

CV0-004^{Q&As}

CompTIA Cloud+ (2024)

Pass CompTIA CV0-004 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.leads4pass.com/cv0-004.html>

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CompTIA
Official Exam Center

-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers



QUESTION 1

A database analyst reports it takes two hours to perform a scheduled job after onboarding 10,000 new users to the system. The analyst made no changes to the scheduled job before or after onboarding the users. The database is hosted in an IaaS instance on a cloud provider.

Which of the following should the cloud administrator evaluate to troubleshoot the performance of the job?

- A. The IaaS compute configurations, the capacity trend analysis reports, and the storage IOPS
- B. The hypervisor logs, the memory utilization of the hypervisor host, and the network throughput of the hypervisor
- C. The scheduled job logs for successes and failures, the time taken to execute the job, and the job schedule
- D. Migrating from IaaS to on premises, the network traffic between on-premises users and the IaaS instance, and the CPU utilization of the hypervisor host

Correct Answer: A

To troubleshoot the performance of a scheduled job that takes two hours to run after onboarding 10,000 new users to a cloud-based system, the administrator should evaluate the IaaS compute configurations, the capacity trend analysis reports, and the storage IOPS. These factors can affect the performance of a database job in an IaaS instance on a cloud provider. The IaaS compute configurations include the CPU, memory, and network resources assigned to the instance. The capacity trend analysis reports show the historical and projected usage and demand of the resources. The storage IOPS (Input/Output Operations Per Second) measure the speed and performance of the disk storage. The administrator should check if these factors are sufficient, optimal, or need to be adjusted to improve the performance of the job.

QUESTION 2

A cross-site request forgery vulnerability exploited a web application that was hosted in a public IaaS network. A security engineer determined that deploying a WAF in blocking mode at a CDN would prevent the application from being exploited again. However, a week after implementing the WAF, the application was exploited again. Which of the following should the security engineer do to make the WAF control effective?

- A. Configure the DDoS protection on the CDN.
- B. Install endpoint protection software on the VMs
- C. Add an ACL to the VM subnet.
- D. Deploy an IDS on the IaaS network.

Correct Answer: C

After a WAF deployment fails to prevent an exploit, adding an Access Control List (ACL) to the Virtual Machine (VM) subnet can be an effective control. ACLs provide an additional layer of security by explicitly defining which traffic can or cannot enter a network segment. By setting granular rules based on IP addresses, protocols, and ports, ACLs help to restrict access to resources, thereby mitigating potential exploits and enhancing the security of the IaaS network. References: CompTIA Cloud+ materials cover governance, risk, compliance, and security for the cloud, including the implementation of network security controls like ACLs, to protect cloud environments from unauthorized access and potential security threats.

QUESTION 3

A systems administrator is planning to deploy a database cluster in a virtualization environment. The administrator needs to ensure the database nodes do not exist on the same physical host.

Which of the following would best meet this requirement?

- A. Oversubscription
- B. Anti-affinity
- C. A firewall
- D. A separate cluster

Correct Answer: B

Anti-affinity is a rule that specifies that certain virtual machines should not run on the same physical host. This can help to improve availability and performance by avoiding single points of failure and resource contention. For example, if the

database nodes are running on the same host and the host fails, the entire database cluster will be unavailable. By using anti-affinity rules, the systems administrator can ensure the database nodes are distributed across different hosts in the

virtualization environment. References:

CompTIA Cloud+ CV0-003 Study Guide, Chapter 2: Deploying a Cloud Environment, page 76.

QUESTION 4

A cloud engineer is designing a cloud-native, three-tier application. The engineer must adhere to the following security best practices:

1.
Minimal services should run on all layers of the stack.
2.
The solution should be vendor agnostic.
3.
Virealization could be used over physical hardware.

Which of the following concepts should the engineer use to design the system to best meet these requirements?

- A. Virtual machine
- B. Micro services
- C. Fan-out

D. Cloud-provided managed services

Correct Answer: B

Microservices architecture is the most suitable design principle that aligns with the security best practices mentioned. It involves developing a suite of small services, each running in its own process and communicating with lightweight mechanisms, often an HTTP resource API. This architecture minimizes the services running on each layer, allows for vendor-agnostic solutions, and is well-suited for virtualization over physical hardware. References: Microservices as an architectural approach is discussed in the context of cloud-native applications within the CompTIA Cloud+ material.

QUESTION 5

An organization's internal security team mandated that public cloud resources must be accessible only by a corporate VPN and not by direct public internet access.

Which of the following would achieve this objective?

- A. WAF
- B. ACL
- C. VPC
- D. SSH

Correct Answer: C

A Virtual Private Cloud (VPC) allows users to create a secluded section of the public cloud where resources can be launched in a defined virtual network. This enables an organization to have a section of the cloud that is secured and isolated from the public internet, thus, access to public cloud resources can be restricted to only a corporate VPN. References: CompTIA Cloud+ Study Guide (V0-004) - Chapter on Cloud Security

[CV0-004 PDF Dumps](#)

[CV0-004 Practice Test](#)

[CV0-004 Exam Questions](#)