CompTIA Cloud+ Certification Exam Objectives

EXAM NUMBER: CV0-004

About the Exam

The CompTIA Cloud+ certification exam will certify the successful candidate has the knowledge and skills required to:

- Understand cloud architecture and design concepts.
- Implement and maintain a secure cloud environment.
- Successfully provision and configure cloud resources.
- Demonstrate the ability to manage operations throughout the cloud environment life cycle using observability, scaling, and automation.
- Understand fundamental DevOps concepts related to deployment and integration.
- Troubleshoot common issues related to cloud management.

ANSI ACCREDITATION

The CompTIA Cloud+ exam is accredited by ANSI to show compliance with the ISO 17024 standard and, as such, undergoes regular reviews and updates to the exam objectives.

EXAM DEVELOPMENT

CompTIA exams result from subject matter expert workshops and industry-wide survey results regarding the skills and knowledge required of an IT professional.

COMPTIA AUTHORIZED MATERIALS USE POLICY

CompTIA Certifications, LLC is not affiliated with and does not authorize, endorse, or condone utilizing any content provided by unauthorized third-party training sites (aka "brain dumps"). Individuals who utilize such materials in preparation for any CompTIA examination will have their certifications revoked and be suspended from future testing in accordance with the CompTIA Candidate Agreement. In an effort to more clearly communicate CompTIA's exam policies on use of unauthorized study materials, CompTIA directs all certification candidates to the CompTIA Certification Exam Policies. Please review all CompTIA policies before beginning the study process for any CompTIA exam. Candidates will be required to abide by the CompTIA Candidate Agreement. If a candidate has a question as to whether study materials are considered unauthorized (aka "brain dumps"), they should contact CompTIA at examsecurity@comptia.org to confirm.

PLEASE NOTE

The lists of examples provided in bulleted format are not exhaustive lists. Other examples of technologies, processes, or tasks pertaining to each objective may also be included on the exam, although not listed or covered in this objectives document. CompTIA is constantly reviewing the content of our exams and updating test questions to be sure our exams are current, and the security of the questions is protected. When necessary, we will publish updated exams based on existing exam objectives. Please know that all related exam preparation materials will still be valid.

TEST DETAILS

Required exam	CV0-004
Number of questions	Maximum of 90
Types of questions	Multiple-choice and performance-based
Length of test	90 minutes
Recommended experience	• 2–3 years of hands-on experience as a systems administrator or cloud engineer • CompTIA Network+ and Server+ or equivalent knowledge
Passing score	750

EXAM OBJECTIVES (DOMAINS)

The table below lists the domains measured by this examination and the extent to which they are represented.

DOMAIN		PERCENTAGE OF EXAMINATION
1.0	Cloud Architecture	23%
2.0	Deployment	19%
3.0	Operations	17%
4.0	Security	19%
5.0	DevOps Fundamentals	10%
6.0	Troubleshooting	12%
Total		**100%**

1.0 Cloud Architecture

1.1 Given a scenario, use the appropriate cloud service model.

- Cloud service models
  - Infrastructure as a service (IaaS)
  - Platform as a service (PaaS)
  - Software as a service (SaaS)
  - Function as a service (FaaS)
- Shared responsibility model

1.2 Explain concepts related to service availability.

- Resource availability
  - Region
  - Availability zone
  - Cloud bursting
  - Edge computing
  - Availability monitoring
- Disaster recovery (DR)
  - Recovery time objective (RTO)
  - Recovery point objective (RPO)
  - Hot site
  - Warm site
  - Cold site
- Multicloud tenancy

1.3 Explain cloud networking concepts.

- Public and private connections to the cloud
  - Virtual private network (VPN)
  - Dedicated connections
- Network functions, components, and services
  - Application load balancer
  - Network load balancer
  - Application gateway
  - Content delivery network (CDN)
  - Firewalls
  - Virtual private cloud (VPC)
    - Peering
    - Transit gateway
  - Subnets
  - Routing and switching
    - Virtual local area network (VLAN)
    - Softwaredefined network (SDN)
    - Border Gateway Protocol (BGP)
    - Static routes
    - Route tables

1.4 Compare and contrast storage resources and technologies.

- Tiered storage
  - Hot
  - Warm
  - Cold
  - Archive
- Disk types
  - Solid-state drive (SSD)
  - Hard disk drive (HDD)
- Storage types
  - Object storage
  - Block storage
  - File storage
- Performance implications
- Cost implications

1.5 Explain the purpose of cloud-native design concepts.

- Cloud-provided managed services
- Microservices
- Loosely coupled architecture
- Fan-out
- Service discovery

