director, Learning Design: Rebecca von Gillern

Senior Manager, Learning Design: Leigh Hefferon

Learning Designer: Natalie Onderdonk

Vice President, Marketing—Science, Technology, & Math: Jason Sakos

Senior Marketing Director: Michele McTighe

Marketing Manager: Cassie Cloutier

Senior Market Development Manager: Sam Best

Product Specialist: Mackenzie Paine

Director, Content Creation: Juliet Steiner

Senior Manager, Content Creation: Patty Stephan

Senior Content Manager: Maria Garguilo

Director, Digital Production Services: Krista Kellman

Digital Delivery Lead: Jim Vaughey

Technical Editor: John Freitas

Developmental Editor: Lisa Ruffolo

Production Service/Composition: SPi Global

Design Director: Jack Pendleton

Designer: Erin Griffin

Library of Congress Control Number: 2020919524

ISBN: 978-0-357-54139-5

Cengage
200 Pier 4 Boulevard
Boston, MA 02210

Cengage is a leading provider of customized learning solutions with employees residing in nearly 40 different countries and sales in more than 125 countries around the world. Find your local representative at: **www.cengage.com.**

To learn more about Cengage platforms and services, register or access your online learning solution, or purchase materials for your course, visit **www.cengage.com.**

Printed in Mexico
Print Number: 01 Print Year: 2020

BRIEF CONTENTS

TABLE OF CONTENTS

COMPTIA CLOUD+ EXAM OBJECTIVES MAPPED TO MODULES

These tables provide a complete list of the latest CompTIA Cloud+ CV0-002 certification exam objectives. The official list of objectives is available at CompTIA's website, comptia.org. For your reference, the following tables list each exam objective and the module and section that explains the objective, plus the amount of the exam that will cover each certification domain.

DOMAIN 1.0 CONFIGURATION AND DEPLOYMENT—24 PERCENT OF EXAMINATION

1.1 Given a scenario, analyze system requirements to ensure successful system deployment.

Objective	Module	Section
• Appropriate commands, structure, tools, and automation/orchestration as needed	3	Section 3-1: Migration Planning Section 3-2: Migration Execution
• Platforms and applications	2 3	Section 2-5: VM Migrations Section 3-1: Migration Planning Section 3-2: Migration Execution
• Interaction of cloud components and services	1	Section 1-3: Cloud Service Models Section 1-4: Cloud Service Providers
• Network components	1	Section 1-3: Cloud Service Models Section 1-4: Cloud Service Providers
• Application components	1	Section 1-3: Cloud Service Models Section 1-4: Cloud Service Providers
• Storage components	1	Section 1-3: Cloud Service Models Section 1-4: Cloud Service Providers
• Compute components	1	Section 1-3: Cloud Service Models Section 1-4: Cloud Service Providers
• Security components	1	Section 1-3: Cloud Service Models Section 1-4: Cloud Service Providers
• Interaction of non-cloud components and services	3	Section 3-1: Migration Planning
• Baselines	3	Section 3-1: Migration Planning
• Target hosts	3	Section 3-1: Migration Planning
• Existing systems	3	Section 3-1: Migration Planning
• Cloud architecture	3	Section 3-1: Migration Planning
• Cloud elements/target objects	3	Section 3-1: Migration Planning

1.2 Given a scenario, execute a provided deployment plan.

Objective	Module	Section
• Apply the change management process	3	Section 3-2: Migration Execution
• Approvals	3	Section 3-2: Migration Execution
• Scheduling	3	Section 3-2: Migration Execution
• Refer to documentation and follow standard operating procedures	3	Section 3-2: Migration Execution
• Execute workflow	3	Section 3-2: Migration Execution
• Configure automation and orchestration, where appropriate, for the system being deployed	3	Section 3-2: Migration Execution
• Use commands and tools as needed	3	Section 3-2: Migration Execution
• Document results	3	Section 3-2: Migration Execution

1.3 Given a scenario, analyze system requirements to determine if a given testing plan is appropriate.

Objective	Module	Section
• Underlying environmental considerations included in the testing plan	3	Section 3-3: Deployment Testing and Validation
• Shared components	3	Section 3-3: Deployment Testing and Validation
• Storage	3	Section 3-3: Deployment Testing and Validation
• Compute	3	Section 3-3: Deployment Testing and Validation
• Network	3	Section 3-3: Deployment Testing and Validation
• Production vs. deployment vs. QA	10	Section 10-1: Automation Workflow
• Sizing	3	Section 3-3: Deployment Testing and Validation
• Performance	3	Section 3-3: Deployment Testing and Validation
• High availability	3	Section 3-3: Deployment Testing and Validation
• Connectivity	3	Section 3-3: Deployment Testing and Validation
• Data integrity	3	Section 3-3: Deployment Testing and Validation
• Proper function	3	Section 3-3: Deployment Testing and Validation
• Replication	3	Section 3-3: Deployment Testing and Validation
• Load balancing	5	Section 5-2: Extending Network Services
• Automation/orchestration	10	Section 10-1: Automation Workflow
• Testing techniques	3	Section 3-3: Deployment Testing and Validation
• Vulnerability testing	3	Section 3-3: Deployment Testing and Validation
• Penetration testing	3	Section 3-3: Deployment Testing and Validation
• Load testing	3	Section 3-3: Deployment Testing and Validation

1.4 Given a scenario, analyze testing results to determine if the testing was successful in relation to given system requirements.

Objective	Module	Section
• Consider success factor indicators of the testing environment	3	Section 3-3: Deployment Testing and Validation
• Sizing	3	Section 3-3: Deployment Testing and Validation
• Performance	3	Section 3-3: Deployment Testing and Validation
• Availability	3	Section 3-3: Deployment Testing and Validation
• Connectivity	3	Section 3-3: Deployment Testing and Validation

Objective	Module	Section
• Data integrity	3	Section 3-3: Deployment Testing and Validation
• Proper functionality	3	Section 3-3: Deployment Testing and Validation
• Document results	3	Section 3-3: Deployment Testing and Validation
• Baseline comparisons	3	Section 3-3: Deployment Testing and Validation
• SLA comparisons	3	Section 3-3: Deployment Testing and Validation
• Cloud performance fluctuation variables	9	Section 9-1: Monitoring Resources

1.5 Given a scenario, analyze sizing, subnetting, and basic routing for a provided deployment of a virtual network.

Objective	Module	Section
• Cloud deployment models	1	Section 1-2: Cloud Deployment Models
• Public	1	Section 1-2: Cloud Deployment Models
• Private	1	Section 1-2: Cloud Deployment Models
• Hybrid	1	Section 1-2: Cloud Deployment Models
• Community	1	Section 1-2: Cloud Deployment Models
• Network components	4	Section 4-1: Networking Concepts in the Cloud Section 4-2: IP Address Spaces
• Applicable port and protocol considerations when extending to the cloud	5	Section 5-1: Hybrid Cloud and Multi-Cloud Networking
• Determine configuration for the applicable platforms as it applies to the network	4	Section 4-2: IP Address Spaces Section 4-3: Networking in AWS Section 4-4: Networking in Azure Section 4-5: Networking in GCP
• VPN	5	Section 5-1: Hybrid Cloud and Multi-Cloud Networking
• IDS/IPS	6	Section 6-2: Virtual Network Security
• DMZ	6	Section 6-2: Virtual Network Security
• VXLAN	5	Section 5-1: Hybrid Cloud and Multi-Cloud Networking
• Address space required	4	Section 4-2: IP Address Spaces
• Network segmentation and microsegmentation	4 5 6	Section 4-3: Networking in AWS Section 4-4: Networking in Azure Section 4-5: Networking in GCP Section 5-1: Hybrid Cloud and Multi-Cloud Networking Section 6-2: Virtual Network Security
• Determine if cloud resources are consistent with the SLA and/or change management requirements	3	Section 3-3: Deployment Testing and Validation

1.6 Given a scenario, analyze CPU and memory sizing for a provided deployment.

Objective	Module	Section
• Available vs. proposed resources	2	Section 2-1: Virtualization Technologies
• CPU	2	Section 2-1: Virtualization Technologies
• RAM	2	Section 2-1: Virtualization Technologies

Objective	Module	Section
• Memory technologies	2	Section 2-3: Virtualized Memory
• Bursting and ballooning	2	Section 2-3: Virtualized Memory
• Overcommitment ratio	2	Section 2-3: Virtualized Memory
• CPU technologies	2	Section 2-2: Virtualized Processing
• Hyperthreading	2	Section 2-2: Virtualized Processing
• VT-x	2	Section 2-2: Virtualized Processing
• Overcommitment ratio	2	Section 2-2: Virtualized Processing
• Effect to HA/DR	2	Section 2-4: Virtual CPU and Memory in the Cloud
• Performance considerations	2	Section 2-2: Virtualized Processing Section 2-3: Virtualized Memory
• Cost considerations	2	Section 2-4: Virtual CPU and Memory in the Cloud
• Energy savings	2	Section 2-4: Virtual CPU and Memory in the Cloud
• Dedicated compute environment vs. shared compute environment	2	Section 2-4: Virtual CPU and Memory in the Cloud

1.7 Given a scenario, analyze the appropriate storage type and protection capability for a provided deployment.

Objective	Module	Section
• Requested IOPS and read/write throughput	8	Section 8-1: Storage Types
• Protection capabilities	8	Section 8-3: Creating and Storing Backups
• High availability	8	Section 8-3: Creating and Storing Backups
• Failover zones	8	Section 8-3: Creating and Storing Backups
• Storage replication	8	Section 8-3: Creating and Storing Backups
• Regional	8	Section 8-3: Creating and Storing Backups
• Multiregional	8	Section 8-3: Creating and Storing Backups
• Synchronous and asynchronous	8	Section 8-3: Creating and Storing Backups
• Storage mirroring	8	Section 8-3: Creating and Storing Backups
• Cloning	8	Section 8-3: Creating and Storing Backups
• Redundancy level/factor	8	Section 8-3: Creating and Storing Backups
• Storage types	8	Section 8-1: Storage Types
• NAS	8	Section 8-1: Storage Types
• DAS	8	Section 8-1: Storage Types
• SAN	8	Section 8-1: Storage Types
• Object storage	8	Section 8-1: Storage Types
• Access protocols	8	Section 8-1: Storage Types
• Management differences	8	Section 8-2: Cloud Storage Services
• Provisioning model	8	Section 8-1: Storage Types
• Thick provisioned	8	Section 8-1: Storage Types
• Thin provisioned	8	Section 8-1: Storage Types
• Encryption requirements	8	Section 8-4: Storage Security
• Tokenization	8	Section 8-4: Storage Security
• Storage technologies	8	Section 8-1: Storage Types
• Deduplication technologies	8	Section 8-1: Storage Types
• Compression technologies	8	Section 8-1: Storage Types

Objective	Module	Section
• Storage tiers	8	Section 8-1: Storage Types Section 8-2: Cloud Storage Services
• Overcommitting storage	8	Section 8-1: Storage Types
• Security configurations for applicable platforms	8	Section 8-2: Cloud Storage Services Section 8-4: Storage Security
• ACLs	8	Section 8-2: Cloud Storage Services Section 8-4: Storage Security
• Obfuscation	8	Section 8-4: Storage Security
• Zoning	8	Section 8-4: Storage Security
• User/host authentication and authorization	8	Section 8-4: Storage Security

1.8 Given a scenario, analyze characteristics of the workload (storage, network, compute) to ensure a successful migration.

