



CompTIA

Exam Questions CV0-003

CompTIA Cloud+ Certification Exam

NEW QUESTION 1

- (Topic 1)

A systems administrator needs to configure monitoring for a private cloud environment. The administrator has decided to use SNMP for this task. Which of the following ports should the administrator open on the monitoring server's firewall?

- A. 53
- B. 123
- C. 139
- D. 161

Answer: D

Explanation:

Port 161 is the default port used by Simple Network Management Protocol (SNMP) to communicate with network devices and collect information about their status, performance, configuration, and events. Opening port 161 on the monitoring server's firewall will allow SNMP traffic to pass through and enable monitoring for a private cloud environment. If port 161 is closed or blocked, SNMP traffic will be denied or dropped, resulting in a failure to monitor the network devices.

References: CompTIA Cloud+ Certification Exam Objectives, page 15, section 2.8

NEW QUESTION 2

- (Topic 1)

An organization has two businesses that are developing different software products. They are using a single cloud provider with multiple IaaS instances. The organization identifies that the tracking of costs for each business are inaccurate.

Which of the following is the BEST method for resolving this issue?

- A. Perform segregation of the VLAN and capture egress and ingress values of each network interface
- B. Tag each server with a dedicated cost and sum them based on the businesses
- C. Split the total monthly invoice equally between the businesses
- D. Create a dedicated subscription for the businesses to manage the costs

Answer: B

Explanation:

Tagging each server with a dedicated cost and summing them based on the businesses is the best method for resolving the issue of inaccurate cost tracking for different businesses that use multiple IaaS instances within a single cloud provider. Tagging can help identify and organize the servers based on various criteria, such as name, purpose, owner, or cost center. Tagging can also enable granular and accurate billing and reporting based on the tags. Summing the costs based on the businesses can help allocate and distribute the costs correctly and fairly among the different businesses. References: CompTIA Cloud+ Certification Exam Objectives, page 13, section 2.5

NEW QUESTION 3

- (Topic 1)

Which of the following strategies will mitigate the risk of a zero-day vulnerability MOST efficiently?

- A. Using only open-source technologies
- B. Keeping all resources up to date
- C. Creating a standby environment with a different cloud provider
- D. Having a detailed incident response plan

Answer: D

Explanation:

An incident response plan is a document or procedure that defines the roles, responsibilities, and actions to be taken in the event of a security incident or breach. Having a detailed incident response plan can help mitigate the risk of a zero-day vulnerability most efficiently, as it can provide a clear and consistent framework for identifying, containing, analyzing, and resolving any potential threats or exploits related to the unknown or unpatched vulnerability. Having a detailed incident response plan can also help minimize the impact and damage of a security incident or breach, as it can enable timely and effective recovery and restoration processes. References: CompTIA Cloud+ Certification Exam Objectives, page 14, section 2.7

NEW QUESTION 4

- (Topic 1)

A DevOps administrator is automating an existing software development workflow. The administrator wants to ensure that prior to any new code going into production, tests confirm the new code does not negatively impact existing automation activities.

Which of the following testing techniques would be BEST to use?

- A. Usability testing
- B. Regression testing
- C. Vulnerability testing
- D. Penetration testing

Answer: B

Explanation:

Regression testing is a type of testing that ensures that new code or changes to existing code do not break or degrade the functionality of the software. Regression testing is often used in software development workflows to verify that new features or bug fixes do not introduce new errors or affect the performance of the software. Regression testing can help prevent negative impacts on existing automation activities by checking that the new code is compatible with the existing code and does not cause any unexpected failures or errors. References: CompTIA Cloud+ Certification Exam Objectives, page 19, section 4.1
Reference: <https://www.softwaretestinghelp.com/regression-testing-tools-and-methods/>

NEW QUESTION 5

- (Topic 1)

Due to a policy change, a few of a customer's application VMs have been migrated to synchronously replicated storage. The customer now reports that performance is lower. The systems administrator checks the resource usage and discovers CPU utilization is at 60% and available memory is at 30%. Which of the following is the MOST likely cause?

- A. There is not enough vCPU assigned
- B. The application is not compatible with the new settings
- C. The new configuration is adding latency
- D. The memory of the VM is underallocated

Answer: C

Explanation:

Latency is the delay or time taken for data to travel from one point to another in a network or system. Latency can affect the performance of applications and processes that depend on fast and reliable data transfer. Synchronous replication is a method of data replication that ensures that data is written to two or more storage devices at the same time, providing high availability and consistency. However, synchronous replication can also introduce latency, as the write operation has to wait for the confirmation from all the replicated devices before completing. The new configuration of migrating some application VMs to synchronously replicated storage is most likely adding latency, which can lower the performance of the applications. References: [CompTIA Cloud+ Certification Exam Objectives], page 10, section 1.5

NEW QUESTION 6

- (Topic 1)

An administrator is performing an in-place upgrade on a guest VM operating system. Which of the following can be performed as a quick method to roll back to an earlier state, if necessary?

- A. A configuration file backup
- B. A full backup of the database
- C. A differential backup
- D. A VM-level snapshot

Answer: D

Explanation:

A VM-level snapshot is a point-in-time copy of the state and data of a virtual machine (VM). A VM-level snapshot can be used as a quick method to roll back to an earlier state, if necessary, as it can restore the VM to the exact condition it was in when the snapshot was taken. A VM-level snapshot can be useful for performing an in-place upgrade on a guest VM operating system, as it can allow the administrator to revert to the previous operating system version in case of any issues or errors. References: CompTIA Cloud+ Certification Exam Objectives, page 10, section 1.5
Reference: <https://cloud.google.com/compute/docs/tutorials/performing-in-place-upgrade-windows-server>

NEW QUESTION 7

- (Topic 1)

The security team for a large corporation is investigating a data breach. The team members are all trying to do the same tasks but are interfering with each other's work. Which of the following did the team MOST likely forget to implement?

