CV0-003 Q&As

CompTIA Cloud+ Certification

Pass CompTIA CV0-003 Exam with 100% Guarantee

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

https://www.leads4pass.com/cv0-003.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

An IaaS provider has numerous devices and services that are commissioned and decommissioned automatically on an ongoing basis. The cloud administrator needs to implement a solution that will help reduce administrative overhead.

Which of the following will accomplish this task?

A. IPAM

B. NAC

C. NTP

D. DNS

Correct Answer: A

IP address management (IPAM) is a type of tool or system that automates and standardizes the allocation, tracking, and management of IP addresses in an IP network. IPAM can help reduce administrative overhead for an IaaS provider that has numerous devices and services that are commissioned and decommissioned automatically on an ongoing basis, as it can simplify and centralize the process of assigning and reclaiming IP addresses for different devices and services without manual intervention or errors. IPAM can also help optimize network performance and security, as it can monitor and report any issues or conflicts related to IP addresses. References: CompTIA Cloud+ Certification Exam Objectives, page 15, section 2.8

Reference: https://www.infoblox.com/glossary/ipam-ip-address-management/

QUESTION 2

An organization is hosting a cloud-based web server infrastructure that provides web-hosting solutions. Sudden continuous bursts of traffic have caused the web servers to saturate CPU and network utilizations.

Which of the following should be implemented to prevent such disruptive traffic from reaching the web servers?

A. Solutions to perform NAC and DLP

B. DDoS protection

C. QoS on the network

D. A solution to achieve microsegmentation

Correct Answer: B

Distributed denial-of-service (DDoS) protection is a type of security solution that detects and mitigates DDoS attacks that aim to overwhelm or disrupt a system or service by sending large volumes of traffic from multiple sources. DDoS protection can prevent such disruptive traffic from reaching the web servers by filtering out malicious or unwanted traffic and allowing only legitimate traffic to pass through. DDoS protection can also help maintain the availability and functionality of web services and applications during a DDoS attack. References: CompTIA Cloud+ Certification Exam Objectives, page 14, section 2.7 Reference: https://blog.paessler.com/the-top-5-causes-of-sudden-network-spikes

Reference: https://blog.paessler.com/the-top-5-causes-of-sudden-network-spikes

QUESTION 3

A company needs to access the cloud administration console using its corporate identity. Which of the following actions would MOST likely meet the requirements?

A. Implement SSH key-based authentication.

B. Implement cloud authentication with local LDAP.

C. Implement multifactor authentication.

D. Implement client-based certificate authentication.

Correct Answer: D

Implementing client-based certificate authentication is what the administrator should do to access the cloud administration console using corporate identity. Client-based certificate authentication is a method of verifying and authenticating users or devices based on digital certificates issued by a trusted authority. Digital certificates are electronic documents that contain information such as identity, public key, expiration date, etc., that can be used to prove one\\'s identity and establish secure communication over a network. Client-based certificate authentication can allow users or devices to access cloud resources or services using their corporate identity without requiring passwords or other credentials.

QUESTION 4

A systems administrator needs to migrate email services to the cloud model that requires the least amount of administrative effort. Which of the following should the administrator select?

A. DBaaS

B. SaaS

C. IaaS

D. PaaS

Correct Answer: B

The cloud model that requires the least amount of administrative effort to migrate email services is software as a service (SaaS). SaaS is a cloud model that provides applications or software that are hosted and managed by a cloud provider and delivered to users over the internet. SaaS eliminates the need for installing, configuring, updating, or maintaining the software or its underlying infrastructure, as these tasks are handled by the cloud provider. The systems administrator only needs to subscribe to the email service and configure the user accounts and settings. Reference: CompTIA Cloud+ Certification Exam Objectives, Domain 1.0 Configuration and Deployment, Objective 1.4 Given a scenario, execute a provided deployment plan.

QUESTION 5

A systems administrator adds servers to a round-robin, load-balanced pool, and then starts receiving reports of the website being intermittently unavailable. Which of the following is the MOST likely cause of the issue?