Objective	Module	Section
• Migration types	2 3	Section 2-5: VM Migrations Section 3-2: Migration Execution
• P2V	2	Section 2-5: VM Migrations
• V2V	2	Section 2-5: VM Migrations
• V2P	2	Section 2-5: VM Migrations
• P2P	2	Section 2-5: VM Migrations
• Storage migrations	3	Section 3-2: Migration Execution
• Online vs. offline migrations	2 3	Section 2-5: VM Migrations Section 3-2: Migration Execution
• Source and destination format of the workload	2 3	Section 2-5: VM Migrations Section 3-1: Migration Planning Section 3-2: Migration Execution
• Virtualization format	2	Section 2-5: VM Migrations
• Application and data portability	3	Section 3-1: Migration Planning Section 3-2: Migration Execution
• Network connections and data transfer methodologies	3	Section 3-2: Migration Execution
• Standard operating procedures for the workload migration	3	Section 3-1: Migration Planning Section 3-2: Migration Execution
• Environmental constraints	3	Section 3-1: Migration Planning Section 3-2: Migration Execution
• Bandwidth	3	Section 3-2: Migration Execution
• Working hour restrictions	3	Section 3-1: Migration Planning
• Downtime impact	3	Section 3-1: Migration Planning
• Peak time frames	3	Section 3-1: Migration Planning
• Legal restrictions	3	Section 3-1: Migration Planning
• Follow-the-sun constraints/time zones	3	Section 3-1: Migration Planning

1.9 Given a scenario, apply elements required to extend the infrastructure into a given cloud solution.

Objective	Module	Section
• Identity management elements	7	Section 7-4: IAM for Hybrid Clouds
• Identification	7	Section 7-4: IAM for Hybrid Clouds
• Authentication	7	Section 7-4: IAM for Hybrid Clouds
• Authorization	7	Section 7-4: IAM for Hybrid Clouds
• Approvals	7	Section 7-4: IAM for Hybrid Clouds
• Access policy	7	Section 7-4: IAM for Hybrid Clouds
• Federation	7	Section 7-4: IAM for Hybrid Clouds
• Single sign-on	7	Section 7-4: IAM for Hybrid Clouds
• Appropriate protocols given requirements	6	Section 6-2: Virtual Network Security
• Element considerations to deploy infrastructure services such as:	5	Section 5-2: Extending Network Services
• DNS	5	Section 5-2: Extending Network Services
• DHCP	5	Section 5-2: Extending Network Services
• Certificate services	7	Section 7-4: IAM for Hybrid Clouds
• Local agents	9	Section 9-1: Monitoring Resources
• Antivirus	6	Section 6-2: Virtual Network Security
• Load balancer	5	Section 5-2: Extending Network Services
• Multifactor authentication	7	Section 7-4: IAM for Hybrid Clouds
• Firewall	6	Section 6-2: Virtual Network Security
• IPS/IDS	6	Section 6-2: Virtual Network Security

DOMAIN 2.0 SECURITY—16 PERCENT OF EXAMINATION

2.1 Given a scenario, apply security configurations and compliance controls to meet given cloud infrastructure requirements.

Objective	Module	Section
• Company security policies	6	Section 6-1: Security Configurations
• Apply security standards for the selected platform	6	Section 6-2: Virtual Network Security
• Compliance and audit requirements governing the environment	1	Section 1-2: Cloud Deployment Models
• Laws and regulations as they apply to the data	1	Section 1-2: Cloud Deployment Models
• Encryption technologies	6	Section 6-4: Data Security
• IPSec	5	Section 5-1: Hybrid Cloud and Multi-Cloud Networking
• SSL/TLS	6	Section 6-4: Data Security
• Other ciphers	6	Section 6-4: Data Security
• Key and certificate management	6	Section 6-4: Data Security
	7	Section 7-2: Authentication

Objective	Module	Section
• PKI	7	Section 7-2: Authentication
• Tunneling protocols	5	Section 5-1: Hybrid Cloud and Multi-Cloud Networking
• L2TP	5	Section 5-1: Hybrid Cloud and Multi-Cloud Networking
• PPTP	5	Section 5-1: Hybrid Cloud and Multi-Cloud Networking
• GRE	5	Section 5-1: Hybrid Cloud and Multi-Cloud Networking
• Implement automation and orchestration processes as applicable	10	Section 10-1: Automation Workflow
• Appropriate configuration for the applicable platform as it applies to compute	6	Section 6-3: Compute Security
• Disabling unneeded ports and services	6	Section 6-3: Compute Security
• Account management policies	6	Section 6-3: Compute Security
• Host-based/software firewalls	6	Section 6-3: Compute Security
• Antivirus/anti-malware software	6	Section 6-3: Compute Security
• Patching	10	Section 10-2: Cloud Maintenance Processes
• Deactivating default accounts	6 7	Section 6-3: Compute Security Section 7-1: Account Management

2.2 Given a scenario, apply the appropriate ACL to the target objects to meet access requirements according to a security template.

Objective	Module	Section
• Authorization to objects in the cloud	7	Section 7-3: Authorization to Cloud Objects
• Processes	7	Section 7-3: Authorization to Cloud Objects
• Resources	7	Section 7-3: Authorization to Cloud Objects
• Users	7	Section 7-3: Authorization to Cloud Objects
• Groups	7	Section 7-3: Authorization to Cloud Objects
• System	7	Section 7-3: Authorization to Cloud Objects
• Compute	7	Section 7-3: Authorization to Cloud Objects
• Networks	7	Section 7-3: Authorization to Cloud Objects
• Storage	7	Section 7-3: Authorization to Cloud Objects
• Services	7	Section 7-3: Authorization to Cloud Objects
• Effect of cloud service models on security implementations	1	Section 1-3: Cloud Service Models
• Effect of cloud deployment models on security implementations	1	Section 1-2: Cloud Deployment Models
• Access control methods	7	Section 7-2: Authentication Section 7-3: Authorization to Cloud Objects
• Role-based administration	7	Section 7-3: Authorization to Cloud Objects
• Mandatory access controls	7	Section 7-3: Authorization to Cloud Objects
• Discretionary access controls	7	Section 7-3: Authorization to Cloud Objects
• Non-discretionary access controls	7	Section 7-3: Authorization to Cloud Objects
• Multifactor authentication	7	Section 7-2: Authentication
• Single sign-on	7	Section 7-2: Authentication

2.3 Given a cloud service model, implement defined security technologies to meet given security requirements.

Objective	Module	Section
• Data classification	7	Section 7-3: Authorization to Cloud Objects
• Concepts of segmentation and microsegmentation	4	Section 4-3: Networking in AWS Section 4-4: Networking in Azure Section 4-5: Networking in GCP
	6	Section 6-1: Security Configurations
• Network	4	Section 4-3: Networking in AWS Section 4-4: Networking in Azure Section 4-5: Networking in GCP
• Storage	8	Section 8-4: Storage Security
• Compute	4	Section 4-3: Networking in AWS Section 4-4: Networking in Azure Section 4-5: Networking in GCP
• Use encryption as defined	6	Section 6-4: Data Security
• Use multifactor authentication as defined	7	Section 7-2: Authentication
• Apply defined audit/compliance requirements	7	Section 7-1: Account Management

2.4 Given a cloud service model, apply the appropriate security automation techniques to the target system.

Objective	Module	Section
• Tools	10	Section 10-1: Automation Workflow
• APIs	10	Section 10-1: Automation Workflow
• Vendor applications	10	Section 10-1: Automation Workflow
• CLI	10	Section 10-1: Automation Workflow
• Web GUI	10	Section 10-1: Automation Workflow
• Cloud portal	10	Section 10-1: Automation Workflow
• Techniques	10	Section 10-1: Automation Workflow
• Orchestration	10	Section 10-1: Automation Workflow
• Scripting	10	Section 10-1: Automation Workflow
• Custom programming	10	Section 10-1: Automation Workflow
• Security services	10	Section 10-3: Security Automation
• Firewall	10	Section 10-3: Security Automation
• Antivirus/anti-malware	10	Section 10-3: Security Automation
• IPS/IDS	10	Section 10-3: Security Automation
• HIPS	10	Section 10-3: Security Automation
• Impact of security tools to systems and services	10	Section 10-3: Security Automation
• Scope of impact	10	Section 10-3: Security Automation
• Impact of security automation techniques as they relate to the criticality of systems	10	Section 10-3: Security Automation
• Scope of impact	10	Section 10-3: Security Automation

DOMAIN 3.0 MAINTENANCE—18 PERCENT OF EXAMINATION

3.1 Given a cloud service model, determine the appropriate methodology to apply given patches.

Objective	Module	Section
• Scope of cloud elements to be patched	10	Section 10-2: Cloud Maintenance Processes
• Hypervisors	10	Section 10-2: Cloud Maintenance Processes
• Virtual machines	10	Section 10-2: Cloud Maintenance Processes
• Virtual appliances	10	Section 10-2: Cloud Maintenance Processes
• Networking components	10	Section 10-2: Cloud Maintenance Processes
• Applications	10	Section 10-2: Cloud Maintenance Processes
• Storage components	10	Section 10-2: Cloud Maintenance Processes
• Clusters	10	Section 10-2: Cloud Maintenance Processes
• Patching methodologies and standard operating procedures	10	Section 10-1: Automation Workflow Section 10-2: Cloud Maintenance Processes
• Production vs. development vs. QA	10	Section 10-1: Automation Workflow
• Rolling update	10	Section 10-2: Cloud Maintenance Processes
• Blue-green deployment	10	Section 10-1: Automation Workflow Section 10-2: Cloud Maintenance Processes
• Failover cluster	10	Section 10-2: Cloud Maintenance Processes
• Use order of operations as it pertains to elements that will be patched	10	Section 10-2: Cloud Maintenance Processes
• Dependency considerations	10	Section 10-2: Cloud Maintenance Processes

3.2 Given a scenario, apply the appropriate automation tools to update cloud elements.

Objective	Module	Section
• Types of updates	10	Section 10-2: Cloud Maintenance Processes
• Hotfix	10	Section 10-2: Cloud Maintenance Processes
• Patch	10	Section 10-2: Cloud Maintenance Processes
• Version update	10	Section 10-2: Cloud Maintenance Processes
• Rollback	10	Section 10-2: Cloud Maintenance Processes
• Automation workflow	10	Section 10-1: Automation Workflow
• Runbook management	10	Section 10-1: Automation Workflow
• Single node	10	Section 10-1: Automation Workflow
• Orchestration	10	Section 10-1: Automation Workflow
• Multiple nodes	10	Section 10-1: Automation Workflow
• Multiple runbooks	10	Section 10-1: Automation Workflow
• Activities to be performed by automation tools	10	Section 10-1: Automation Workflow
• Snapshot	10	Section 10-1: Automation Workflow
• Cloning	10	Section 10-1: Automation Workflow
• Patching	10	Section 10-1: Automation Workflow
• Restarting	10	Section 10-1: Automation Workflow

Objective	Module	Section
• Shut down	10	Section 10-1: Automation Workflow
• Maintenance mode	10	Section 10-1: Automation Workflow
• Enable/disable alerts	10	Section 10-1: Automation Workflow

3.3 Given a scenario, apply an appropriate backup or restore method.

Objective	Module	Section
• Backup types	8	Section 8-3: Creating and Storing Backups
• Snapshot/redirect-on-write	8	Section 8-3: Creating and Storing Backups
• Clone	8	Section 8-3: Creating and Storing Backups
• Full	8	Section 8-3: Creating and Storing Backups
• Differential	8	Section 8-3: Creating and Storing Backups
• Incremental	8	Section 8-3: Creating and Storing Backups
• Change block/delta tracking	8	Section 8-3: Creating and Storing Backups
• Backup targets	8	Section 8-3: Creating and Storing Backups
• Replicas	8	Section 8-3: Creating and Storing Backups
• Local	8	Section 8-3: Creating and Storing Backups
• Remote	8	Section 8-3: Creating and Storing Backups
• Other considerations	8	Section 8-3: Creating and Storing Backups
• SLAs	8	Section 8-3: Creating and Storing Backups
• Backup schedule	8	Section 8-3: Creating and Storing Backups
• Configurations	8	Section 8-3: Creating and Storing Backups
• Objects	8	Section 8-3: Creating and Storing Backups
• Dependencies	8	Section 8-3: Creating and Storing Backups
• Online/offline	8	Section 8-3: Creating and Storing Backups

