Free Questions for CV0-003 by certsinside

Shared by Carey on 29-01-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: **MultipleChoice**

A cloud administrator has received a physical disk that was analyzed by the incident response team. Which of the following documents should the cloud administrator update?

Options:

A- Chain of custody

B- Incident taxonomy

C- Risk register

D- Incident playbook

Answer:

A

Explanation:

A) Chain of custody

A chain of custody is a document that records the sequence of custody, control, transfer, analysis, and disposition of physical or electronic evidence. A chain of custody is important to ensure the integrity and admissibility of evidence in legal cases. A cloud administrator who receives a physical disk that was analyzed by the incident response team should update the chain of custody to document when, how, and by whom the disk was handled, and what actions were performed on it12.

An incident taxonomy is a classification system that provides additional information about an incident, such as the nature, impact, intent, root cause, and data exposed. An incident taxonomy is useful for identifying trends and patterns, but it does not track the movement or manipulation of evidence3.

A risk register is a document that identifies, records, and assesses potential risks in a project or an organization. A risk register helps to prioritize and mitigate risks, and to develop contingency plans. A risk register is not directly related to the analysis of a physical disk by the incident response team4.

An incident playbook is a document that provides a series of prescriptive steps and guidance for responding and resolving incidents. An incident playbook helps to simplify and standardize the response process, and to reduce human error. An incident playbook does not record the details or outcomes of the response actions5.

Question 2

Question Type: MultipleChoice

The Chief Information Officer of a financial services company wants to ensure stringent security measures are maintained while migrating customer financial information from a private cloud to the public cloud. The cloud engineer must deploy automated validation and verification checks to prevent unauthorized disclosure of financial information. Which of the following should be configured during the migration?

Options:

A- ACL

B- VPN

C- P2V

D- VDI

Answer:

B

Explanation:

One possible answer is:

B) VPN

A VPN (Virtual Private Network) is a technology that creates a secure and encrypted connection between a remote device and a private network over the internet. A VPN can help prevent unauthorized disclosure of financial information during the migration from a private cloud to the public cloud, as it can protect the data in transit from interception, tampering, or leakage. A VPN can also help maintain compliance with data privacy regulations, such as GDPR or PCI DSS, by ensuring that the data is only accessible by authorized parties12.

ACL (Access Control List) is a method of controlling access to resources based on user or group permissions. ACL can help enforce security policies and restrict access to sensitive data, but it does not encrypt or protect the data in transit3.

P2V (Physical to Virtual) is a process of converting a physical machine into a virtual machine. P2V can help migrate workloads from on-premises servers to cloud servers, but it does not ensure the security of the data during the migration4.

VDI (Virtual Desktop Infrastructure) is a technology that provides users with virtual desktops hosted on a centralized server. VDI can help improve the performance, availability, and manageability of desktop environments, but it does not address the security of the data during the migration5.

Question 3

Question Type: **MultipleChoice**

A security analyst is investigating a recurring alert. The alert is reporting an insecure firewall configuration state after every cloud application deployment. The process of identifying the issue, requesting a fix, and waiting for the developers to manually patch the environment is being repeated multiple times. In an effort to identify the root issue, the following logs were collected:

Deploying template app prod. *yaml

Instance DB successfully created

DB keys successfully stored on vault

Instance WebApp successfully created

Access rules successfully applied

Access---keys successfully created

Which of the following options will provide a permanent fix for the issue?

Options:

A- Validate the Iac code used during the deployment.

B- Avoid the use of a vault to store database passwords.

C- Rotate the access keys that were created during deployment.

D- Recommend that the developers do not create multiple resources at once.