A. The network is being saturated.

B. The load balancer is being overwhelmed.

C. New web nodes are not operational.

D. The API version is incompatible.

E. There are time synchronization issues.

Correct Answer: C

New web nodes are not operational is the most likely cause of the issue of website being intermittently unavailable after adding servers to a round-robin, load- balanced pool. A round-robin, load-balanced pool is a method of distributing network traffic evenly and sequentially among multiple servers or nodes that provide the same service or function. A round-robin, load-balanced pool can help to improve performance, availability, and scalability of network applications or services by ensuring that no server or node is overloaded or underutilized. New web nodes are not operational if they are not configured properly or functioning correctly to provide web service or function. New web nodes are not operational can cause website being intermittently unavailable by disrupting the round- robin, load-balanced pool and creating inconsistency or unreliability in web service or function.

QUESTION 6

An organization located in Asia connects to a cloud infrastructure hosted in North America and Europe. Sporadic slowness has been observed when using the PaaS and IaaS components. A diagnostic using the following commands was run, and the following results were collected:

Command	Destination	Observation
PING	<Public IP of Cloud Provider>	• Sporadic timeout • Increased round-trip value 520ms
TRACERT	<Public IP of Cloud Provider>	• Increased round-trip value 520ms

Which of the following is the most likely reason for the latency?

A. Service degradation on the ISP

B. A DDoS attack on the organization\\'s infrastructure

C. Misconfiguration of the network security groups

D. Switch failure at the organization

Correct Answer: A

Explanation: The most likely reason for the latency is service degradation on the ISP. The results show that the ping and traceroute commands have sporadic timeout and increased round-trip values when reaching the public IP address of the cloud provider. This indicates that there is a network issue between the organization and the cloud provider, which could be caused by service degradation on the ISP. Service degradation on the ISP means that the ISP is experiencing reduced performance or availability of its network services, which can affect the quality and speed of the data transmission. Service degradation on the ISP can be caused by various factors, such as congestion, routing problems, hardware failures, or maintenance activities. To resolve this issue, the systems administrator should contact the ISP and

report the problem, and request a status update or a resolution plan. References: CompTIA Cloud+ CV0-003 Certification Study Guide, Chapter 3, Objective 3.2: Given a scenario, troubleshoot network connectivity issues.

QUESTION 7

Which of the following cloud services is fully managed?

A. IaaS

B. GPU in the cloud

C. IoT

D. Serverless compute

E. SaaS

Correct Answer: E

SaaS (Software as a Service) is a cloud service model that provides fully managed applications to the end users. The users do not have to worry about installing, updating, or maintaining the software, as the cloud provider handles all these tasks. Examples of SaaS are Gmail, Office 365, Salesforce, etc.

QUESTION 8

A company has just completed a security audit and received initial results from the auditor. The results show that the ethical hacker was able to gain access to the company servers by exploiting non-hardened VMs and hosts as guests and administrators. Which of the following should be implemented to harden the environment? (Select two.)

A. Discretionary access controls

B. Disable unnecessary accounts

C. Change default passwords

D. Install antivirus software

E. Role-based access controls

Correct Answer: BE

QUESTION 9

A systems administrator is implementing a new file storage service that has been deployed in the company\\'s private cloud instance. The key requirement is fast read/write times for the targeted users, and the budget for this project is not a concern. Which of the following storage types should the administrator deploy?

A. Spinning disks

B. NVMe

C. SSD

D. Hybrid

Correct Answer: B

QUESTION 10

A cloud security analyst is implementing a vulnerability scan of the web server in the DMZ, which is running in an IaaS compute instance. The default inbound firewall settings are as follows:

Protocol	Port	Source	Action
TCP	80	any	allow
TCP	443	any	allow
ICMP	echo request	any	allow
any	any	any	deny

Which of the following will provide the analyst with the MOST accurate report?

