COURSE SYLLABUS

CompTIA Cloud+ Exam Preparation Course (Self-Paced)

Build the vendor-neutral cloud skills the CompTIA Cloud+ exam covers so you can sit it and apply them on the job.

> Group classes (Live Online) and onsite training are available for this course. For more information, email onsite@graduateschool.edu or visit: https://www.graduateschool.edu/courses/cloud-plus-exam-prep-course-self-paced



support@graduateschool.edu •
(888) 744-4723

Course Outline

Module 1: Cloud Service Models and the Shared Responsibility Model

- Lessons:
  - Cloud Service Models: IaaS, PaaS, and SaaS
  - Function as a Service and Serverless Computing
  - The Shared Responsibility Model
- Applied activity: Learners review a short scenario describing a company evaluating three different workloads and match each to the service model that fits it, then identify which party is responsible for a stated security control under the shared responsibility model.

Module 2: Service Availability, Resilience, and Disaster Recovery

- Lessons:
  - Regions, Availability Zones, and Edge Computing
  - Cloud Bursting and Availability Monitoring
  - Disaster Recovery Metrics: RTO and RPO
  - DR Site Strategies: Hot, Warm, and Cold Sites
  - Multicloud Tenancy Strategies
- Applied activity: Learners review a short scenario describing an organization's recovery time and budget requirements and select an appropriate DR site strategy, then justify it using RTO and RPO.

Module 3: Cloud Networking Concepts

- Lessons:
  - VPNs and Dedicated Connections
  - Load Balancers, Application Gateways, CDNs, and Firewalls
  - Virtual Private Clouds: Peering and Transit Gateways
  - Subnets in a Cloud Network
  - Cloud Routing and Switching: VLANs, SDN, BGP, and Route Tables

- Applied activity: Learners review a short scenario describing two VPCs that need to communicate and a public-facing application that needs traffic distributed across multiple instances, then select the appropriate networking components for each need.

Module 4: Cloud Storage and Database Concepts

- Lessons:
  - Storage Tiers: Hot, Warm, Cold, and Archive
  - Disk Types and Storage Types: Object, Block, and File
  - Performance and Cost Tradeoffs in Cloud Storage
  - Database Types and Deployment Options
- Applied activity: Learners review a short scenario describing several data sets with different access frequencies and durability needs and assign each to the correct storage tier and storage type, then recommend a database type and deployment option for a described application.

Module 5: Virtualization and Containerization

- Lessons:
  - Virtual Machine Fundamentals: Stand-Alone, Clustering, and Cloning
  - Host Affinity, Hardware Pass-Through, and VM Networking and Storage
  - Container Fundamentals and Workload Orchestration
  - Container Networking and Port Mapping
  - Container Storage and Image Registries
- Applied activity: Learners review a short scenario describing an application being migrated from virtual machines to containers and identify which virtualization and containerization concepts apply at each stage, including storage and networking choices.

Module 6: Cloud-Native Design, Cost Management, and Emerging Technologies

- Lessons:
  - Cloud-Native Design: Microservices and Loosely Coupled Architecture
  - Cost Considerations: Billing Models and Rightsizing
  - Optimizing Cloud Workloads
  - Machine Learning and AI in the Cloud
  - Internet of Things (IoT) in the Cloud
- Applied activity: Learners review a short scenario describing a monolithic application with rising cloud costs and propose at least one cloud-native design change and one cost-management change that would address it.

Module 7: Cloud Deployment Models and Strategies

- Lessons:
  - Cloud Deployment Models: Public, Private, Hybrid, and Community
  - Deployment Strategies: Blue-Green and Canary
  - Deployment Strategies: Rolling and In-Place
- Applied activity: Learners review a short scenario describing an organization choosing a deployment model for a new application and a release strategy for updating it, and select the model and strategy that best fit the stated risk tolerance.

Module 8: Cloud Migration Planning

- Lessons:
  - Cloud Migration Types
  - Resource Allocation Considerations for a Migration
  - The Six Application Migration Strategies

- Weighing Migration Tradeoffs in a Real Scenario

- Applied activity: Learners review a short scenario describing a portfolio of legacy applications with different technical and business constraints and assign each application the migration strategy that best fits it.