3.4 Given a cloud-based scenario, apply appropriate disaster recovery methods.

Objective	Module	Section
• DR capabilities of a cloud service provider	9	Section 9-4: Planning for Problems
• Other considerations	9	Section 9-4: Planning for Problems
• SLAs for DR	9	Section 9-4: Planning for Problems
• RPO	9	Section 9-4: Planning for Problems
• RTO	9	Section 9-4: Planning for Problems
• Corporate guidelines	9	Section 9-4: Planning for Problems
• Cloud service provider guidelines	9	Section 9-4: Planning for Problems
• Bandwidth or ISP limitations	9	Section 9-4: Planning for Problems
• Techniques	9	Section 9-4: Planning for Problems
• Site mirroring	9	Section 9-4: Planning for Problems
• Replication	9	Section 9-4: Planning for Problems
• File transfer	9	Section 9-4: Planning for Problems
• Archiving	9	Section 9-4: Planning for Problems
• Third-party sites	9	Section 9-4: Planning for Problems

3.5 Given a cloud-based scenario, apply the appropriate steps to ensure business continuity.

Objective	Module	Section
• Business continuity plan	9	Section 9-4: Planning for Problems
• Alternate sites	9	Section 9-4: Planning for Problems
• Continuity of operations	9	Section 9-4: Planning for Problems
• Connectivity	9	Section 9-4: Planning for Problems
• Edge sites	9	Section 9-4: Planning for Problems
• Equipment	9	Section 9-4: Planning for Problems
• Availability	9	Section 9-4: Planning for Problems
• Partners/third parties	9	Section 9-4: Planning for Problems
• SLAs for BCP and HA	9	Section 9-3: Cloud Optimization

3.6 Given a scenario, apply the appropriate maintenance automation techniques to the target objects.

Objective	Module	Section
• Maintenance schedules	10	Section 10-2: Cloud Maintenance Processes
• Impact and scope of maintenance tasks	10	Section 10-2: Cloud Maintenance Processes
• Impact and scope of maintenance automation techniques	10	Section 10-2: Cloud Maintenance Processes
• Include orchestration as appropriate	10	Section 10-2: Cloud Maintenance Processes
• Maintenance automation tasks	10	Section 10-2: Cloud Maintenance Processes
• Clearing logs	10	Section 10-2: Cloud Maintenance Processes
• Archiving logs	10	Section 10-2: Cloud Maintenance Processes
• Compressing drives	10	Section 10-2: Cloud Maintenance Processes
• Removing inactive accounts	10	Section 10-2: Cloud Maintenance Processes
• Removing stale DNS entries	10	Section 10-2: Cloud Maintenance Processes
• Removing orphaned resources	10	Section 10-2: Cloud Maintenance Processes
• Removing outdated rules from firewall	10	Section 10-2: Cloud Maintenance Processes
• Removing outdated rules from security	10	Section 10-2: Cloud Maintenance Processes
• Resource reclamation	10	Section 10-2: Cloud Maintenance Processes
• Maintain ACLs for the target object	10	Section 10-2: Cloud Maintenance Processes

DOMAIN 4.0 MANAGEMENT—20 PERCENT OF EXAMINATION

4.1 Given a scenario, analyze defined metrics to determine the presence of an abnormality and/or forecast future needed cloud resources.

Objective	Module	Section
• Monitoring	9	Section 9-1: Monitoring Resources Section 9-2: Analysis and Response
• Target object baselines	9	Section 9-2: Analysis and Response
• Target object anomalies	9	Section 9-2: Analysis and Response

Objective	Module	Section
• Common alert methods/messaging	9	Section 9-2: Analysis and Response
• Alerting based on deviation from baseline	9	Section 9-2: Analysis and Response
• Event collection	9	Section 9-1: Monitoring Resources
• Event correlation	9	Section 9-1: Monitoring Resources
• Forecasting resource capacity	9	Section 9-3: Cloud Optimization
• Upsize/increase	9	Section 9-3: Cloud Optimization
• Downsize/decrease	9	Section 9-3: Cloud Optimization
• Policies in support of event collection	9	Section 9-1: Monitoring Resources
• Policies to communicate alerts appropriately	9	Section 9-2: Analysis and Response

4.2 Given a scenario, determine the appropriate allocation of cloud resources.

Objective	Module	Section
• Resources needed based on cloud deployment models	1	Section 1-2: Cloud Deployment Models
• Hybrid	1	Section 1-2: Cloud Deployment Models
• Community	1	Section 1-2: Cloud Deployment Models
• Public	1	Section 1-2: Cloud Deployment Models
• Private	1	Section 1-2: Cloud Deployment Models
• Capacity/elasticity of cloud environment	9	Section 9-1: Monitoring Resources
• Support agreements	10	Section 10-2: Cloud Maintenance Processes
• Cloud service model maintenance responsibility	10	Section 10-2: Cloud Maintenance Processes
• Configuration management tool	10	Section 10-1: Automation Workflow
• Resource balancing techniques	9	Section 9-3: Cloud Optimization
• Change management	3	Section 3-2: Migration Execution
• Advisory board	3	Section 3-2: Migration Execution
• Approval process	3	Section 3-2: Migration Execution
• Document actions taken	3	Section 3-2: Migration Execution
• CMDB	3	Section 3-2: Migration Execution
• Spreadsheet	3	Section 3-2: Migration Execution

4.3 Given a scenario, determine when to provision/deprovision cloud resources.

Objective	Module	Section
• Usage patterns	9	Section 9-1: Monitoring Resources
• Cloud bursting	9	Section 9-2: Analysis and Response
• Auto-scaling technology	9	Section 9-2: Analysis and Response
• Cloud provider migrations	3	Section 3-1: Migration Planning
• Extending cloud scope	3	Section 3-1: Migration Planning
• Application lifecycle	3	Section 3-5: Increasing Agility
• Application deployment	3	Section 3-5: Increasing Agility
• Application upgrade	3	Section 3-5: Increasing Agility
• Application retirement	3	Section 3-5: Increasing Agility
• Application replacement	3	Section 3-5: Increasing Agility

Objective	Module	Section
• Application migration	3	Section 3-5: Increasing Agility
• Application feature use	3	Section 3-5: Increasing Agility
• Increase/decrease	3	Section 3-5: Increasing Agility
• Business need change	1	Section 1-1: Characteristics of Cloud Computing
• Mergers/acquisitions/divestitures	1	Section 1-1: Characteristics of Cloud Computing
• Cloud service requirement changes	1	Section 1-1: Characteristics of Cloud Computing
• Impact of regulation and law changes	1	Section 1-1: Characteristics of Cloud Computing

4.4 Given a scenario, implement account-provisioning techniques in a cloud environment to meet security and policy requirements.

Objective	Module	Section
• Identification	7	Section 7-1: Account Management
• Authentication methods	7	Section 7-2: Authentication
• Federation	7	Section 7-2: Authentication
• Single sign-on	7	Section 7-2: Authentication
• Authorization methods	7	Section 7-3: Authorization to Cloud Objects
• ACLs	7	Section 7-3: Authorization to Cloud Objects
• Permissions	7	Section 7-3: Authorization to Cloud Objects
• Account lifecycle	7	Section 7-1: Account Management
• Account management policy	7	Section 7-1: Account Management Section 7-2: Authentication
• Lockout	7	Section 7-1: Account Management
• Password complexity rules	7	Section 7-2: Authentication
• Automation and orchestration activities	10	Section 10-3: Security Automation
• User account creation	10	Section 10-3: Security Automation
• Permission settings	10	Section 10-3: Security Automation
• Resource access	10	Section 10-3: Security Automation
• User account removal	10	Section 10-3: Security Automation
• User account disablement	10	Section 10-3: Security Automation

4.5 Given a scenario, analyze deployment results to confirm they meet the baseline.

Objective	Module	Section
• Procedures to confirm results	3	Section 3-3: Deployment Testing and Validation
• CPU usage	3	Section 3-3: Deployment Testing and Validation
• RAM usage	3	Section 3-3: Deployment Testing and Validation
• Storage utilization	3	Section 3-3: Deployment Testing and Validation
• Patch versions	3	Section 3-3: Deployment Testing and Validation
• Network utilization	3	Section 3-3: Deployment Testing and Validation
• Application version	3	Section 3-3: Deployment Testing and Validation
• Auditing enable	3	Section 3-3: Deployment Testing and Validation
• Management tool compliance	3	Section 3-3: Deployment Testing and Validation

4.6 Given a specific environment and related data (e.g., performance, capacity, trends), apply appropriate changes to meet expected criteria.

Objective	Module	Section
• Analyze performance trends	9	Section 9-3: Cloud Optimization
• Refer to baselines	9	Section 9-3: Cloud Optimization
• Refer to SLAs	9	Section 9-3: Cloud Optimization
• Tuning of cloud target objects	9	Section 9-3: Cloud Optimization
• Compute	9	Section 9-3: Cloud Optimization
• Network	9	Section 9-3: Cloud Optimization
• Storage	9	Section 9-3: Cloud Optimization
• Service/application resources	9	Section 9-3: Cloud Optimization
• Recommend changes to meet expected performance/capacity	9	Section 9-3: Cloud Optimization
• Scale up/down (vertically)	9	Section 9-3: Cloud Optimization
• Scale in/out (horizontally)	9	Section 9-3: Cloud Optimization

4.7 Given SLA requirements, determine the appropriate metrics to report.

Objective	Module	Section
• Chargeback/showback models	9	Section 9-1: Monitoring Resources
• Reporting based on company policies	9	Section 9-1: Monitoring Resources
• Reporting based on SLAs	9	Section 9-1: Monitoring Resources
• Dashboard and reporting	9	Section 9-1: Monitoring Resources Section 9-2: Analysis and Response
• Elasticity usage	9	Section 9-1: Monitoring Resources
• Connectivity	9	Section 9-1: Monitoring Resources
• Latency	9	Section 9-1: Monitoring Resources
• Capacity	9	Section 9-1: Monitoring Resources
• Overall utilization	9	Section 9-1: Monitoring Resources
• Cost	9	Section 9-1: Monitoring Resources
• Incidents	9	Section 9-1: Monitoring Resources
• Health	9	Section 9-1: Monitoring Resources
• System availability	9	Section 9-1: Monitoring Resources
• Uptime	9	Section 9-1: Monitoring Resources
• Downtime	9	Section 9-1: Monitoring Resources

DOMAIN 5.0 TROUBLESHOOTING—22 PERCENT OF EXAMINATION

5.1 Given a scenario, troubleshoot a deployment issue.

Objective	Module	Section
• Common issues in the deployments	3	Section 3-4: Troubleshooting the Deployment
• Breakdowns in the workflow	10	Section 10-4: Troubleshooting Automation Issues

Objective	Module	Section
• Integration issues related to different cloud platforms	3	Section 3-4: Troubleshooting the Deployment
• Resource contention	3	Section 3-4: Troubleshooting the Deployment
• Connectivity issues	5	Section 5-3: Troubleshooting Cloud Connectivity
• Cloud service provider outage	3	Section 3-4: Troubleshooting the Deployment
• Licensing outages	3	Section 3-4: Troubleshooting the Deployment
• Template misconfiguration	3	Section 3-4: Troubleshooting the Deployment
• Time synchronization issues	3	Section 3-4: Troubleshooting the Deployment
• Language support	3	Section 3-4: Troubleshooting the Deployment
• Automation issues	10	Section 10-4: Troubleshooting Automation Issues

5.2 Given a scenario, troubleshoot common capacity issues.

Objective	Module	Section
• Exceeded cloud capacity boundaries	9	Section 9-3: Cloud Optimization
• Compute	9	Section 9-3: Cloud Optimization
• Storage	9	Section 9-3: Cloud Optimization
• Networking	9	Section 9-3: Cloud Optimization
• IP address limitations	9	Section 9-3: Cloud Optimization
• Bandwidth limitations	9	Section 9-3: Cloud Optimization
• Licensing	9	Section 9-3: Cloud Optimization
• Variance in number of users	9	Section 9-3: Cloud Optimization
• API request limit	9	Section 9-3: Cloud Optimization
• Batch job scheduling issues	10	Section 10-4: Troubleshooting Automation Issues
• Deviation from original baseline	9	Section 9-3: Cloud Optimization
• Unplanned expansions	9	Section 9-3: Cloud Optimization