1.6 Compare and contrast containerization concepts.

- Stand-alone
- Workload orchestration
- Networking
  - Port mapping
- Storage types
  - Persistent volumes
  - Ephemeral storage
- Image registries

1.7 Compare and contrast virtualization concepts.

- Stand-alone
- Clustering
- Cloning
- Host affinity
- Hardware pass-through
- Network types
  - Overlay networks
  - Virtual machine (VM) networks
- Storage
  - Local
  - Storage area network (SAN)
  - Network-attached storage (NAS)

1.8 Summarize cost considerations related to cloud usage.

- Billing models
  - Dedicated host
  - Reserved resources
  - Pay-as-you-go
  - Spot instance
- Resource metering
- Tagging
- Rightsizing

1.9 Explain the importance of database concepts.

- Types
  - Relational
  - Non-relational
- Deployment options
  - Self-managed
  - Provider-managed

1.10 Compare and contrast methods for optimizing workloads using cloud resources.

- Compute resources
  - VM
  - Container
  - Serverless
- Orchestration
- Workflow
- Network
  - Latency
  - Throughput
- Storage
  - Input/output operations per second (IOPS)
  - Throughput
- Managed services

1.11 Identify evolving technologies in the cloud.

- Machine learning and artificial intelligence (AI)
  - Text recognition
  - Text translation
  - Visual recognition
  - Sentiment analysis
  - Voice-to-text
  - Text-to-voice
  - Generative AI
- Internet of Things (IoT)
  - Sensors
  - Gateways
  - Communication
  - Transmission protocols

2.0 Deployment

2.1 Compare and contrast cloud deployment models.

- Public
- Private
  - On premises
- Hybrid
- Community

2.2 Given a scenario, implement appropriate deployment strategies.

- Blue-green
- Canary
- Rolling
- In-place

2.3 Summarize aspects of cloud migration.

- Migration types
  - On-premises–to-cloud
  - Cloud-to–on-premises
  - Cloud-to-cloud
- Resource allocation
- Considerations
  - Storage
  - Platform compatibility
  - Compute
  - Cost
  - Networking
  - Management overhead
  - Service availability
  - Vendor lock-in
  - Environmental
    - Power and cooling
  - Regulatory
  - Compliance
- Application migration strategies
  - Rehost
  - Replatform
  - Re-architect
  - Retain
  - Retire
  - Refactor

2.4 Given a scenario, use code to deploy and configure cloud resources.

- Infrastructure as code (IaC)
- Configuration as code (CaC)
- Scripting logic
  - Variables
  - Conditionals
  - Operators
  - Data types
  - Functions
- Repeatability
- Drift detection
- Versioning
- Testing
- Documentation
- Formats
  - JavaScript Object Notation (JSON)
  - Yet Another Markup Language (YAML)

2.5 Given a set of requirements, provision the appropriate cloud resources.

- Storage requirements
- Performance requirements
- Security requirements
- Cost requirements
- Availability requirements
- Compliance requirements
- Network requirements
- Compute requirements

3.0 Operations

3.1 Given a scenario, configure appropriate resources to achieve observability.

- Logging
  - Collection
  - Aggregation
  - Retention
- Tracing
- Monitoring
  - Metrics
- Alerting
  - Triage
  - Response

3.2 Given a scenario, configure appropriate scaling approaches.

- Approaches
  - Triggered
    - Trending
    - Load
    - Event
  - Scheduled
  - Manual
- Types
  - Horizontal
  - Vertical

3.3 Given a scenario, use appropriate backup and recovery methods.

- Backup types
  - Incremental
  - Full
  - Differential
- Backup locations
  - On site
  - Off site
- Schedule
- Retention
- Replication
- Encryption
- Testing
  - Recoverability
  - Integrity
- Recovery types
  - In-place
  - Parallel
- Recovery options
  - Bulk
  - Granular

3.4 Given a scenario, manage the life cycle of cloud resources.

- Patches
- Updates
  - Major
  - Minor
- Testing
- Data
  - Ephemeral
  - Persistent
- Decommissioning
  - End of life
  - End of support

4.0 Security

4.1 Explain vulnerability management concepts.

- Steps
  - Scanning scope
  - Identification
  - Assessment
  - Remediation
- Common Vulnerabilities and Exposures (CVEs)

4.2 Compare and contrast aspects of compliance and regulation.

- Data sovereignty
- Data ownership
- Data locality
- Data classification
- Data retention
  - Litigation hold
  - Contractual
  - Regulatory
- Industry standards
  - Systems and Organization Controls 2 (SOC2)
  - Payment Card Industry Data Security Standards (PCI DSS)
  - International Organization for Standardization (ISO) 27001
  - Cloud Security Alliance