Module 9: Code-Based Deployment and Resource Provisioning

- Lessons:
  - Infrastructure as Code and Configuration as Code
  - Scripting Logic for Automation
  - Repeatability, Drift Detection, Versioning, and Testing
  - Provisioning Cloud Resources to Meet Requirements

- Applied activity: Learners review a short scenario listing an application's storage, performance, security, cost, and compliance requirements and select the cloud resources that satisfy them, then identify how infrastructure as code would make that provisioning repeatable.

Module 10: Observability, Scaling, and Elasticity

- Lessons:
  - Logging: Collection, Aggregation, and Retention
  - Alerting, Tracing, and Monitoring
  - Scaling Approaches: Triggered, Scheduled, and Manual
  - Horizontal and Vertical Scaling

- Applied activity: Learners review a short scenario describing an application with unpredictable traffic spikes and design an observability and scaling approach, selecting the correct scaling trigger and scaling type.

Module 11: Backup, Recovery, and Cloud Resource Life Cycle Management

- Lessons:
  - Backup Types and Locations
  - Backup Schedule, Retention, Replication, and Encryption
  - Recovery Types, Recovery Options, and Backup Testing
  - Patching, Updates, and Decommissioning Cloud Resources

- Applied activity: Learners review a short scenario describing an application's recovery point and recovery time requirements and select an appropriate backup type, schedule, and recovery approach, then identify the life cycle stage of a resource nearing end of support.

Module 12: Vulnerability Management, Compliance, and Regulation

- Lessons:
  - The Vulnerability Management Life Cycle
  - Common Vulnerabilities and Exposures
  - Data Sovereignty, Ownership, Locality, and Retention
  - Industry Compliance Standards: SOC 2, PCI DSS, ISO 27001, and CSA

- Applied activity: Learners review a short scenario describing a company storing regulated customer data across multiple countries and identify the data sovereignty and compliance considerations that apply, then walk a described vulnerability through the management life cycle from identification to remediation.

Module 13: Identity and Access Management in the Cloud

- Lessons:
  - Secure Access to the Cloud Management Environment
  - Secure Access to Cloud Resources: SSH, RDP, and Bastion Hosts
  - Authentication Models: Federation, SAML, and MFA

- Authorization Models: RBAC and OAuth 2.0
- Accounting and Audit Trails

- Applied activity: Learners review a short scenario describing a company setting up access for employees, external partners, and automated scripts and select the appropriate authentication and authorization model for each group.

Module 14: Security Best Practices, Controls, and Attack Monitoring

- Lessons:
  - Zero Trust, Benchmarks, and Hardening
  - Encryption, Secrets Management, and API Security
  - Container and Storage Security
  - Cloud Security Controls: DLP, IPS/IDS, DDoS Protection, and Firewalls
  - Monitoring for Suspicious Activity and Common Attack Types

- Applied activity: Learners review a short scenario describing a cloud environment with several described weaknesses, including an overly permissive IAM policy, an unencrypted storage bucket, and an unpatched container image, and identify which security best practice or control addresses each weakness, then identify the attack type suggested by a described set of suspicious activity indicators.

Module 15: DevOps Fundamentals: Source Control, CI/CD, and Tools

- Lessons:
  - Source Control Concepts
  - CI/CD Pipeline Concepts: Build, Test, and Deploy
  - Integration of Systems: REST, SOAP, and GraphQL
  - DevOps Tools for Automation and Configuration
  - DevOps Tools for Monitoring, Orchestration, and CI/CD

- Applied activity: Learners review a short scenario describing a development team's manual, error-prone release process and identify which source control practice, CI/CD pipeline stage, or DevOps tool would address each described pain point.

Module 16: Troubleshooting Cloud Deployment, Network, and Security Issues

- Lessons:
  - Troubleshooting Deployment Issues: Misconfigurations and Resource Limits
  - Troubleshooting Outages and Regional Service Availability
  - Troubleshooting Network Issues: Service Unavailability and Performance
  - Troubleshooting Routing and Switching Issues
  - Troubleshooting Security Issues

- Applied activity: Learners review a short, described set of symptoms for a failed deployment, a network connectivity complaint, and a suspicious access pattern, and classify each as a deployment, network, or security issue, then identify the most likely specific cause.