5.3 Given a scenario, troubleshoot automation/orchestration issues.

Objective	Module	Section
• Breakdowns in workflow	10	Section 10-4: Troubleshooting Automation Issues
• Account mismatch issues	10	Section 10-4: Troubleshooting Automation Issues
• Change management failure	10	Section 10-4: Troubleshooting Automation Issues
• Server name changes	10	Section 10-4: Troubleshooting Automation Issues
• IP address changes	10	Section 10-4: Troubleshooting Automation Issues
• Location changes	10	Section 10-4: Troubleshooting Automation Issues
• Version/feature mismatch	10	Section 10-4: Troubleshooting Automation Issues
• Automation tool incompatibility	10	Section 10-4: Troubleshooting Automation Issues
• Job validation issue	10	Section 10-4: Troubleshooting Automation Issues

5.4 Given a scenario, troubleshoot connectivity issues.

Objective	Module	Section
• Common networking issues	5	Section 5-1: Hybrid Cloud and Multi-Cloud Networking Section 5-3: Troubleshooting Cloud Connectivity
• Incorrect subnet	5	Section 5-3: Troubleshooting Cloud Connectivity
• Incorrect IP address	5	Section 5-3: Troubleshooting Cloud Connectivity

Objective	Module	Section
• Incorrect gateway	5	Section 5-3: Troubleshooting Cloud Connectivity
• Incorrect routing	5	Section 5-3: Troubleshooting Cloud Connectivity
• DNS errors	5	Section 5-3: Troubleshooting Cloud Connectivity
• QoS issues	5	Section 5-3: Troubleshooting Cloud Connectivity
• Misconfigured VLAN or VXLAN	5	Section 5-1: Hybrid Cloud and Multi-Cloud Networking
• Misconfigured firewall rule	5	Section 5-3: Troubleshooting Cloud Connectivity
• Insufficient bandwidth	5	Section 5-3: Troubleshooting Cloud Connectivity
• Latency	5	Section 5-3: Troubleshooting Cloud Connectivity
• Misconfigured MTU/MSS	5	Section 5-1: Hybrid Cloud and Multi-Cloud Networking
• Misconfigured proxy	5	Section 5-3: Troubleshooting Cloud Connectivity
• Network tool outputs	5	Section 5-3: Troubleshooting Cloud Connectivity
• Network connectivity tools	5	Section 5-3: Troubleshooting Cloud Connectivity
• ping	5	Section 5-3: Troubleshooting Cloud Connectivity
• tracert/traceroute	5	Section 5-3: Troubleshooting Cloud Connectivity
• telnet	5	Section 5-3: Troubleshooting Cloud Connectivity
• netstat	5	Section 5-3: Troubleshooting Cloud Connectivity
• nslookup/dig	5	Section 5-3: Troubleshooting Cloud Connectivity
• ipconfig/ifconfig	5	Section 5-3: Troubleshooting Cloud Connectivity
• route	5	Section 5-3: Troubleshooting Cloud Connectivity
• arp	5	Section 5-3: Troubleshooting Cloud Connectivity
• ssh	5	Section 5-3: Troubleshooting Cloud Connectivity
• tcpdump	5	Section 5-3: Troubleshooting Cloud Connectivity
• Remote access tools for troubleshooting	5	Section 5-3: Troubleshooting Cloud Connectivity

5.5 Given a scenario, troubleshoot security issues.

Objective	Module	Section
• Authentication issues	7	Section 7-5: Troubleshooting Cloud IAM
• Account lockout/expiration	7	Section 7-5: Troubleshooting Cloud IAM
• Authorization issues	7	Section 7-5: Troubleshooting Cloud IAM
• Federation and single sign-on issues	7	Section 7-5: Troubleshooting Cloud IAM
• Certificate expiration	7	Section 7-5: Troubleshooting Cloud IAM
• Certification misconfiguration	7	Section 7-5: Troubleshooting Cloud IAM
• External attacks	6	Section 6-1: Security Configurations
• Internal attacks	6	Section 6-1: Security Configurations
• Privilege escalation	7	Section 7-5: Troubleshooting Cloud IAM
• Internal role change	7	Section 7-5: Troubleshooting Cloud IAM
• External role change	7	Section 7-5: Troubleshooting Cloud IAM
• Security device failure	6	Section 6-5: Troubleshooting Cloud Security
• Incorrect hardening settings	6	Section 6-5: Troubleshooting Cloud Security
• Unencrypted communication	6	Section 6-5: Troubleshooting Cloud Security
• Unauthorized physical access	6	Section 6-5: Troubleshooting Cloud Security
• Unencrypted data	6	Section 6-5: Troubleshooting Cloud Security

Objective	Module	Section
• Weak or obsolete security technologies	6	Section 6-5: Troubleshooting Cloud Security
• Insufficient security controls and processes	6	Section 6-5: Troubleshooting Cloud Security
• Tunneling or encryption issues	6	Section 6-5: Troubleshooting Cloud Security

5.6 Given a scenario, explain the troubleshooting methodology.

Objective	Module	Section
• Always consider corporate policies, procedures, and impacts before implementing changes	1	Section 1-5: Troubleshooting Methodology
• 1. Identify the problem	1	Section 1-5: Troubleshooting Methodology
• Question the user and identify user changes to computer and perform backups before making changes	1	Section 1-5: Troubleshooting Methodology
• 2. Establish a theory of probable cause (question the obvious)	1	Section 1-5: Troubleshooting Methodology
• If necessary, conduct internal or external research based on symptoms	1	Section 1-5: Troubleshooting Methodology
• 3. Test the theory to determine cause	1	Section 1-5: Troubleshooting Methodology
• Once theory is confirmed, determine the next steps to resolve the problem	1	Section 1-5: Troubleshooting Methodology
• If the theory is not confirmed, reestablish a new theory or escalate	1	Section 1-5: Troubleshooting Methodology
• 4. Establish a plan of action to resolve the problem and implement the solution	1	Section 1-5: Troubleshooting Methodology
• 5. Verify full system functionality, and if applicable, implement preventive measures	1	Section 1-5: Troubleshooting Methodology
• 6. Document findings, actions, and outcomes	1	Section 1-5: Troubleshooting Methodology

PREFACE

CompTIA Cloud+ Guide to Cloud Computing, 1st edition, is intended to serve the needs of students and professionals who are interested in mastering fundamental, vendor-independent cloud computing concepts. No previous cloud computing experience is necessary to begin learning from this course, although knowledge of basic computer, networking, and security principles is helpful. Those seeking to pass CompTIA's Cloud+ certification exam will find the course's content, approach, and numerous projects and study questions especially helpful. For more information on CompTIA® Cloud+ certification, visit CompTIA's website at *comptia.org*.

MODULE DESCRIPTIONS

The following list summarizes the topics covered in each module of this course:

Module 1, "Introduction to Cloud Computing," gives an initial overview of foundational cloud computing concepts, beginning with a survey of cloud certifications, a review of characteristics that define cloud computing, and a description of how an IT professional must adapt existing skills to succeed in a career focused on cloud technologies. The module then compares cloud deployment models (such as public cloud and hybrid cloud), cloud service models (such as PaaS and IaaS), and security concerns specific to each of these models. Finally, the module introduces popular cloud platforms, such as AWS (Amazon Web Services), Microsoft Azure, and GCP (Google Cloud Platform), and reviews sound troubleshooting methodology.

Module 2, "Virtual Hardware," begins with a description of virtualization technologies, including a thorough comparison of type 1 and type 2 hypervisors. The module then takes a deep dive into VM (virtual machine) configuration parameters, especially virtualized processing and virtual memory. It then applies these concepts specifically to the context of cloud computing, followed by a survey of VM allocation factors and VM alternative technologies such as serverless computing and containers. The module concludes with coverage of VM migration techniques and considerations.

Module 3, "Migration to the Cloud," focuses on how to get existing resources into the cloud. The module explores factors to be considered before, during, and after migration, including a comparison of migration strategies (such as lift-and-shift and lift-tinker-and-shift), and the timing of migration tasks that might affect user experience. Related migration topics include documentation, change management processes, and data transfer technologies. The module proceeds to discuss types of testing used to help the migration go smoothly. It then concludes with a synopsis of common problems encountered during migration as well as CLI (command-line interface) tools available in popular cloud platforms for addressing these problems.

Module 4, "Cloud Infrastructure," initiates the discussion of cloud-based networking concepts with a comparison of the OSI Model and the cloud stack. The module includes a review of IP addressing and subnetting concepts followed by an exploration of networking services in AWS, Azure, and GCP. These sections include a thorough discussion of concepts such as regions, availability zones, VPCs (virtual private clouds), VNets (virtual networks), subnetting in the cloud, and the use of gateways and route tables to manage cloud traffic.

Module 5, "Cloud Connectivity and Troubleshooting," continues the cloud networking discussion with an exploration of technologies that connect the on-prem network with cloud-based resources. Network segmentation on-prem is contrasted with network segmentation in the cloud. The module explores technologies available to extend networking services across a hybrid or multi-cloud, such as DHCP, DNS, routing, and load balancing. It concludes with an overview of available CLI commands used to troubleshoot cloud connectivity as well as situations where these tools might be useful.

Module 6, "Securing Cloud Resources," introduces security-related threats specific to cloud computing. While security is addressed throughout most of the modules, this module brings additional focus to cloud-based security strategies. The module highlights concerns and techniques specific to virtual network security, compute security, and data security, followed by an overview of common security weak spots in the cloud.

Module 7, "Identity and Access Management," furthers the security discussion with thorough coverage of IAM (identity and access management) techniques used to control access to cloud resources. The module covers account types that offer identity services to human users and application or cloud services, followed by a thorough discussion of authentication technologies and tools used in a cloud environment. Continuing with the theme of the three-tiered AAA (authentication, authorization, and accounting) approach to network access control, the module then explores options for managing authorization and permissions in AWS, Azure, and GCP. The module concludes with a brief discussion of how to extend IAM across a hybrid cloud as well as common IAM troubleshooting issues.

Module 8, "Cloud Storage," explains common storage technologies both on-prem and in the cloud, followed by storage optimization techniques. The module then highlights popular storage services in AWS, Azure, and GCP. It continues with an exploration of common backup types and techniques, including clones, snapshots, and redundancy levels. The module concludes with an emphasis on the security of cloud-hosted data storage.

Module 9, "Managing Cloud Capacity and Performance," illustrates the need for effective monitoring techniques in the cloud along with an introduction to the benefits realized when automating cloud management tasks. Following a comparison of data collection tools—such as metrics, events, and logs—the module continues with coverage of analysis and response tools available in AWS, Azure, and GCP. A discussion of the inherent limitations of cloud capacity emphasizes the need for capacity planning. The topic of planning ahead is then expanded to include considerations for business continuity and disaster recovery.

Module 10, "Cloud Automation," rounds out the foundations of cloud computing with further exploration into the possibilities and sheer necessity of using automation techniques in the cloud. Due to the fast-paced changes constantly occurring in cloud configurations and customer demand, automation through IaC (infrastructure as code) technologies provides adaptable and efficient modifications performed by tools covered in this module. The module then explores maintenance and security techniques that can be automated, including in-depth coverage of patch management tools available in AWS, Azure, and GCP. The module finishes with coverage of common obstacles to establishing successful automation workflows.

FEATURES

To aid you in fully understanding cloud computing concepts, this course includes many features designed to enhance your learning experience.

Running scenario—Each module begins with a running scenario giving real-world context for the technology and concepts presented. The ongoing story provides insight into a variety of cloud computing challenges from the perspective of an IT team preparing to migrate its data center to the cloud.

Module objectives—Each module lists the concepts to be mastered within that module. This list serves as a quick reference to the module's contents and a useful study aid.

Scenario-based practice questions—Within each module are scenario-based questions similar to what you might encounter on the CompTIA Cloud+ exam. These questions put module content in real-world context and provide on-time application of covered concepts.