4.3 Given a scenario, implement identity and access management.

- Secure access to the cloud management environment
  - Programmatic access
    - Application programming interface (API)
    - Software development kit (SDK)
  - Common Language Infrastructure (CLI)
  - Web portal
- Secure access to the cloud resources
  - API
  - Secure Shell (SSH)
  - Remote Desktop Protocol (RDP)
  - Bastion host
- Authentication models
  - Local users
  - Federation
    - Security Assertion Markup Language (SAML)
  - Token-based
  - Directory-based
  - Multifactor authentication (MFA)
  - OpenID Connect
- Authorization models
  - Role-based access control
  - Group-based access control
  - OAuth 2.0
  - Discretionary
- Accounting
  - Audit trail

4.4 Given a scenario, apply security best practices.

- Zero Trust
- Benchmark
  - Center for Internet Security (CIS)
  - Vendor-specific
- Hardening
- Patching
- Encryption
  - Data in transit
  - Data at rest
- Secrets management
- API security
- Principle of least privilege
- Container security
  - Privileged
  - Unprivileged
  - File access permissions
- Storage security
  - Object storage
  - File storage

4.5 Given a scenario, apply security controls in the cloud.

- Endpoint protection
- Data loss prevention (DLP)
- Intrusion prevention system/intrusion detection system (IPS/IDS)
- Distributed denial-of-service (DDoS) protection
- Identity and access management (IAM) policies
- Firewall
  - Network access control list (ACL)
  - Web application firewall (WAF)
  - Network security group

4.6 Given a scenario, monitor suspicious activities to identify common attacks.

- Event monitoring
- Deviation from the baseline
- Unnecessary open ports
- Attack types
  - Vulnerability exploitation
    - Human error
    - Outdated software
  - Social engineering
    - Phishing
  - Malware
    - Ransomware
  - DDoS
  - Cryptojacking
  - Zombie instances
  - Metadata

5.0 DevOps Fundamentals

5.1 Explain source control concepts.

- Version management
- Code review
- Pull request
- Code push
- Code commit
- Code merge
- Branch management

5.2 Explain concepts related to continuous integration/continuous deployment (CI/CD) pipelines.

- Automation
- Code integration
- Code deployment
  - Build
- Testing
- Security
- Workflow
- Artifacts
  - Images
    - VM
    - Container
  - Packages
    - Red Hat Package Manager (RPM)
    - Debian
    - ZIP
    - tar
  - Flat file
- Repositories
  - Public
  - Private

5.3 Explain concepts related to integration of systems.

- Event-driven architectures
- Web services
  - Representational State Transfer (REST)
  - Simple Object Access Protocol (SOAP)
  - Remote procedure call (RPC)
- Web sockets
- GraphQL

5.4 Explain the importance of tools used in DevOps environments.

- Ansible
- Docker
- Elasticsearch, Logstash, and Kibana (ELK) stack
- Git
- GitHub actions
- Grafana
- Jenkins
- Kubernetes
- Terraform

6.0 Troubleshooting

6.1 Given a scenario, troubleshoot deployment issues.

- Incompatibility
- Misconfigurations
  - Resource allocation
  - Permission issues
  - Oversubscription
  - Sizing issues
- Outdated component definitions
- Deprecation of functionality
- Outages
  - Full
  - Partial
- Resource limits
  - API throttling
  - Service quotas
- Regional service availability

6.2 Given a scenario, troubleshoot network issues.

- Network service unavailability
  - Dynamic Host Configuration Protocol (DHCP)
  - Domain Name System (DNS)
  - Network Time Protocol (NTP)
  - Network Address Translation (NAT)
  - Hypertext Transfer Protocol (HTTP)
    - Status codes
- Latency
- Bandwidth/throughput issues
- Network device misconfiguration
- Protocol incompatibility
- Protocol deprecations
- IP addressing issues
  - Scope exhaustion
  - Network overlap
- Routing issues
  - Missing routes
  - Misconfigured routes
- Switching issues
  - VLAN issues
    - Misconfigured tags
  - Access vs. trunk ports

6.3 Given a scenario, troubleshoot security issues.

- Cipher suite deprecations
- Authorization issues
  - Privilege escalation
  - Unauthorized access
- Authentication issues
  - Leaked credentials
- Software vulnerability issues
- Unauthorized software

CompTIA Cloud+ CV0-004 Acronym List

The following is a list of acronyms that appears on the CompTIA Cloud+ CV0-004 exam. Candidates are encouraged to review the complete list and attain a working knowledge of all listed acronyms as part of a comprehensive exam preparation program.

