

100% Money Back
Guarantee

Vendor:CompTIA

Exam Code:CV0-003

Exam Name:CompTIA Cloud+ Certification

Version:Demo

QUESTION 1

A company has a web application that is accessed around the world. An administrator has been notified of performance issues regarding the application. Which of the following will BEST improve performance?

- A. IPAM
- B. SDN
- C. CDN
- D. VPN

Correct Answer: C

Reference: <https://www.cloudflare.com/learning/cdn/what-is-a-cdn/>

QUESTION 2

A cloud administrator is provisioning five VMs, each with a minimum of 8GB of RAM and a varying load throughout the day. The hypervisor has only 32GB of RAM. Which of the following features should the administrator use?

- A. Memory overcommitment
- B. Thin-provisioned model
- C. Process scheduling
- D. Hyperthreading

Correct Answer: C

QUESTION 3

A cloud administrator configured a local cloud-resource pool to offer 64GB of memory, 64 cores, and 640GB of storage. Thirty-two machines with identical resource allocations are started, but one machine is unable to handle requests. Which of the following is the MOST likely cause?

- A. Insufficient guest bandwidth
- B. Overwhelmed vCPU
- C. A storage error on the guest
- D. Incorrect VLAN assignment
- E. Inadequate memory allocation

Correct Answer: E

QUESTION 4

Which of the following cloud deployment models allows a company to have full control over its IT infrastructure?

- A. Private
- B. Cloud within a cloud
- C. Hybrid
- D. Public

Correct Answer: A

A private cloud is a type of cloud deployment model that provides cloud services exclusively to a single organization or tenant. A private cloud allows a company to have full control over its IT infrastructure, as it can customize, configure, manage, and secure its own cloud environment according to its specific needs and preferences. A private cloud can also offer higher performance, reliability, and privacy than other cloud deployment models, as it does not share resources or data with other customers. References: CompTIA Cloud+ Certification Exam Objectives, page 8, section 1.2 Reference: <https://www.sciencedirect.com/topics/computer-science/private-cloud>

QUESTION 5

A cloud administrator is setting up a DR site on a different zone of the same CSP. The application servers are replicated using the VM replication, and the database replication is set up using log shipping. Upon testing the DR site, the application servers are unable to access the database servers. The administrator has verified the systems are running and are accessible from the CSP portal.

Which of the following should the administrator do to fix this issue?

- A. Change the database application IP
- B. Create a database cluster between the primary site and the DR site
- C. Update the connection string
- D. Edit the DNS record at the DR site for the application servers

Correct Answer: C

A connection string is a parameter that specifies how to connect to a database server or instance. A connection string typically includes information such as the server name, database name, user name, password, and other options. Updating the connection string is the best way to fix the issue of application servers being unable to access the database servers after setting up a DR site on a different zone of the same CSP and replicating the application and database servers using VM replication and log shipping. Updating the connection string can ensure that the application servers can connect to the correct database server or instance in the DR site, as the server name or IP address may have changed after the replication. References: CompTIA Cloud+ Certification Exam Objectives, page 10, section 1.5

QUESTION 6

Which of the following actions should a systems administrator perform during the containment phase of a security

incident in the cloud?

- A. Deploy a new instance using a known-good base image.
- B. Configure a firewall rule to block the traffic on the affected instance.
- C. Perform a forensic analysis of the affected instance.
- D. Conduct a tabletop exercise involving developers and systems administrators.

Correct Answer: B

Configuring a firewall rule to block the traffic on the affected instance is what the administrator should perform during the containment phase of a security incident in the cloud. A security incident is an event or situation that affects or may affect the confidentiality, integrity, or availability of cloud resources or data. A security incident response is a process of managing and resolving a security incident using various phases, such as identification, containment, eradication, recovery, etc. The containment phase is where the administrator tries to isolate and prevent the spread or escalation of the security incident. Configuring a firewall rule to block the traffic on the affected instance can help to contain a security incident by cutting off any communication or interaction between the instance and other systems or networks, which may stop any malicious or unauthorized activity or access.