Colorful illustrations, screenshots, tables, and bulleted lists—Numerous full-color diagrams illustrating abstract ideas and screenshots of various cloud platform consoles help you visualize common cloud computing tools, theories, and concepts. In addition, the many tables and bulleted lists provide details and comparisons of both practical and theoretical information that can be easily reviewed and referenced in the future.

CompTIA Cloud+ Exam Tips and Notes—Each module's content is supplemented with Note features that provide additional insight and understanding, while CompTIA Cloud+ Exam Tips guide you in your preparations for taking the CompTIA Cloud+ certification exam.

Cengage Unlimited cross-references—If you have a Cengage Unlimited subscription, convenient cross-references to other publications with additional information on relevant concepts invite further study and exploration.

You're Ready prompts—As you read through each module, you'll encounter prompts that indicate when you're ready for a specific project, inviting you to customize your learning path with what works best for your learning style.

Key Terms and Glossary—Clickable key terms emphasize the core concepts of cloud computing and are defined in the convenient Glossary.

Module Summaries—Each module reading concludes with a summary of the concepts introduced in that module. These summaries help you revisit the ideas covered in each module.

Acronyms table—As in all things IT, cloud computing relies on extensive use of acronyms. The CompTIA Cloud+ objectives include a list of acronyms pertinent to the exam content, and a table at the end of each module indicates which of these acronyms are covered in that module.

Hands-On Projects—Although it is important to understand the theory behind cloud computing technology, nothing beats real-world experience. To this end, each module provides several Hands-On Projects aimed at providing you with practical implementation experience as well as practice in applying critical thinking skills to the concepts learned throughout the module. Hands-On Projects use free trial or free student accounts in the three major cloud platforms: Amazon Web Services, Microsoft Azure, and Google Cloud Platform. Many projects also take advantage of the free Yellow Circle platform designed specifically for student use.

INSTRUCTOR'S MATERIALS

Instructors, please visit *cengage.com* and sign in to access instructor-specific resources, which includes the Instructor's Manual, Solutions Manual, PowerPoint Presentation, Syllabus, and Figure Files.

Instructor's Manual: The Instructor's Manual that accompanies this course includes additional instructional material to assist in class preparation, including suggestions for classroom activities, discussion topics, and additional projects.

Solutions Manual: Answers to the scenario-based practice questions, embedded video questions, Hands-On Projects, and Reflection are provided along with grading rubrics where appropriate.

PowerPoint Presentations: This course comes with Microsoft PowerPoint slides for each module. These are included as a teaching aid for classroom presentation, to make available to students on the network for module review, or to be printed for classroom distribution. Instructors, please feel at liberty to add your own slides for additional topics you introduce to the class.

Figure Files: All of the figures in the course are reproduced on the Instructor Companion Site. Similar to the PowerPoint presentations, these are included as a teaching aid for classroom presentation, to make available to students for review, or to be printed for classroom distribution.

MINDTAP FOR CLOUD+ GUIDE TO CLOUD COMPUTING

MindTap is an online learning solution designed to help you master the skills you need in today's workforce. Research shows employers need critical thinkers, troubleshooters, and creative problem-solvers to stay relevant in our fast-paced, technology-driven world. MindTap helps you achieve this with assignments and activities that provide hands-on practice, real-life relevance, and certification test prep. MindTap guides you through assignments that help you master basic knowledge and understanding before moving on to more challenging problems. MindTap activities and assignments are tied to CompTIA Cloud+ certification exam objectives. MindTap features include the following:

- ***Integrated videos*** embedded in the module readings to show you concrete skills in four cloud platforms (Amazon Web Services, Microsoft Azure, Google Cloud Platform, and Yellow Circle). These author-led videos demonstrate skills, tools, and concepts covered in the modules, making abstract concepts and skills more concrete and preparing you to perform similar tasks in the Hands-On Projects. While videos assist in raising your comfort level with the platform(s) you're using in the projects, you'll benefit from watching videos for all the platforms in order to develop your expertise with those platforms and deepen your understanding of covered concepts.
- ***Live Virtual Machine Labs*** allow you to practice, explore, and try different solutions in a safe sandbox environment. Each module provides you with an opportunity to complete an in-depth project hosted in a live virtual machine environment. You implement the skills and knowledge gained in the module through real design and configuration scenarios in a private cloud created with OpenStack.
- ***Adaptive Test Prep (ATP)*** app is designed to help you quickly review and assess your understanding of key IT concepts. Test yourself multiple times to track your progress and improvement by filtering results by correct answers, by all questions answered, or only by incorrect answers to show where additional study help is needed.
- ***Pre- and Post- Assessments*** emulate the Cloud+ certification exam.
- ***Cloud for Life*** assignments encourage you to stay current with what's happening in the IT field.
- ***Reflection*** activities encourage classroom and online discussion of key issues covered in the modules.

Instructors, MindTap is designed around learning objectives and provides analytics and reporting so you can easily see where the class stands in terms of progress, engagement, and completion rates. Use the content and learning path as-is, or pick and choose how your materials will integrate with the learning path. You control what the students see and when they see it. Learn more at *cengage.com/mindtap/*.

STATE OF CLOUD COMPUTING IN IT (INFORMATION TECHNOLOGY)

Most organizations rely on the cloud to some degree. The RightScale 2019 State of the Cloud Survey (*blogs.flexera.com/cloud/cloud-industry-insights/cloud-computing-trends-2019-state-of-the-cloud-survey/*) polled 786 IT professionals and found that 94 percent of all respondents currently use cloud services at their companies, with 91 percent in the public cloud and 72 percent hosting a private cloud. Clearly, organizations aren't limiting themselves to a single cloud platform, with 84 percent of respondents reporting their organizations employ a multi-cloud strategy combining, on average, 3.4 public and private clouds currently in use with 1.5 more clouds under experimental evaluation for a total of 4.9 clouds per organization.

According to the same survey, the value of cloud computing shows in these organizations' budgets as well, with companies reporting a planned increase of 24 percent to their public cloud spending in the year following the survey. More than half of the respondents reported their companies already spend more than $1.2 million annually for cloud services. And nearly two-thirds of surveyed organizations report the operation of an existing cloud-specialist team, such as a cloud center of excellence, with another fifth planning to create such a team in the near future.

Certifications

While unemployment rates for technology occupations are hitting record lows according to CompTIA (*comptia.org/about-us/newsroom/press-releases/2019/06/07/u.s.-tech-unemployment-rate-at-record-low-comptia-analysis-reveals*), rising salaries for jobs such as cloud architect, cloud infrastructure engineer, and cloud administrator reveal the soaring demand specifically for cloud computing expertise. According to the Global Knowledge 2019 IT Skills and Salary Report (*globalknowledge.com/us-en/content/salary-report/it-skills-and-salary-report/*), cloud computing is in higher demand than any other IT sector, exceeding even cybersecurity. Traditional degrees and diplomas do not identify the skills that a job applicant possesses, especially in relation to fast-changing cloud technologies. Companies are relying increasingly on technical certifications to adequately identify skilled job applicants, and these certifications can offer job seekers a competitive edge in the job market.

Certifications fall into one of two categories:

- Vendor-neutral certifications are those that test for the skills and knowledge required in specific industry job roles and do not subscribe to a vendor's specific technology solutions. Some examples of vendor-neutral certifications include all of the CompTIA certifications (*comptia.org*) and certifications from CSA (Cloud Security Alliance) and (ISC)2, which is the International Information System Security Certification Consortium.
- Vendor-specific certifications validate the skills and knowledge necessary to be successful while utilizing a specific vendor's technology. Some examples of vendor-specific certifications include those offered by Amazon Web Services (*aws.amazon.com*), Microsoft (*microsoft.com*), Google (*cloud.google.com*), Red Hat (*redhat.com*), Salesforce (*salesforce.com*), and Cisco (*learningnetwork.cisco.com*).

As employers struggle to fill open IT positions with qualified candidates, certifications are a means of validating the skill sets necessary to be successful within organizations. In most careers, salary and advancement are determined by experience and education, but in the IT field, the number and type of certifications an employee earns also determine salary and wage increases. For example, Global Knowledge (*globalknowledge.com/us-en/content/salary-report/it-skills-and-salary-report/*) reports that certified IT staff earn between 7 and 21 percent more than non-certified IT staff, depending on location. Cloud certifications also make up 7 of the 10 top-paying certifications worldwide. According to the same report, nearly two-thirds of IT professionals are currently pursuing training for the purpose of obtaining additional certifications. The report shows that adding an AWS certification to nearly any other certification (such as Cisco, CompTIA, or ITIL) yields a salary increase of around $10,000.

Certification provides job applicants with more than just a competitive edge over their noncertified counterparts competing for the same IT positions. Some institutions of higher education grant college credit to students who successfully pass certification exams, moving them further along in their degree programs. For those already employed, achieving a new certification increases job effectiveness, which opens doors for advancement and job security. Certification also gives individuals who are interested in careers in the military the ability to move into higher positions more quickly.

What's New with CompTIA Cloud+ Certification

Now in its second iteration, the CompTIA Cloud+ exam (CV0-002) reflects the maturation of the cloud industry with updated technologies and concepts framed in the larger context of business priorities and existing IT systems. With less emphasis on physical host configuration and much greater emphasis on cloud infrastructure, management, and security, the new exam requires proficiency with standard cloud services that demonstrates a student's understanding and knowledge in cloud networking, security, storage, and maintenance. These concepts are not directly transferrable from the on-premises data center to the cloud but, rather, require an abstraction of functions to a software-defined environment where everything is virtualized and underlying hardware is essentially invisible to the cloud consumer. Common compute, network, security, and storage standards must be reimagined to take full advantage of the cloud's potential. The new CompTIA Cloud+ exam invites candidates to contemplate these ideas more deeply and in ways more relevant to the cloud ecosystem.

The verbs in the exam's objectives indicate the increased depth of knowledge required for this new version of the exam. In the field of educational psychology, Bloom's Taxonomy is an industry-standard classification system used to help identify the level of ability that learners need to demonstrate proficiency. It is often used to classify educational learning objectives into various levels of complexity. Bloom's Taxonomy reflects the "cognitive process dimension" of learning and understanding that represents a continuum of increasing cognitive complexity, from remember (lowest level) to create (highest level).

There are six levels in Bloom's Taxonomy as shown in Figure A. The first CompTIA Cloud+ exam (CV0-001) was more heavily weighted toward level 2, Understand. Many of that exam's objectives began with the verb "explain" or "identify." The new exam, CV0-002, contains only one objective at level 2 and is almost evenly distributed across level 3, Apply, and level 4, Analyze. Many objectives use verbs such as "analyze," "apply," "implement," "determine," or "troubleshoot," all of which require much greater understanding than what is needed to explain or identify related concepts.

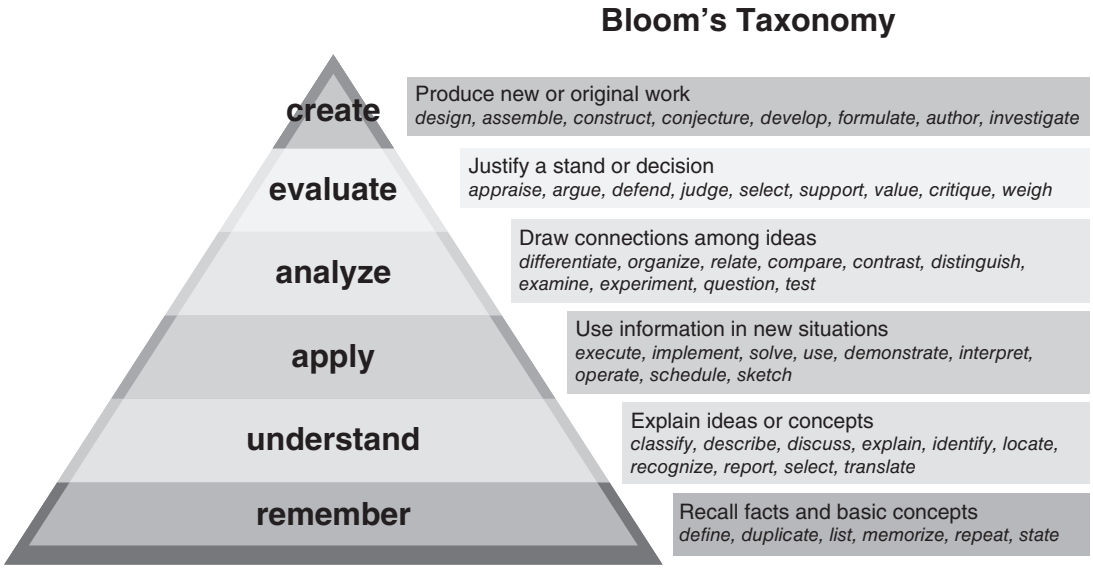

Figure A

Also new for this exam are the many performance-based questions. These questions present simulations with complex interactions designed to test a candidate's ability to apply concepts and analyze problems. Mastering, rather than simply memorizing, the material in this course will help you succeed on the exam and on the job.

