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.certbus.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 cloud solution needs to be replaced without interruptions. The replacement process can be completed in phases, but the cost should be kept as low as possible.

Which of the following is the best strategy to implement?

A. Blue-green

B. Rolling

C. In-place

D. Canary

Correct Answer: B

A rolling strategy is the best to implement when needing to replace a cloud solution without interruptions and keeping costs low. This approach updates or replaces parts of the system gradually with minimal downtime and allows for a phased implementation. References: CompTIA Cloud+ Study Guide (V0-004) - Chapter on Cloud Deployment and Provisioning

QUESTION 2

A cloud architect is preparing environments to develop a new application that will process sensitive data. The project team consists of one internal developer, two external consultants, and three testers. Which of the following is the most important security control for the cloud architect to consider implementing?

A. Setting up private development, public development, and testing environments

B. Segregating environments for internal and external teams

C. Configuring DDoS protection to mitigate the risk of downtime

D. Using IAM and ACL in order to bolster DLP

Correct Answer: D

In a project handling sensitive data with a mix of internal and external team members, implementing Identity and Access Management (IAM) and Access Control Lists (ACL) is crucial for Data Loss Prevention (DLP). These controls ensure that only authorized individuals have access to specific resources, and actions are governed according to the principle of least privilege, minimizing the risk of data leakage or unauthorized access.

QUESTION 3

A company recently set up a CDN for its photography and image-sharing website. Which of the following is the most likely reason for the company\\'s action?

A. To eliminate storage costs

B. To improve site speed

C. To enhance security of static assets

D. To prevent unauthorized access

Correct Answer: B

The most likely reason for setting up a Content Delivery Network (CDN) is to improve site speed, especially for a photography and image-sharing website. CDNs cache content at edge locations closer to end-users, significantly reducing load times for static assets like images and videos. This enhancement in speed can improve user experience and site performance. References: CompTIA Cloud+ resources and CDN functionality

QUESTION 4

A cloud engineer is collecting web server application logs to troubleshoot intermittent issues. However, the logs are piling up and causing storage issues.

Which of the following log mechanisms should the cloud engineer implement to address this issue?

A. Splicing

B. Rotation

C. Sampling

D. Inspection

Correct Answer: B

Log rotation is the mechanism the cloud engineer should implement to address the issue of logs piling up and causing storage issues. Log rotation involves automatically archiving old log files and creating new ones after a certain size or time period, preventing storage issues. References: CompTIA Cloud+ Study Guide (V0-004) - Chapter on Cloud Monitoring and Management

QUESTION 5

A cloud engineer is developing an operating expense report that will be used to purchase various cloud billing models for virtual machine instances. The cloud billing model must meet the following requirements:

1.

The instance cannot be ephemeral.

2.

The minimum life cycle of the instance is expected to be five years.

3.

The software license is charged per physical CPU count.

Which of the following models would best meet these requirements?

A. Dedicated host

B. Spot instance

C. Pay-as-you-go

D. Reserved resources

Correct Answer: D

Reserved resources, or Reserved Instances, are ideal for workloads with predictable usage and a long-term commitment, such as a minimum lifecycle of five years. This model allows for significant cost savings compared to on-demand pricing, and the instance is not ephemeral, meaning it persists and is dedicated to the user for the duration of the reservation. The licensing charged per physical CPU count aligns with dedicated host or reserved instance models, but the long- term commitment points more towards reserved resources.

QUESTION 6

An organization is hosting a seminar with eight individuals who need to connect to their own dedicated VM. The technician used the following VM configurations:

IP address: DHCP NIC: 1Gbps Network: 10.1.10.0/29

Several users are unable to access their VMs. Which of the following best describes the reason?

A. Not enough addresses are available.

B. The routes are misconfigured.

C. Too much traffic is on the network.

D. DHCP is not working correctly on the VM.

Correct Answer: A

The network is configured with a subnet of /29, which provides only 6 usable IP addresses after accounting for the network and broadcast addresses. With eight individuals needing to connect to their own dedicated VMs, there are not enough IP addresses available to assign to each VM, leading to several users being unable to access their VMs. This issue is not related to misconfigured routes, network traffic, or DHCP functionality, but rather the limited number of IP addresses available in the given subnet.

QUESTION 7

A company recently migrated to a public cloud provider. The company\\'s computer incident response team needs to configure native cloud services tor detailed logging.

Which of the following should the team implement on each cloud service to support root cause analysis of past events? {Select two).

A. Log retention

B. Tracing

C. Log aggregation

D. Log rotation

E. Hashing

F. Encryption

Correct Answer: AC

For detailed logging to support root cause analysis of past events, the team should implement log retention to ensure logs are kept for the necessary amount of time and log aggregation to compile logs from various sources for easier analysis

and correlation.

References: Log management practices, including retention and aggregation, are part of the cloud management strategies covered in the CompTIA Cloud+ curriculum, particularly in the domain of technical operations.

QUESTION 8

A web application server farm has the following configuration:

1.

16vCPU

2.

128GB of memory

3.

512GB of local storage

The performance-testing team reports the web application farm is unable to process requests beyond 5,000 concurrent connections. Which of the following should be performed?

A. Review the memory capacity parameters in the web server

B. Restart and redeploy the application.

C. Restart the performance-testing tool.

D. Review the application configuration

Correct Answer: D

QUESTION 9

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 10

A systems engineer is migrating a batch of 25 VMs from an on-premises compute cluster to a public cloud using the public cloud\\'s migration agent. The migration job shows data copies at a rate of 250Mbps. After five servers migrate, the data copies at a rate of 25Mbps.