Answer:

A

Explanation:

The issue of an insecure firewall configuration state after every cloud application deployment is likely caused by a flaw in the IaC code used during the deployment.IaC stands for Infrastructure as Code, which is a method of managing and provisioning IT infrastructure using code, rather than manual configuration1. IaC allows teams to automate the setup and management of their infrastructure, making it more efficient and consistent.However, if the IaC code contains errors, vulnerabilities, or misconfigurations, it can result in security issues or compliance violations in the deployed infrastructure2. Therefore, to provide a permanent fix for the issue, the IaC code used during the deployment should be validated and tested to ensure that it meets the security requirements and best practices for firewall configuration. The IaC code can be validated using tools such asAzure Resource Manager Template Toolkit,AWS CloudFormation Linter, orTerraform Validate.These tools can check the syntax and semantics of the IaC code, and identify any potential errors or inconsistencies before deployment

Question 4

Question Type: **MultipleChoice**

A cloud engineer recently set up a container image repository. The engineer wants to ensure that downloaded images are not modified in transit. Which of the following is the best method to achieve this goal?

Options:

A- SHA-256

B- IPSec

C- AES-256

D- MD5
serpent-256

Answer:

A

Explanation:

SHA-256 is the best method to ensure that downloaded images are not modified in transit. SHA-256 is a type of cryptographic hash function that can generate a unique and fixed-length digest for any input dat

a. The digest can be used to verify the integrity and authenticity of the data, as any modification or tampering of the data would result in a different digest.SHA-256 is more secure and reliable than MD5, which is an older and weaker hash function that has been proven to be vulnerable to collisions and attacks12. AES-256 and serpent-256 are types of encryption algorithms, not hash functions, and they are used to protect the confidentiality of the data, not the integrity.IPSec is a network security protocol that can use encryption and hashing to secure data in transit, but it is not a method by itself

Question 5

Question Type: MultipleChoice

A web consultancy group currently works in an isolated development environment. The group uses this environment for the creation of the final solution, but also for showcasing it to customers, before commissioning the sites in production. Recently, customers of newly commissioned sites have reported they are not receiving the final product shown by the group, and the website is performing in unexpected ways. Which of the following additional environments should the group adopt and include in its process?

Options:

A- Provide each web consultant a local environment on their device.

B- Require each customer to have a blue-green environment.

C- Leverage a staging environment that is tightly controlled for showcasing.

D- Initiate a disaster recovery environment to fail to in the event of reported issues.

Answer:

C

Explanation:

A staging environment is a type of development environment that is used to test and demonstrate the final product before deploying it to the production environment. A staging environment can help the web consultancy group avoid the issues of delivering a different or faulty product to the customers, as it can ensure that the product is fully functional, compatible, and secure. A staging environment can also help the group showcase the product to the customers in a realistic and controlled way, as it can mimic the production environment and avoid any interference from other development activities.A staging environment can be leveraged by using cloud services that allow for easy provisioning, scaling, and deployment of web applications

Question 6

Question Type: **MultipleChoice**

An organization hosts an ERP database in on-premises infrastructure. A recommendation has been made to migrate the ERP solution to reduce operational overhead in the maintenance of the data center. Which of the following should be considered when migrating this on-premises database to DBaaS?

Options:

A- * Database application version compatibility

* Database IOPS values

* Database storage utilization

B- * Physical database server CPU cache value

* Physical database server DAS type

* Physical database server network I/O

C- * Database total user count

* Database total number of tables

* Database total number of storage procedures

D- * Physical database server operating system

* Physical database server memory configuration

* Physical database server CPU frequency

Answer:

A

Explanation:

When migrating an on-premises database to DBaaS, it is important to consider the database application version compatibility, the database IOPS values, and the database storage utilization. These factors can affect the performance, functionality, and cost of the migration. Database application version compatibility refers to the ability of the DBaaS provider to support the same or compatible version of the database software as the on-premises database. This can ensure that the database features, syntax, and behavior are consistent and compatible across the environments. Database IOPS values refer to the input/output operations per second that the database performs. This can indicate the workload and throughput of the database, and help determine the appropriate size and configuration of the DBaaS instance. Database storage utilization refers to the amount of disk space that the database consumes. This can affect the cost and scalability of the DBaaS service, and help optimize the storage allocation and backup strategies.Reference:= CompTIA Cloud+ source documents or study guide

CompTIA Cloud+ Certification Exam Objectives, Domain 2.0: Deployment, Objective 2.1: Given a scenario, execute and implement solutions using appropriate cloud migration tools and methods.