ACRONYM	DEFINITION
ACL	Access Control List
AES	Advanced Encryption Standard
AI	Artificial Intelligence
API	Application Programming Interface
AZ	Availability Zone
BGP	Border Gateway Protocol
BYOD	Bring Your Own Device
CaC	Configuration as Code
CDN	Content Delivery Network
CI/CD	Continuous Integration/Continuous Deployment
CIS	Center for Internet Security
CLI	Common Language Infrastructure
CPU	Central Processing Unit
CRM	Customer Relationship Management
CRUD	Create, Read, Update, Delete
CSA	Cloud Security Alliance
CSP	Cloud Service Provider
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
CWE	Common Weakness Enumeration
CWSS	Common Weakness Scoring System
DBaaS	Database as a Service
DDoS	Distributed Denial of Service
DHCP	Dynamic Host Configuration Protocol
DLP	Data Loss Prevention
DNS	Domain Name System
DR	Disaster Recovery
DSS	Data Security Standard
ELK	Elasticsearch, Logstash, and Kibana
FaaS	Function as a Service
GDPR	General Data Protection Regulation
GPU	Graphics Processing Unit
HDD	Hard Disk Drive
HTTP	Hypertext Transfer Protocol
IaaS	Infrastructure as a Service
IaC	Infrastructure as Code
IAM	Identity and Access Management
ICMP	Internet Control Management Protocol
IDS	Intrusion Detection System
IOPS	Input/Output Operations Per Second
IP	Internet Protocol
IPS	Intrusion Prevention System
iSCSI	Internet Small Computer System Interface

ACRONYM	DEFINITION
ISO	International Organization for Standardization
ISP	Internet Service Provider
ITIL	Information Technology Infrastructure Library
JSON	JavaScript Object Notation
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LUN	Logical Unit Number
MFA	Multifactor Authentication
ML	Machine Learning
MTU	Maximum Transmission Unit
NAS	Network Attached Storage
NAT	Network Address Translation
NIC	Network Interface Card
NoSQL	Not Only Structured Query Language
NTP	Network Time Protocol
NVME	Non-volatile Memory Express
OAuth	Open Authorization
OIDC	OpenID Connect Protocol
OS	Operating System
PaaS	Platform as a Service
PCI	Payment Card Industry
RACI	Responsible, Accountable, Consulted, Informed
RAID	Redundant Array of Inexpensive Disks
RAM	Random-access Memory
RDP	Remote Desktop Protocol
REST	Representational State Transfer
RPC	Remote Procedure Call
RPM	Red Hat Package Manager
RPO	Recovery Point Objective
RTMP	Real-time Messaging Protocol
RTO	Recovery Time Objective
SaaS	Software as a Service
SAML	Security Assertion Markup Language
SAN	Storage Area Network
SDK	Software Development Kit
SDN	Software-defined Network
SOAP	Simple Object Access Protocol
SOC2	System and Organization Controls 2
SQL	Structured Query Language
SSD	Solid-state Drive
SSH	Secure Shell
SSL	Secure Sockets Layer
SSO	Single Sign-On
STAR	Security, Trust, Assurance, Risk
TCP	Transmission Control Protocol
TLS	Transport Layer Security
USB	Universal Serial Bus
vCPU	Virtual CPU
VDI	Virtual Desktop Interface
VLAN	Virtual LAN
VM	Virtual Machine
vNIC	Virtual NIC
VPC	Virtual Private Cloud
VPN	Virtual Private Network
WAF	Web Application Firewall

CompTIA Cloud+ CV0-004 Hardware and Software List

CompTIA has included this sample list of hardware and software to assist candidates as they prepare for the Cloud+ CV0-004 certification exam. This list may also be helpful for training companies that wish to create a lab component for their training offering. The bulleted lists below each topic are sample lists and are not exhaustive.

HARDWARE

- Cables*
- Compute (CPU, RAM, etc.)*
- Computer capable of running virtualization
- NAS or SAN*
- Network router*
- Network switch*

SOFTWARE

- Automation tools
- CLI*
- Client (and server) Operating System (OS)
- Hypervisor (Type 1, Type 2)
- Various web browsers
- Virtualization format converter*

OTHER

- Internet access
- Access to SaaS, PaaS, or IaaS environments
- Remote access to cloud service providers (trial or free service)

**Ideal, but not necessary for lab setup*