CompTIA

CV0-003 vs CV0-002 Exam Objectives Comparison

As organizations leverage the benefits of the cloud, the need for skilled IT professionals to deploy and automate secure solutions is increasing. The rise of a remote workforce and emerging technologies make it imperative for IT professionals to have the skillset sought by organizations to secure environments, while providing constant availability to data and applications. Updates to CompTIA Cloud+ reflect current competencies relevant to job roles tasked with managing and optimizing infrastructure services.

The new CompTIA Cloud+ CV0-003 certification validates the skills necessary for cloud engineers and IT professionals to deploy, optimize, and troubleshoot cloud instances and solutions. New objectives reflect the increased importance of scalability, high availability, and the various cloud models that have emerged from different vendor solutions. The CV0-003 Cloud+ objectives emphasize a vendor-neutral, multicloud approach to meet business needs.

CompTIA Cloud+

Exam Objectives Comparison

Cloud+ CV0-003 contains five domains (the same number as the previous version). The main differences are an increased emphasis on security and more content on cloud architectures. CV0-003 contains 27 objectives, as compared to 32 on the previous version. The change does not indicate a significant decrease of content, but instead is due to streamlining grouped technologies into related objectives.

The following table aligns exam objectives from CV0-002 to CV0-003 for comparison. Skills are aligned by best match.

CV0-003	CV0-002	COMMENTS
1.1 Compare and contrast the different types of cloud models.		New content that examines validates high-level knowledge of cloud services and solutions.
1.2 Explain the factors that contribute to capacity planning.		Cloud solutions often feature analytics that can inform cost-saving, this objective introduces these concepts to the exam.
1.3 Explain the importance of high availability and scaling in cloud environments.		Two key features of the cloud are high availability and scalability. They are now covered in depth on Cloud+.
1.4 Given a scenario, analyze the solution design in support of the business requirements.	1.1 Given a scenario, analyze system requirements to ensure successful system deployment.	
2.1 Given a scenario, configure identity and access management.	2.2 Given a scenario, apply the appropriate ACL to the target objects to meet access requirements according to a security template.	
2.1 Given a scenario, configure identity and access management.	2.3 Given a cloud service model, implement defined security technologies to meet given security requirements.	
2.2 Given a scenario, secure a network in a cloud environment.	2.1 Given a scenario, apply security configurations and compliance controls to meet given cloud infrastructure requirements.	
2.2 Given a scenario, secure a network in a cloud environment	2.2 Given a scenario, apply the appropriate ACL to the target objects to meet access requirements according to a security template.	
2.2 Given a scenario, secure a network in a cloud environment.	2.3 Given a cloud service model, implement defined security technologies to meet given security requirements.	
2.3 Given a scenario, apply the appropriate OS and application security controls.	2.2 Given a scenario, apply the appropriate ACL to the target objects to meet access requirements according to a security template.	
2.3 Given a scenario, apply the appropriate OS and application security controls.	2.3 Given a cloud service model, implement defined security technologies to meet given security requirements.	

CV0-003	CV0-002	COMMENTS
2.3 Given a scenario, apply the appropriate OS and application security controls.	2.1 Given a scenario, apply security configurations and compliance controls to meet given cloud infrastructure requirements.	
2.4 Given a scenario, apply data security and compliance controls in cloud environments.	2.1 Given a scenario, apply security configurations and compliance controls to meet given cloud infrastructure requirements.	
2.4 Given a scenario, apply data security and compliance controls in cloud environments.	2.3 Given a cloud service model, implement defined security technologies to meet given security requirements.	
2.5 Given a scenario, implement measures to meet security requirements.	2.1 Given a scenario, apply security configurations and compliance controls to meet given cloud infrastructure requirements.	
2.5 Given a scenario, implement measures to meet security requirements.	2.3 Given a cloud service model, implement defined security technologies to meet given security requirements.	
2.5 Given a scenario, implement measures to meet security requirements.	2.4 Given a cloud service model, apply the appropriate security automation technique to the target system.	
2.6 Explain the importance of incident response procedures.		This objective reflects the increased management role of cloud engineers and the importance of the cloud as relates to business outcomes after an incident.
3.1 Given a scenario, integrate components into a cloud solution.		New content area that emphasizes the changing technology solutions in the cloud, especially scaling, containers, and subscription models.
3.2 Given a scenario, provision storage in cloud environments.	1.7 Given a scenario, analyze the appropriate storage type and protection capability for a provided deployment.	
3.3 Given a scenario, deploy cloud networking solutions.	1.5 Given a scenario, analyze sizing, subnetting, and basic routing for a provided deployment of the virtual network.	
3.4 Given a scenario, configure the appropriate compute sizing for a deployment.	1.6 Given a scenario, analyze CPU and memory sizing for a provided deployment.	

CV0-003	CV0-002	COMMENTS
3.5 Given a scenario, perform cloud migrations.	1.8 Given a scenario, analyze characteristics of the workload (storage, network, compute) to ensure a successful migration.	
4.1 Given a scenario, configure logging, monitoring, and alerting to maintain operational status.	3.6	
4.1 Given a scenario, configure logging, monitoring, and alerting to maintain operational status.	4.1	
4.2 Given a scenario, maintain efficient operation of a cloud environment.	3.1	
4.2 Given a scenario, maintain efficient operation of a cloud environment.	3.3	
4.3 Given a scenario, optimize cloud environments.	3.6	
4.3 Given a scenario, optimize cloud environments.	4.2	
4.3 Given a scenario, optimize cloud environments.	4.3	
4.3 Given a scenario, optimize cloud environments.	4.5	
4.3 Given a scenario, optimize cloud environments.	4.6	
4.4 Given a scenario, apply proper automation and orchestration techniques.	3.2	
4.4 Given a scenario, apply proper automation and orchestration techniques.	3.6	
4.5 Given a scenario, perform appropriate backup and restore operations.	3.3	
4.6 Given a scenario, perform disaster recovery tasks.	3.3	
4.6 Given a scenario, perform disaster recovery tasks.	3.5	
5.1 Given a scenario, use the trouble-shooting methodology to resolve cloud-related issues.	5.6 Given a scenario, explain the trouble-shooting methodology.	
5.2 Given a scenario, troubleshoot security issues.	5.5 Given a scenario, troubleshoot security issues.	
5.3 Given a scenario, troubleshoot deployment issues.	5.1 Given a scenario, troubleshoot a deployment issue.	

CV0-003	CV0-002	COMMENTS
5.4 Given a scenario, troubleshoot connectivity issues.	5.4 Given a scenario, troubleshoot connectivity issues.	
5.5 Given a scenario, troubleshoot common performance issues.	4.6 Given a specific environment and related data (e.g., performance, capacity, trends), apply appropriate changes to meet expected criteria.	Additional content in this objective includes resource utilization and load balancing; the cognitive level has also increased to highlight the hand-on technical nature of cloud troubleshooting.
5.5 Given a scenario, troubleshoot common performance issues.	5.2 Given a scenario, troubleshoot common capacity issues.	
5.6 Given a scenario, troubleshoot automation or orchestration issues.	5.3 Given a scenario, troubleshoot automation/orchestration issues.	