Migrate your relational databases to Azure - .NET | Microsoft Learn, Migrate On-premises Tablespaces to DBaaS Database Using Cross-Platform Tablespace Transport

Migrating On-Premises Databases to the DBaaS Database Using RMAN - Oracle, Overview

Question 7

Question Type: MultipleChoice

A cloud administrator needs to implement a new system within the current CSR The system requires a storage service to allocate a large number of digital files and images. The storage service must keep files for distributed access and serve images directly to the user's browser. Which of the following solutions would best meet these requirements?

Options:

A- NAS storage

B- Object storage

C- File storage

D- Block storage

Answer:

B

Explanation:

One possible solution for the cloud administrator is to use object storage. Object storage is a type of cloud storage service that stores data as objects, which consist of data, metadata, and a unique identifier. Object storage can allocate a large number of digital files and images, as it can scale to petabytes of capacity and handle billions of objects. Object storage can also keep files for distributed access, as it can store data across multiple regions and zones, and provide high availability and durability.Object storage can also serve images directly to the user's browser, as it can generate public URLs for each object that can be accessed over the internet12.

NAS storage, file storage, and block storage are not the best solutions for these requirements, as they have some limitations compared to object storage. NAS storage and file storage store data as files in a hierarchical structure, which can be inefficient for managing a large number of files and images. Block storage stores data as blocks in a fixed structure, which can be wasteful for storing variable-sized files and images.NAS storage, file storage, and block storage also require a file system or a protocol to access the data, which can add complexity and overhead to the system12.

Question 8

Question Type: MultipleChoice

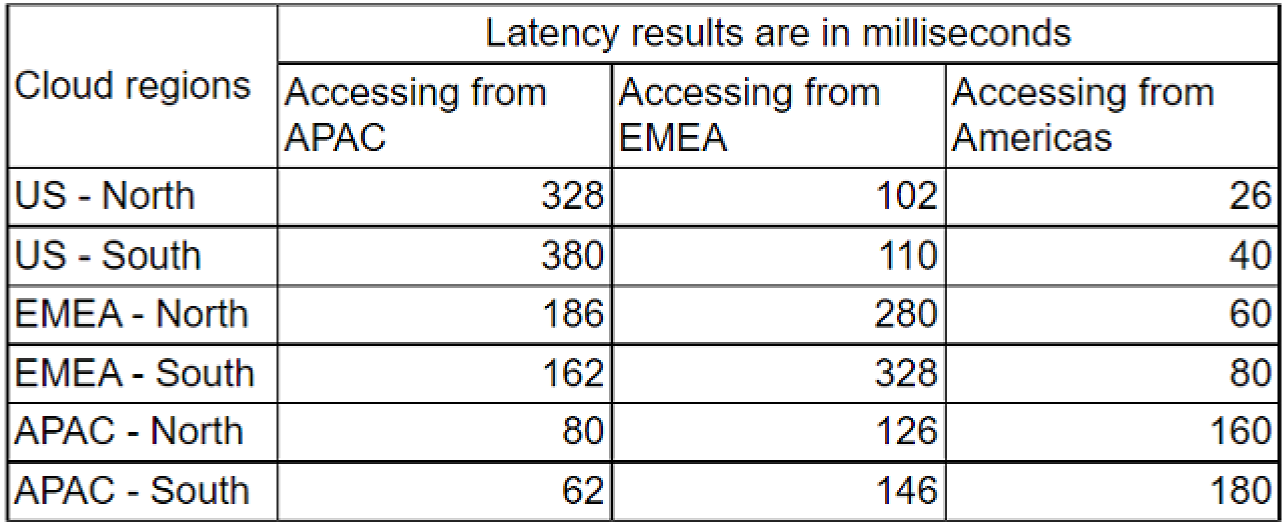
An application deployment team has observed delays in deployments and has asked the cloud administrator to evaluate the issue. Below is the result of a latency test that was conducted by the cloud administrator from offices located in the following regions:

* Asia-Pacific (APAC)

* Europe, the Middle East, and Africa (EMEA)

* Americas

Tests were conducted from each location, and the results are shown below:



Cloud regions	Latency results are in milliseconds		
	Accessing from APAC	Accessing from EMEA	Accessing from Americas
US - North	328	102	26
US - South	380	110	40
EMEA - North	186	280	60
EMEA - South	162	328	80
APAC - North	80	126	160
APAC - South	62	146	180

Which of the following locations needs to be investigated further?