Following are the domains covered on the new CompTIA Cloud+ exam:

CV0-002 Domain	% of Examination
Domain 1.0 Configuration and Deployment	24%
Domain 2.0 Security	16%
Domain 3.0 Maintenance	18%
Domain 4.0 Management	20%
Domain 5.0 Troubleshooting	22%

ABOUT THE AUTHOR

Jill West, coauthor of Cengage's Network+ and A+ textbooks and author of the new Cloud+ digital course, has taught kindergarten through college using a flipped classroom approach, distance learning, hybrid teaching, and educational counseling. She currently teaches computer technology courses at Georgia Northwestern Technical College, both online and in the classroom. Jill regularly presents at state and national conferences and international webinars on CompTIA certifications for students and train-the-trainer sessions for instructors. She's also a member of the inaugural cohort of Faculty Ambassadors for AWS Educate. Jill and her husband, Mike, live in northwest Georgia with their four children.

ACKNOWLEDGMENTS

It takes a village to write a book … especially if it's a digital course like this one. I wish that you, the reader, could meet all the wonderful people who contributed to this effort. An entire community of caring and talented professionals built this course piece by piece, block by block, with mindful dedication and persistent commitment to excellence.

I wish that you could meet Lisa Ruffolo, who fought in the trenches with me to meet heavy deadlines and keep an intense pace. I wish you could meet Maria Garguilo, who kept the whole project on track with exceptional organizational skills and always a bright and optimistic attitude, and Natalie Onderdonk, whose thoughtful insights and ideas will benefit you throughout this course. I think you would enjoy—as everyone who knows her does—Amy Savino, whose compassionate leadership style exemplifies integrity and honor. We round out the team with John Freitas, whose sharp eyes and careful testing help ensure the projects will run smoothly. I'd also like to give a shout-out to David Staples for contributing his expertise and creativity for the myriad testbank questions. Special thanks to all our reviewers who contributed expertise, ideas, insights, and passion:

- Phyllis Davis (St. Louis Community College)
- Dr. Johnathan Yerby (Middle Georgia State University)
- Susan Booth (Cape Fear Community College)
- Dr. Daniela Marghitu (Auburn University)
- And my friend and colleague, Dwight Watt (Georgia Northwestern Technical College)

Each of us works in community with other co-workers, colleagues, friends, and family. Thanks to all of you for your ideas, assistance, feedback, and encouragement. Also, a special thanks goes to my husband, Mike, for his tireless support and encouragement.

READ THIS BEFORE YOU BEGIN

Getting into the cloud is not as difficult as you might initially think. Many cloud providers offer generous free trials, especially for students. In this course, you'll have the opportunity to work in three different public clouds: AWS (Amazon Web Services), Microsoft Azure, and GCP (Google Cloud Platform). You can choose any one, two, or all three of these platforms, depending on your needs, preferences, and available resources. They all offer some level of free trial credit and free tier services during the free trial, and some of these options don't even require a credit card. Alternatively, some gift cards from major credit card companies can be used instead of a traditional credit card. Module 1 will walk you through the free trial options. Regardless of which platforms you decide to use, you can read through the material giving parallel information for the other platforms. You can also watch the videos for the other platforms so you can see those cloud services in action.

You'll also have the opportunity to work in Yellow Circle, which is a cloud platform designed specifically for educational use. Yellow Circle offers a free tier subscription for students. Although services in this free subscription are very limited and the platform sometimes suffers from service issues, the Yellow Circle projects are written to give you an on-ramp to more complex tasks in other cloud platforms.

Finally, the Live Virtual Machine Lab in each module will help you learn OpenStack, which is a private cloud platform. These labs are accessed through MindTap and let you work in fully functioning virtual machines to build your own private cloud. With detailed steps and helpful screenshots, you'll find the support you need to perform complex provisioning tasks. Or you can explore and experiment beyond the parameters of the lab because these virtual machines are real systems and not simulations.

As for hardware and software, nearly all of the projects in this course are completed through your browser. A decent computer with a good browser such as Chrome, Edge, Firefox, or Safari will work well. A few projects in the Azure platform work best if you're using a Windows computer. To remote in to cloud-hosted VMs in AWS and Azure, you will occasionally need to install or use existing remote access software on your local computer, such as PuTTY or Remote Desktop. You will also need administrative access to your computer's CLI (command-line interface) tool, such as PowerShell on a Windows computer. In one project in Module 2, you will install and use VirtualBox, a free hypervisor, and you'll need an ISO file for Windows or a Linux OS. You can instead use a different hypervisor for this project if you prefer.

These projects have been designed to make the cloud as accessible as possible for students and schools in all kinds of settings and circumstances. Nearly all of the projects can be completed for free in their respective cloud platforms, especially if you're still within your free trial limits. Any steps that might accrue charges are identified, along with instructions on how to circumvent charges if you don't have free trial credits available.

Overall, the course offers many layers of options and resources that help you get into the cloud and build hands-on experience, making concepts concrete and memorable while helping you understand and apply the skills you're learning.

INTRODUCTION TO CLOUD COMPUTING

MODULE 1

After reading this module, you will be able to:

1. Evaluate reasons for pursuing a Cloud+ certification.
2. Explore defining characteristics of cloud computing.
3. Determine new skill sets required for working in the cloud.
4. Identify various cloud deployment models, including public cloud, private cloud, hybrid cloud, multi-cloud, and community cloud.
5. Analyze security concerns specific to each cloud deployment model.
6. Identify various cloud service models, including SaaS (Software as a Service), PaaS (Platform as a Service), and IaaS (Infrastructure as a Service).
7. Analyze security concerns specific to each cloud service model.
8. Recognize popular cloud service providers.
9. Evaluate common cloud service types, including compute, storage, network, and security services.
10. Analyze security concerns specific to each cloud service model.
11. Anticipate common cloud issues.
12. Explain the troubleshooting steps.
13. Identify helpful preventive measures.

MODULE 1 SCENARIO

The clock says 8:56 as you slide in through the basement door of your building, shaking the rain off your umbrella and wiping your feet on the doormat. You're right on time for once! You notice the empty boxes still sitting by the doorway after yesterday's delivery of new cabling supplies. When you glance up at the security camera in the lobby area, you wonder yet again who might be sitting on the other side of that camera watching you move through the office space toward your desk. You make a mental note to ask Henry, the security guard at the front gate, where the camera feed goes and how often someone sits staring at the feeds . . . just out of curiosity, of course.

As you hang your jacket on the back of your chair and prop your umbrella in the corner near your desk, Kendra, your boss, calls out from her office, "Come on, everyone—we've got a meeting!"

Oh, that's right. Your IT team is discussing the upcoming cloud migration today. At the meeting, the CIO of the private school you work for summarizes an Amazon Web Services (AWS) conference he recently attended touting the benefits of cloud computing. He's seeing dollar signs as he excitedly describes all the ways your school can save money by migrating to the cloud. "We won't have to pay so much for IT hardware anymore, our expenses will flex with our changing IT needs throughout the year, and even our electric bill will go down. Plus, the cloud apps we can use in the classroom are good for our students. We'll be able to attract more students from tech-savvy families moving to the area because of the tech start-ups and other IT companies migrating here."

Sounds like a good plan. Now it's up to your team to figure out how to do it. Your cloud conversion team will be led by your boss, Kendra, the network administrator. You've been recruited to help, along with a recently hired co-worker, Nigel, who passed his A+ certification exam last spring while taking night classes and then asked to be transferred

to IT from his former position as a security guard. None of you have much experience with the cloud yet, other than Netflix binge watching on the weekends and your personal Gmail and social media accounts. The technology seems a little futuristic and "out there" when you think about it. But you're also secretly excited about learning some new stuff. Supposedly, "the cloud" is the next big revolution in the IT industry, and you'd rather be ahead of the curve than behind it on something so significant.

As the meeting rolls along, the entire team discusses what kinds of information you all need to know to have an intelligent conversation about the cloud. As you wrap up your action list in preparation for your next meeting, the questions you want to answer for yourself are the following:

- What is cloud computing?
- What new skills do I need to learn?
- Who owns the cloud?
- How does the cloud affect the security of my organization's data?

CHARACTERISTICS OF CLOUD COMPUTING

CERTIFICATION

4.3 Given a scenario, determine when to provision/deprovision cloud resources.

Cloud Computing Certifications

CompTIA (Computing Technology Industry Association) released its first Cloud+ certification (CV0-001) in 2015 as a more advanced and technical cloud computing certification than the earlier Cloud Essentials certification, which is intended for non-IT professionals or for IT professionals needing to bridge the gap between technical concepts and business concerns. The newest version of the Cloud+ certification, CV0-002, became available to the public in early 2018. The Cloud+ exam builds on the knowledge required for other certification exams, as shown in Figure 1-1, including the following:

- ***A+***: Covers skills required for IT technical support specialists
- ***Network+***: Covers foundational networking concepts and skills
- ***Security+***: Surveys IT security technologies and strategies at a level necessary for any IT professional

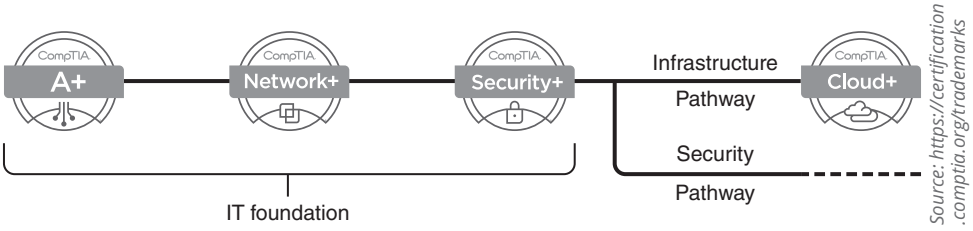

Figure 1-1 Cloud+ is an infrastructure-specialty certification

While these certifications ("certs" for short) are not required for the Cloud+ exam, the knowledge covered by their objectives is directly relevant to the skills required of a Cloud+ certified technician. Cloud+ takes the foundational concepts covered in these earlier exams and applies that information to a cloud environment. This course assumes you are already at least somewhat familiar with A+, Network+, and possibly Security+ skills and concepts.

CompTIA Cloud+ Certification

One aspect that sets Cloud+ apart from most other cloud computing certs is that Cloud+ is vendor neutral. This means that, throughout this course, you will learn cloud computing concepts that span the full range of cloud computing services rather than targeting specific skills for working with any one cloud provider's platform. You might pursue a Cloud+ certification for the following reasons:

- Prepare for a new job or a promotion that likely will include responsibility for interacting with an organization's existing cloud services.
- Build a foundational understanding of cloud computing in preparation for vendor-specific cloud certifications.
- Complement certifications in other specialty areas (such as infrastructure, security, database management, or programming).
- Develop a big-picture perspective of cloud computing technologies, major players, and industry expectations in preparation for choosing vendors and migrating on-premises ("on-prem" for short) services to the cloud.