QUESTION 7

Which of the following are advantages of a public cloud? (Choose two.)

- A. Full control of hardware
- B. Reduced monthly costs
- C. Decreased network latency
- D. Pay as you use
- E. Availability of self-service
- F. More secure data

Correct Answer: BD

Reference: <https://services.global.ntt/ja-jp/insights/blog/5-benefits-of-public-cloud-computing>

QUESTION 8

Which of the following is a best practice used in relation to MTBF?

- A. Determine backup schedule based on uptime requirements
- B. Proactively replace components before they fail
- C. Determine downtime to perform a system recovery
- D. Reactively replace components after failure

Correct Answer: B

QUESTION 9

A security audit related to confidentiality controls found the following transactions occurring in the system:

GET http://gateway.securetransaction.com/privileged/api/v1/changeResource?id=123anduser=277

Which of the following solutions will solve the audit finding?

- A. Using a TLS-protected API endpoint
- B. Implementing a software firewall
- C. Deploying a HIDS on each system
- D. Implementing a Layer 4 load balancer

Correct Answer: A

Reference: https://cheatsheetseries.owasp.org/cheatsheets/Transport_Layer_Protection_Cheat_Sheet.html

QUESTION 10

A cloud administrator is setting up a new coworker for API access to a public cloud environment. The administrator creates a new user and gives the coworker access to a collection of automation scripts. When the coworker attempts to use a deployment script, a 403 error is returned. Which of the following is the MOST likely cause of the error?

- A. Connectivity to the public cloud is down.
- B. User permissions are not correct.
- C. The script has a configuration error.
- D. Oversubscription limits have been exceeded.

Correct Answer: B

User permissions are not correct is the most likely cause of the error 403 (Forbidden) that is returned when a coworker attempts to use a deployment script after being set up for API access to a public cloud environment by an administrator. API (Application Programming Interface) is a set of rules or specifications that defines how different software components or systems can communicate and interact with each other. API access is the ability to use or access an API to perform certain actions or tasks on a software component or system. User permissions are the settings or policies that control and restrict what users can do or access on a software component or system. User permissions can affect API access by determining what actions or tasks users can perform using an API on a software component or system. User permissions are not correct if they do not match or align with the intended or expected actions or tasks that users want to perform using an API on a software component or system. User permissions are not correct can cause error 403 (Forbidden), which means that the user does not have the necessary permission or authorization to perform the requested action or task using an API on a software component or system.

QUESTION 11

A cloud architect is reviewing four deployment options for a new application that will be hosted by a public cloud provider. The application must meet an SLA that allows for no more than five hours of downtime annually. The cloud architect is reviewing the SLAs for the services each option will use: Based on the information above, which of the following minimally complies with the SLA requirements?

Option A		Option B	
VM servers	99.00%	Container hosting	99.90%
Attached block storage	99.99%	Shared network storage	99.90%
Total uptime	99.00%	Total uptime	99.90%
Option C		Option D	
Container deployment services	99.95%	Container application services	99.99%
Attached block storage	99.99%	Shared network storage	99.99%
Total uptime	99.95%	Total uptime	99.99%

A. Option A

B. Option B

C. Option C

D. Option D

Correct Answer: C

(A)

99.00% uptime annually = 3d, 14h, 56m allowed downtime

(B)

99.90% uptime annually = 8h, 41m allowed downtime

(C)

99.95% uptime annually = 4h, 20m allowed downtime

(D)

99.99% uptime annually = 52m allowed downtime

QUESTION 12

An enterprise is considering a cost model for a DBaaS. Which of the following is BEST for a cloud solution?

A. Per gigabyte

B. Per seat

C. Per user

D. Per device

Correct Answer: A

Reference: <https://www.techtarget.com/searchcloudcomputing/tip/Breaking-down-the-costs-of-cloud-storage>