Options:

A- * Connectivity from APAC to APAC regions

* Connectivity from APAC to EMEA and US - North

B- * Connectivity from APAC to all regions

* Connectivity from Americas to all regions

C- * Connectivity from EMEA to all regions

* Connectivity from APAC to APAC and EMEA regions

D- * Connectivity from APAC to EMEA and Americas regions

* Connectivity from EMEA to all regions

Answer:

D

Explanation:

The latency test results show that the connectivity from APAC to EMEA and Americas regions has the highest latency values, ranging from 162 ms to 380 ms. This indicates that there is a significant delay in the network communication between these regions, which could affect the performance and availability of the cloud services. The connectivity from EMEA to all regions also has high latency values, ranging from 60 ms to 328 ms, which could also cause issues for the application deployment team. Therefore, these locations need to be investigated further to identify and resolve the root cause of the network latency.

Some possible causes of network latency are :

Congestion: The network bandwidth may be insufficient to handle the volume of traffic, resulting in packet loss, retransmission, and queuing delays.

Distance: The physical distance between the source and destination nodes may increase the propagation delay, which is the time it takes for a signal to travel through a medium.

Routing: The network topology and configuration may affect the number and quality of hops that a packet takes to reach its destination, resulting in transmission and processing delays.

Hardware: The performance and capacity of the network devices, such as routers, switches, firewalls, and servers, may affect the speed and efficiency of data processing and delivery.

Some possible solutions to reduce network latency are :

Scaling: The network resources can be increased or optimized to handle the traffic demand, such as adding more bandwidth, load balancers, or caching servers.

Location: The network nodes can be placed closer to each other or to the end users, such as using edge computing, content delivery networks (CDNs), or regional cloud data centers.

Routing: The network routes can be improved or optimized to reduce the number and distance of hops, such as using direct peering, dedicated circuits, or software-defined networking (SDN).

Hardware: The network devices can be upgraded or replaced with faster and more reliable ones, such as using solid-state drives (SSDs), fiber-optic cables, or 5G technology.

: What is Network Latency? | Cloudflare

: How To Reduce Network Latency In 2021 - DNSstuff

Question 9

Question Type: **MultipleChoice**

A cloud solutions architect has an environment that must only be accessed during work hours. Which of the following processes should be automated to best reduce cost?

Options:

A- Scaling of the environment after work hours

B- Implementing access control after work hours

C- Shutting down the environment after work hours

D- Blocking external access to the environment after work hours

Answer:

C

Explanation:

Shutting down the environment after work hours is the best process to automate to reduce cost, as it will stop incurring charges for the cloud resources that are not needed outside of work hours. Scaling, implementing access control, or blocking external access may still incur some costs for the cloud resources that are running or reserved, even if they are not fully utilized.Shutting down the environment can be automated using scripts, schedules, or triggers that can turn off or deallocate the cloud resources based on time or usage criteria12.

Question 10

Question Type: MultipleChoice

Following the deployment of a new VM, a cloud engineer notices the backup platform has not added the machine to the appropriate job. The backup platform uses a text-based variable for job configuration. This variable is based on the RPO requirements for the workload. Which of the following did the cloud engineer forget to configure when deploying the virtual machine?

Options:

A- Tags

B- RPO

C- RTO

D- Server name
Template

Answer:

A

Explanation:

Tags are key-value pairs that can be applied to cloud resources to organize, categorize, and filter them. Tags can also be used to assign resources to backup jobs based on their RPO requirements. The cloud engineer forgot to configure the appropriate tag for the new VM that matches the text-based variable of the backup platform. Therefore, the backup platform did not add the VM to the correct job.Reference:Tags and labels | Cloud Storage | Google Cloud,CompTIA Cloud+ Certification Exam Objectives, Domain 4.0: Operations and Support, Objective 4.3: Given a scenario, apply the appropriate methods for cost control in a cloud environment.

20%
DISCOUNT