Other Cloud Certifications

Another vendor-neutral cloud certification is the more advanced CCSP (Certified Cloud Security Professional) certification from CSA (Cloud Security Alliance) and (ISC), which is the International Information System Security Certification Consortium. The CCSP focuses on the security side of cloud computing at an expert level and requires a minimum of five years full-time IT work experience, three of which must be in information security, before you can take the exam, or you must already have their CISSP (Certified Information Systems Security Professional) certification.

Several highly respected, vendor-specific cloud certifications prove increasing levels of proficiency with specific cloud platforms and products. Some of the major vendor cloud certifications include the following:

- **Amazon Web Services (AWS)** holds the lion's share of the cloud platform market. AWS role-based certifications follow one of several certification tracks or learning paths, such as Architect, Developer, or Operations. Within each path, roles progress from Foundational and Associate to Professional and, in some cases, Specialty levels. Popular AWS certs include the three following certifications:
  - ***Cloud Practitioner.*** This entry-level AWS certification is appropriate for professionals in technical, managerial, sales, purchasing, or financial roles.
  - ***AWS Certified Solutions Architect – Associate.*** This intermediate AWS cert focuses on designing applications and systems in AWS. The related, advanced cert is AWS Certified Solutions Architect – Professional.
  - ***AWS Certified SysOps Administrator – Associate.*** This intermediate AWS cert focuses on creating automated deployments of applications, networks, and systems in AWS. The related advanced cert is AWS Certified DevOps Engineer – Professional.
- Microsoft supports the **Azure** cloud platform and offers the following exam pathways to earn their Azure certifications:
  - ***Microsoft Certified Azure Fundamentals.*** This entry-level Azure certification is appropriate for candidates with nontechnical backgrounds or for technical professionals validating foundational knowledge of cloud services.
  - ***Microsoft Certified Azure Administrator Associate.*** This intermediate Microsoft cert focuses on implementing, monitoring, and maintaining Azure-based cloud solutions. Candidates must pass two exams.
- **Google Cloud Platform (GCP)** is another major contender in the global cloud market and is quickly growing. While GCP offers fewer certifications, they are highly relevant if you will be working in a GCP ecosystem. Popular GCP certs include the following:
  - ***Associate Cloud Engineer.*** This entry-level GCP certification covers setting up, deploying, and securely operating a cloud solution.
  - ***Professional Cloud Architect.*** This intermediate GCP cert focuses on designing, managing, optimizing, and securing a cloud solution architecture.
- One of Cisco's many highly respected certifications is CCNA Cloud. As an entry-level exam, its objectives focus on provisioning and support of Cisco's cloud solutions. Candidates must pass two exams.
- VMware, a well-known provider of virtualization solutions, offers solutions that are highly integrated into AWS's cloud platform. The VMware Certified Professional 7 – Cloud Management and Automation (VCP7-CMA) cert is an intermediate-level cert focused on installing, configuring, and administering a VMware cloud environment.

NOTE An entry-level cloud computing job might be called a junior cloud engineer, cloud implementation manager trainee, cloud technical architect, or junior cloud analyst, among many other possibilities. More advanced cloud computing positions might go by titles such as cloud systems administrator (CSA), senior cloud engineer, or cloud infrastructure engineer.

What Is Cloud Computing?

What makes cloud computing so attractive to companies looking to maximize their bottom line? According to **NIST (National Institute of Standards and Technology)**, cloud computing has five essential characteristics, as shown in Figure 1-2:

- ***On-demand self-service.*** In a traditional network or data center setting, network resources must be carefully planned, purchased, configured, and implemented. It can take months from deciding to institute a new resource until that resource becomes available. Many people are typically involved in the decision-making and implementation processes. In contrast, cloud resources, such as virtual machines (VMs) or user accounts, can be created at any time by the service subscriber and other authorized users, which is called **on-demand self-service**. There's no built-in delay to order, install, and configure hardware because cloud resources are virtualized on top of existing hardware at the service provider's location. For example, suppose you need to add a web server to your network. Within a few minutes, you can spin up a VM in the cloud, optimize its virtual hardware resources (such as memory and processing power) and network settings to support web services, and then install the web server software, website files, and content, to produce a live website. This process, once established, can even be automated.
- ***Broad network access.*** Traditional network resources are mostly available only to users located within a specific geographic area. To access these resources from outside the network, the user must "remote in" using a **VPN (virtual private network)** connection or similar remote access technology. Cloud services, however, are available from anywhere on the Internet and using any of a number of device types, such as a laptop, smartphone, or tablet. This type of access is called **broad network access**, and it gives cloud computing the flexibility of access to a larger user population in a wider variety of circumstances.
- ***Resource pooling.*** In traditional networks, physical and virtual resources reside at the organization's own location, and all those resources are dedicated to the organization's own use. If a server is functioning

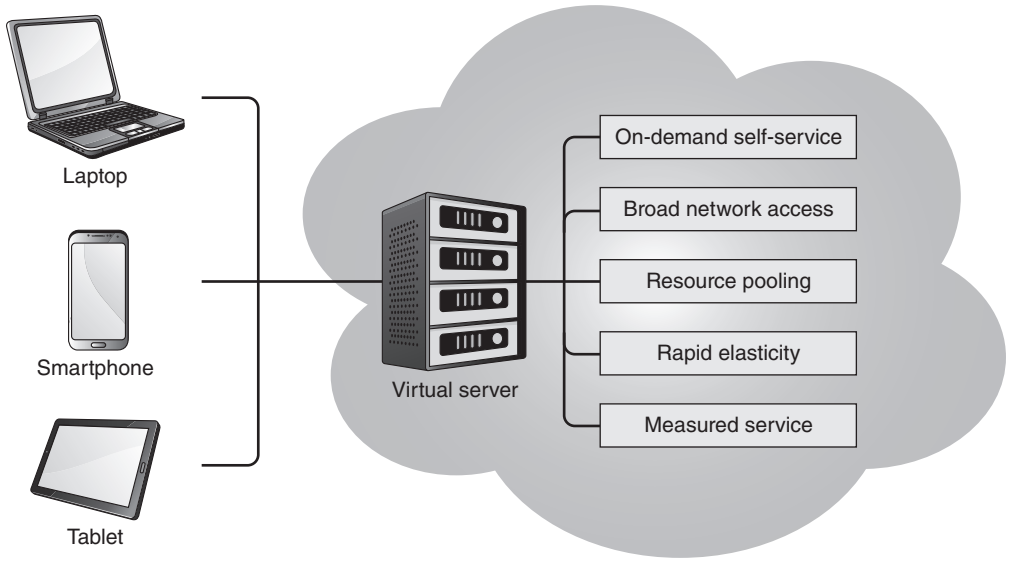

Figure 1-2 Characteristics of cloud computing

at 10 percent capacity to meet the organization's needs, the remaining capacity is simply unused. Cloud providers use **resource pooling** to maximize the potential capacity of physical and virtual resources, which simultaneously serve multiple customers—called **tenants**—at any given time. The cost benefits of this efficiency are passed along to customers. A single server might be performing compute operations for three or four different cloud subscribers, and a single subscriber might be running a database whose data is held by multiple servers at multiple locations owned and operated by the cloud provider. In most cases, the cloud customer doesn't know where their resources are hosted geographically, only how to access them through the Internet.

- ***Rapid elasticity.*** **Rapid elasticity** or scalability refers to a cloud resource's ability to be scaled up or down very quickly—even automatically—according to demand. For example, suppose your company is preparing to run a Super Bowl ad and anticipates a tremendous increase in traffic to their website. On a traditional network, you would need to order additional servers to help support the increased traffic. This could take weeks of preparation and would be very expensive. After the ad traffic subsided, you would be left with several servers whose purpose had waned. If your web server is hosted in the cloud, however, you could provision additional web servers in minutes—or program them to auto-provision as needed—and then decommission those servers as the ad-generated traffic tapers off. You would only pay for the cloud servers while you used them, and once decommissioned, you would incur no additional costs.
- ***Measured service.*** The ability to track your usage of cloud resources at a granular level is what makes cloud computing a **measured service**. You are charged for the resources you use. Many cloud providers allow for detailed tracking of these activities and charges. For example, AWS bills for VM instances by the second, which avoids costly roundups to full-minute or hourly pricing. This pay-as-you-go approach, if configured properly, can save companies a great deal of money even before other optimizations are made for cloud technology.

Cloud providers often describe additional characteristics and benefits to cloud computing, including the following:

- ***Self-patching/self-healing infrastructure.*** Because much of cloud computing is automated, a cloud network can patch or repair itself when encountering certain types of problems.
- ***Adaptive, intelligent security.*** Cloud computing increasingly takes advantage of AI (artificial intelligence) technology to improve built-in security defenses.
- ***Cross-platform.*** Cloud services can be accessed and used from devices running different operating systems (OSs).

Organizations consider many reasons for transitioning to a cloud environment. They might be facing the expiration of a lease at their data center location; they might be looking for ways to optimize their services and become more competitive; or they might expect that cloud services will improve their bottom line. The cloud transition is not an overnight shift—organizations adopt cloud services in phases, and many will never become fully cloud-centric. Even after they've begun to make the transition to the cloud, business needs continue to change, and so do their cloud service requirements. Whether the changes are external, such as changes to regulations or laws, or internal, such as business **mergers** (two businesses blending into one), **acquisitions** (one business buying another), or **divestitures** (one business splitting off part of itself), the cloud services that support the business will need to be adapted, migrated, or replaced. All of these changes require specialized skills from IT technicians to configure, deploy, secure, maintain, manage, and troubleshoot cloud computing services and resources.

What Do I Need to Know?

Cloud computing is a recent—and rapidly changing—development in IT that is also revolutionizing the industry. Skills and knowledge from even five years ago are insufficient to meet the demands of managing cloud-hosted resources. IT professionals throughout the industry are asking what new skills they need to stay relevant as cloud computing technologies emerge and mature. The following list shows areas of professional growth most needed for cloud computing professionals—or any IT professional interacting significantly with the cloud:

- ***Security skills.*** Traditionally, IT security focuses on maintaining a protective perimeter around the on-prem data center, managing all traffic into and out of that secure perimeter (see Figure 1-3). As data, applications, and other resources move to the cloud, security must be built into the resources themselves so it travels

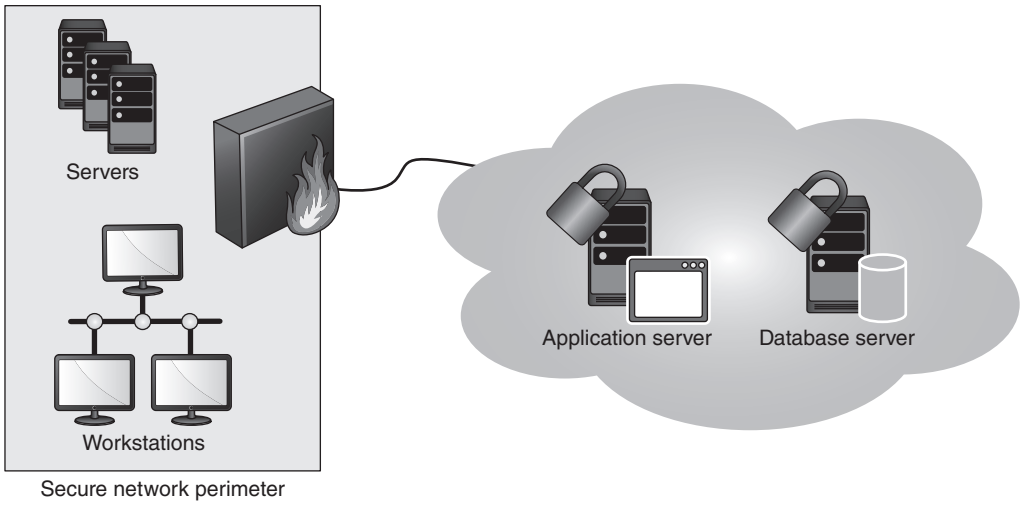

Figure 1-3 Cloud security can't rely on a secure perimeter

with them. Administrators must also carefully consider what data can be outsourced to the cloud, as some types of regulated data are restricted to on-prem storage only. At the same time, cloud service providers offer options with built-in security compliance measures, which can relieve the organization of needing to configure those requirements itself. While the cloud consumer is still responsible for enabling cloud security measures and configuring them in ways that best fit their needs, most cloud providers offer many tools—some that are free—to help with this effort. A cloud IT professional must become familiar with these tools and best practices in using them.