Which of the following should the engineer review first to troubleshoot?

A. The on-premises VM host hardware utilization

B. The on-premises ISP throttling rate

C. The IOPS on the SAN backing the on-premises cluster

D. The compute utilization of the VMs being migrated

Correct Answer: A

The engineer should review the on-premises VM host hardware utilization first. A decrease in transfer rate after a batch of migrations could suggest that the host hardware resources (like CPU, RAM, or network bandwidth) are becoming

saturated, which would slow down additional migrations.

References: CompTIA Cloud+ Certification Study Guide (V0- 004) by Scott Wilson and Eric Vanderburg.

QUESTION 11

Department supervisors have requested a report that will help them understand the utilization of cloud resources, make decisions about budgeting for the following year, and reduce costs.

Which of the following are the most important requisite steps to create the report? (Select two).

A. Set the desired retention of resource logs.

B. Configure application tracing.

C. Integrate email alerts with ticketing software.

D. Enable resource tagging.

E. Configure the collection of performance/utilization logs.

F. Configure metric threshold alerts.

Correct Answer: DE

To create a report that helps understand the utilization of cloud resources, make budget decisions, and reduce costs, the most important steps are to enable resource tagging and configure the collection of performance/utilization logs. Resource tagging helps in categorizing and tracking costs by associating tags with resources, while performance/utilization logs are essential for analyzing resource usage over time. References: CompTIA Cloud+ Study Guide (V0004) - Chapter on Cloud Management

QUESTION 12

A company is required to save historical data for seven years. A cloud administrator implements a script that automatically deletes data older than seven years.

Which of the following concepts best describes why the historical data is being deleted?

A. End of life

B. Data loss prevention

C. Cost implications

D. Tiered storage for archiving

Correct Answer: A

Deleting historical data older than seven years as described is an example of data end of life (EOL) policies in action. These policies dictate when data is no longer needed or relevant and should be securely disposed of, often for compliance,

legal, or cost- saving reasons.

References: CompTIA Cloud+ resources and data management strategies

QUESTION 13

A company that performs passive vulnerability scanning at its transit VPC has detected a vulnerability related to outdated web-server software on one of its public subnets.

Which of the following can the use to verify if this is a true positive with the LEAST effort and cost? (Select TWO).

A. A network-based scan

B. An agent-based scan

C. A port scan

D. A red-team exercise

E. A credentialed scan

F. A blue-team exercise

G. Unknown environment penetration testing

Correct Answer: BE

The correct answer is B and E. An agent-based scan and a credentialed scan can help verify if the vulnerability related to outdated web-server software is a true positive with the least effort and cost. An agent-based scan is a type of vulnerability scan that uses software agents installed on the target systems to collect and report data on vulnerabilities. This method can provide more accurate and detailed results than a network-based scan, which relies on network traffic analysis and probes1. An agent-based scan can also reduce the network bandwidth and performance impact of scanning, as well as avoid triggering false alarms from intrusion detection systems2. A credentialed scan is a type of vulnerability scan that uses valid login credentials to access the target systems and perform a more thorough and comprehensive assessment of their configuration, patch level, and vulnerabilities. A credentialed scan can identify vulnerabilities that are not visible or exploitable from the network level, such as missing updates, weak passwords, or misconfigured services3. A credentialed scan can also reduce the risk of false positives and false negatives, as well as avoid causing damage or disruption to the target systems3. A network-based scan, a port scan, a red-team exercise, a blue-team exercise, and unknown environment penetration testing are not the best options to verify if the vulnerability is a true positive with the least effort and cost. A network-based scan and a port scan may not be able to detect the vulnerability if it is not exposed or exploitable from the network level. A red-team exercise, a blue-team exercise, and unknown environment penetration testing are more complex, time-consuming, and costly methods that involve simulating real-world attacks or defending against them. These methods are more suitable for testing the overall security posture and resilience of an organization, rather than verifying a specific vulnerability4.

QUESTION 14

A security engineer Identifies a vulnerability m a containerized application. The vulnerability can be exploited by a privileged process to read tie content of the host\\'s memory. The security engineer reviews the following Dockerfile to determine a solution to mitigate similar exploits:

FROM alpine:3.17 RUN apk update andand apk upgrade COPY ./myapp ENTRYPOINT ["/myapp/app"]

Which of the following is the best solution to prevent similar exploits by privileged processes?

A. Adding the USER myappuserinstruction

B. Patching the host running the Docker daemon

C. Changing FROM alpiner3.17 to FROM alpine:latest

D. Running the container with the ready-only filesystem configuration

Correct Answer: A

Adding the "USER myappuser" instruction to the Dockerfile is the best solution to prevent similar exploits by privileged processes. This instruction ensures that the container runs as a non-privileged user instead of the root user, significantly reducing the risk of privileged exploits. Running containers with least privilege principles minimizes the potential impact of vulnerabilities, enhancing the overall security posture of the containerized environment.References: The CompTIA Cloud+ framework includes security concerns, measures, and concepts for cloud operations, highlighting the importance of container security practices, such as running containers as non-root users to prevent unauthorized access and exploitation.

QUESTION 15

A company needs to rehost its ERP system to complete a datacenter migration to the public cloud. The company has already migrated other systems and configured VPN connections.

Which of the following MOST likely needs to be analyzed before rehosting the ERP?

A. Software

B. Licensing

C. Right-sizing

D. The network

Correct Answer: B