A. An agent-based scan

B. A network vulnerability scan

C. A default and common credentialed scan

D. A network credentialed vulnerability scan

Correct Answer: D

Reference: https://docs.tenable.com/nessus/Content/NessusCredentialedChecks.htm

QUESTION 11

A systems administrator receives a ticket stating the following:

“The programming team received an error during the process deploying applications to the container platform. The error after the containerized applications were created”

Which the following should the administrator Check FIRST?

A. The containers

B. The application

C. The Scripts

D. The templates

Correct Answer: A

The correct answer is A. The containers.

The error that the programming team received indicates that the problem occurred after the containerized applications were created, but before they were deployed to the container platform. This suggests that the issue is related to the

containers themselves, not the application, the scripts, or the templates.

The containers are the units of software that package up the application code and all its dependencies, such as libraries, frameworks, and configuration files. The containers run on a container platform, such as Docker or Kubernetes, that

provides the runtime environment and orchestration for the containers. The containers are created from images, which are templates that define how to build and run a container.

The administrator should check the containers first to see if they are configured correctly, if they have any errors or warnings, if they have the necessary resources and permissions, and if they can communicate with each other and with the

container platform. The administrator can use tools such as docker ps, docker logs, docker inspect, and docker exec to examine and troubleshoot the containers.

QUESTION 12

A DevOps administrator is building a new application slack in a private cloud. This application will store sensitive information and be accessible from the internet. Which of the following would be MOST useful in maintaining confidentiality?

A. NAC

B. IDS

C. DLP

D. EDR

Correct Answer: C

The most useful tool in maintaining confidentiality for a new application stack that will store sensitive information and be accessible from the internet is data loss prevention (DLP). DLP is a type of security solution that monitors and controls the flow of data in and out of a system or network. It can detect and prevent unauthorized access, transmission, or leakage of sensitive data, such as personal information, financial records, or intellectual property. DLP can also enforce encryption, masking, or deletion of sensitive data to protect its confidentiality. Reference: CompTIA Cloud+ Certification Exam Objectives, Domain 2.0 Security, Objective 2.5 Given a scenario, apply data security techniques in the cloud.

QUESTION 13

A cloud engineer is performing updates to an application and needs to gracefully stop any new transactions from processing before the updates can be applied. Which of the following steps should the engineer take?

A. Enable maintenance mode from the application dashboard

B. Wait until after business hours to conduct the change when the system is not in use

C. Run a kill command on the system to stop the application services

D. Use a load balancer to redirect traffic to other systems serving the application

Correct Answer: A

The best way to gracefully stop any new transactions from processing before applying updates to an application is to enable maintenance mode from the application dashboard. Maintenance mode is a feature that allows temporarily disabling the access or functionality of an application or service while performing maintenance tasks, such as updates, patches, or backups. It also displays a message or notification to the users or clients informing them about the maintenance and the expected downtime. This method will prevent any new transactions from being initiated or interrupted while the updates are being applied. Reference: [CompTIA Cloud+ Certification Exam Objectives], Domain 3.0 Maintenance, Objective 3.1 Given a scenario, apply appropriate changes to meet performance, security and user requirements.

QUESTION 14

A systems administrator has verified that a physical switchport that is connected to a virtualization host is using all available bandwidth. Which of the following would BEST address this issue?

A. Port mirroring

B. Link aggregation

C. Spanning tree

D. Microsegmentation

Correct Answer: D

QUESTION 15

A cloud administrator has built a new private cloud environment and needs to monitor all computer, storage, and network components of the environment.

Which of the following protocols would be MOST useful for this task?

A. SMTP

B. SCP

C. SNMP

D. SFTP

Correct Answer: C

Simple Network Management Protocol (SNMP) is a protocol that enables monitoring and managing network devices and components in an IP network. SNMP can help monitor all computer, storage, and network components of a private

cloud environment, as it can collect and report information about their status, performance, configuration, and events. SNMP can also help troubleshoot and optimize the private cloud environment, as it can detect and alert any issues or anomalies related to the network devices and components. References: CompTIA Cloud+ Certification Exam Objectives, page 15, section 2.8