- ***Other specialty areas.*** The broad possibilities inherent in cloud computing require that cloud technicians understand the business and organizational context of the services provided through the cloud. The more you understand, the more valuable you'll make yourself to potential employers. Important areas include the following:
  - The organization's business goals and the business processes and workflows that affect every department within an organization
  - Software development processes, including automation scripts, **APIs (application programming interface)**, configuration management, virtualization, monitoring, and continuous integration/continuous delivery (CI/CD), making cloud computing essentially a **DevOps (development and operations)** environment
  - Infrastructure concepts, skills, and tools—networking in the cloud transitions the concrete configurations of a local network into a more abstract layer, which will only make sense to you if you thoroughly understand local networking
  - Security vulnerabilities, technologies, and best practices that are specific to cloud-hosted resources
- ***Automation tools.*** One of the biggest advantages of moving to the cloud is gaining a greater degree of **automation**. The underlying virtualization layer and the encompassing monitoring techniques allow for granular and responsive automation. Developing the skills required to establish automation (a process called **orchestration**) in a way that is both efficient and reliable, and then continuing to refine them, is where cloud network admins often are most challenged.
- ***Lifelong learning.*** Cloud technologies are in constant flux, even more so than on-prem technologies. **Cloud service providers (CSPs)** are innovating at an astonishing rate. A service that adequately meets your needs when you first migrate to the cloud could be overshadowed by a much improved—and cheaper—service a few months later. Staying relevant requires monitoring your own learning by identifying your blind spots, finding the information resources you need, and following through on your learning process. The most important computer skill is the ability to teach yourself.

You're Ready

Passing the CompTIA Cloud+ exam will help prepare you to target more specialized and advanced cloud certifications later, such as those published by AWS, Azure, or GCP. Understanding what those certifications cover, how they're organized, and how they're related will help you make better choices about which certifications are the best fit for you and your career aspirations. Project 1-1: Cloud Computing Certifications gives you a chance to explore some of these certifications more in-depth.

You're now ready to complete Project 1-1: Cloud Computing Certifications. You can complete the project now or wait until you've finished all of the readings for this module.

CLOUD DEPLOYMENT MODELS

CERTIFICATION

1.5 Given a scenario, analyze sizing, subnetting, and basic routing for a provided deployment of a virtual network.

2.1 Given a scenario, apply security configurations and compliance controls to meet given cloud infrastructure requirements.

2.2 Given a scenario, apply the appropriate ACL to the target objects to meet access requirements according to a security template.

4.2 Given a scenario, determine the appropriate allocation of cloud resources.

Cloud Deployment Models

One advantage of cloud computing is that a business can use someone else's hardware to host their applications, data, and network infrastructure. One disadvantage of cloud computing is that a business must typically rely on someone else's hardware to host their applications, data, and network infrastructure. Those statements aren't redundant or contradictory—cloud computing adds convenience while also reducing an organization's control of the hardware supporting their IT resources. This creates specific security concerns that vary according to the type of cloud services an organization decides to use. Most organizations don't jump directly into a cloud-only deployment, so you should be aware of the various options for who owns what resources in the cloud.

Public Cloud

When people think of cloud computing, the public cloud is generally what they have in mind. As shown in Figure 1-4, **public cloud** services are hosted on hardware resources at the cloud service provider's (CSP) location, and those physical resources can be shared with any other customer. The CSP might be a business, an academic organization, or a government entity. It provides cloud services (paid or free)—such as storage space, applications, compute capacity, or network functions—that are available to the general public.

With a public cloud, the CSP manages the hardware and can't be accessed directly by the cloud customer. In this case, the customer relies deeply on the CSP's security measures to protect the data and other resources hosted in the public cloud. However, that doesn't mean the customer has no responsibility for its data security or that all CSPs

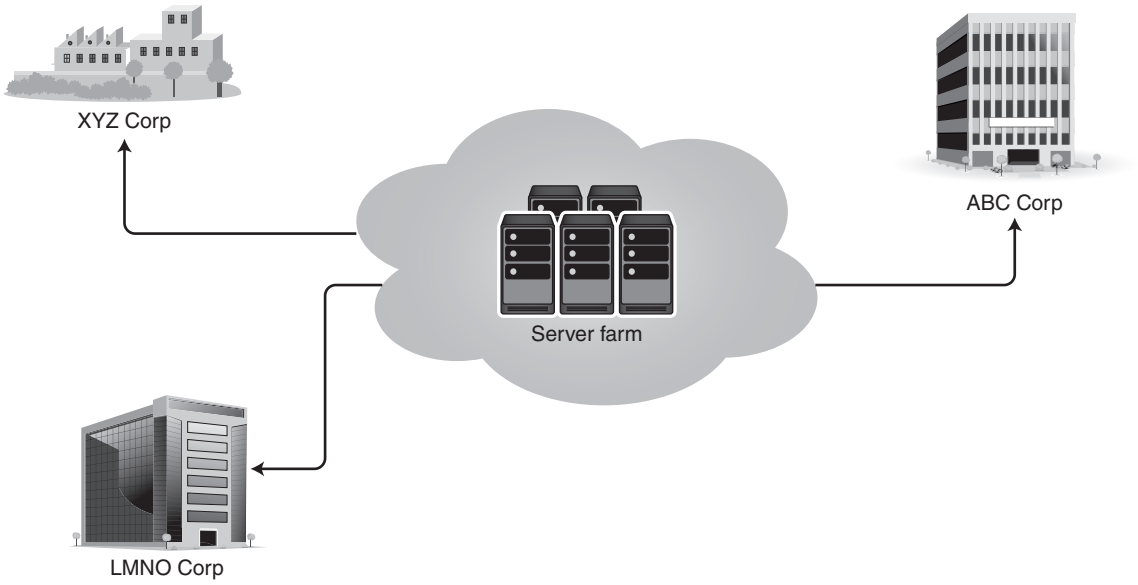

Figure 1-4 A public cloud is hosted on hardware shared by multiple customers

provide sufficient data center security. The following is a list of steps a public cloud consumer can take to help ensure the security of their public cloud:

- Research the CSP's industry certifications and audit compliance reports. Some of the most important to look for include the following:
  - ***ISO/IEC 27001.*** Developed by the ISO (International Organization for Standardization) and the IEC (International Electrotechnical Commission), the **ISO/IEC 27001** standard provides an overarching model for organizations to use in keeping information secure. It addresses people, processes, and IT systems through a risk management process; all of these components together are referred to as an ISMS (information security management system). An organization can become ISO/IEC 27001 certified by meeting these requirements, as determined by an audit conducted by an accredited certification body. Learn more about this certification at *iso.org/isoiec-27001-information-security.html*.

NOTE

The ISO (International Organization for Standardization) is an independent, nongovernmental international organization established in 1947, and is also responsible for having developed the seven-layer OSI (Open Systems Interconnection) model used in networking. Its shortened name, *ISO*, is derived from a Greek word meaning *equal*. The organization's founders chose this abbreviation to avoid confusion from having various acronyms for their name, depending on the language used.

  - ***SSAE 18.*** The **SSAE (Statement on Standards for Attestation Engagements No. 18)**, developed by the AICPA (American Institute of Certified Public Accountants), is a standard used to determine audit compliance. The SSAE 18 replaces earlier standards such as SSAE 16, which replaced an even older standard, SAS 70 (Statement on Auditing Standards No. 70). Instead of resulting in a certification, an SSAE 18 audit results in various **SOC (Service Organization Control) reports**. Two types of SOC 1 (pronounced *sock one*) reports focus on internal financial controls. Most relevant to this discussion, however, are the SOC 2 and SOC 3 reports. Both reports address benchmarks as defined by the organization for information security, availability, processing integrity, confidentiality, and privacy. The SOC 2 report contains proprietary information and often requires a signed **NDA (nondisclosure agreement)** before release to a customer. The SOC 3 report is designed for public release. Learn more about this standard at *aicpa.org/research/standards/auditattest/ssae.html* and *aicpa.org/interestareas/frc/assuranceadvisoryservices/serviceorganization-smanagement.html*.

- ***PCI DSS.*** For all companies that provide credit card services, including accepting, storing, processing, or transmitting credit card data, the **Payment Card Industry Data Security Standard (PCI DSS)** sets requirements for keeping that information secure. Compliance standards are determined by the PCI Security Standards Council in gradations of stringency according to annual transaction volume. The standards are enforced by credit card brands, such as Visa and MasterCard.
- ***HIPAA.*** The **Health Insurance Portability and Accountability Act (HIPAA)** was enacted in 1996 to protect medical information. Among other things, HIPAA set the stage to establish and continually evolve specific guidelines for data security when that data includes any identifiable information about patients or their medical history. It also imposes stiff penalties and fines for data breaches, whether due to criminal intent or even simple negligence.
- ***GDPR.*** A more recent development, the **General Data Protection Regulation (GDPR)** defines broad protections for any personally identifiable information (PII) and standards for how to handle breaches affecting that data. The regulations apply to any organization handling this type of information for European Union (EU) citizens, even if the organization is not based in Europe. The GDPR became effective in mid-2018 and, at the time of this writing, is currently being tested with some recent breaches for how stringently the standards and penalties will be enforced.

- Check security requirements as defined in the CSP's **SLA (service level agreement)**. The SLA might include terms of agreement such as requiring encryption of all data in transit or in storage, geographic location of data storage (which might be regulated by law, depending on your organization and the type of data), consistency of service availability, and penalties for failure in any of these areas. Security failures can be quite costly for your organization, and the SLA should include some kind of compensation for damages resulting from problems on the CSP's end.
- Investigate the CSP's security measures. For example, ask about how the CSP protects against data leakage between tenants on their multi-tenant infrastructure. Ask whether the CSP relies on third-party vendors, what measures are in place to ensure those organizations' compliance with standards and compliance measures, and how those services are handled if there's an availability or other security concern with those vendors.
- Understand the CSP's recommendations and requirements for your own organization's security measures. This might include access monitoring, license management, self-service troubleshooting, trouble ticket reporting requirements, or encryption processes that you're responsible for.

Private Cloud

Private cloud services are hosted on hardware resources used exclusively by a single organization. This hardware might be located in a CSP's data center and dedicated to one customer, or the hardware might be located in the organization's own data center. What makes a cloud private is that no one else is allowed to use the hardware for their own cloud, regardless of where that hardware is located. This increases security and the organization's control over the exact configuration of the hardware used. In fact, the need to keep sensitive data on-site is often the motivating factor in deploying a private cloud on-prem.

You might wonder how a private cloud hosted on-prem is different from the traditional data center that most organizations already have. A traditional data center might use virtualization for network or data services. **Virtualization** is a time-tested technology designed to host many services on a single, physical server. While virtualization provides some flexibility in how the hardware interacts with virtual services, the configurations for these services are still closely tied to the underlying physical hardware. A cloud is more abstracted from the physical hardware in the data center, relying on a cloud **API (application programming interface)** layer of communication that is managed by comprehensive virtualization software. See Figure 1-5. In essence, you can have both at the same time: an on-prem data center that is running a private cloud.

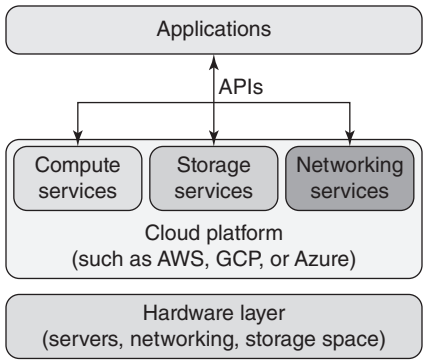

Figure 1-5 Cloud services and underlying hardware communicate with APIs