- A. Incident type categories
- B. A calling tree
- C. Change management
- D. Roles and responsibilities

Answer: D

Explanation:

Roles and responsibilities are definitions or descriptions of what each team member or stakeholder is expected to do or perform in a project or process. Roles and responsibilities can help clarify the scope, authority, and accountability of each team member or stakeholder and avoid any confusion or duplication of work. The security team most likely forgot to implement roles and responsibilities when investigating a data breach, as they are all trying to do the same tasks but are interfering with each other's work. Implementing roles and responsibilities can help improve efficiency and effectiveness, as it can ensure that each team member or stakeholder knows what tasks they need to do and how they need to coordinate with others. References: CompTIA Cloud+ Certification Exam Objectives, page 13, section 2.5

NEW QUESTION 8

- (Topic 1)

A systems administrator is deploying a GPU-accelerated VDI solution. Upon requests from several users, the administrator installs an older version of the OS on their virtual workstations. The majority of the VMs run the latest LTS version of the OS.

Which of the following types of drivers will MOST likely ensure compatibility will all virtual workstations?

- A. Alternative community drivers
- B. Legacy drivers
- C. The latest drivers from the vendor's website
- D. The drivers from the OS repository

Answer: D

Explanation:

The drivers from the OS repository are the drivers that are included or available in the official software repository or package manager of the operating system. The drivers from the OS repository are most likely to ensure compatibility with all virtual workstations that use a GPU-accelerated VDI solution, as they are tested and verified to work with different versions of the operating system and the hardware. The drivers from the OS repository can also provide stability and security, as they are regularly updated and patched by the operating system vendor or community. References: CompTIA Cloud+ Certification Exam Objectives, page 11, section 1.6

NEW QUESTION 9

- (Topic 1)

An organization is hosting a DNS domain with private and public IP ranges. Which of the following should be implemented to achieve ease of management?

- A. Network peering
- B. A CDN solution
- C. A SDN solution
- D. An IPAM solution

Answer: D

Explanation:

An IP address management (IPAM) solution is a type of tool or system that automates and standardizes the allocation, tracking, and management of IP addresses in an IP network. An IPAM solution can help achieve ease of management for hosting a DNS domain with private and public IP ranges, as it can simplify and centralize the process of assigning and updating IP addresses for different DNS records or zones without manual intervention or errors. An IPAM solution can also help optimize DNS performance and security, as it can monitor and report any issues or conflicts related to IP addresses or DNS records. References: CompTIA Cloud+ Certification Exam Objectives, page 15, section 2.8
Reference: <https://www.infoblox.com/glossary/ipam-ip-address-management/>

NEW QUESTION 10

- (Topic 1)

A company has decided to get multiple compliance and security certifications for its public cloud environment. However, the company has few staff members to handle the extra workload, and it has limited knowledge of the current infrastructure.

Which of the following will help the company meet the compliance requirements as quickly as possible?

- A. DLP
- B. CASB
- C. FIM
- D. NAC

Answer: B

Explanation:

A cloud access security broker (CASB) is a type of security solution that acts as a gateway between cloud service users and cloud service providers. A CASB can help a company get multiple compliance and security certifications for its public cloud environment, as it can provide visibility, control, and protection for cloud data and applications. A CASB can also help the company handle the extra workload and overcome the limited knowledge of the current infrastructure, as it can automate and simplify the enforcement of security policies and compliance requirements across multiple cloud services. References: CompTIA Cloud+ Certification Exam Objectives, page 14, section 2.7

NEW QUESTION 10

- (Topic 1)

An organization is implementing a new requirement to facilitate users with faster downloads of corporate application content. At the same time, the organization is also expanding cloud regions.

Which of the following would be suitable to optimize the network for this requirement?

- A. Implement CDN for overall cloud application
- B. Implement auto-scaling of the compute resources
- C. Implement SR-IOV on the server instances
- D. Implement an application container solution

Answer: C

Explanation:

Reference: https://access.redhat.com/documentation/en-us/red_hat_openstack_platform/13/html/network_functions_virtualization_planning_and_configuration_guide/part-sriov-nfv-configuration

NEW QUESTION 11

- (Topic 1)

A cloud administrator is switching hosting companies and using the same script that was previously used to deploy VMs in the new cloud. The script is returning errors that the command was not found.

Which of the following is the MOST likely cause of the script failure?

- A. Account mismatches
- B. IP address changes
- C. API version incompatibility
- D. Server name changes

Answer: C

Explanation:

An application programming interface (API) is a set of rules or protocols that defines how different systems or applications can communicate or interact with each other. An API version is a specific iteration or release of an API that may have different features or functionalities than previous or subsequent versions. API version incompatibility is the most likely cause of the script failure when switching hosting companies and using the same script that was previously used to deploy VMs in the new cloud, as it can result in errors or failures when trying to execute commands or functions that are not supported or recognized by the new cloud provider's API version. The issue can be resolved by updating or modifying the script to match the new cloud provider's API version. References: CompTIA Cloud+ Certification Exam Objectives, page 13, section 2.5

NEW QUESTION 14

- (Topic 1)

A cloud administrator recently deployed an update to the network drivers of several servers. Following the update, one of the servers no longer responds to remote login requests. The cloud administrator investigates the issue and gathers the following information:

- ? The cloud management console shows the VM is running and the CPU and memory utilization is at or near 0%.
- ? The cloud management console does not show an IP address for that server.
- ? A DNS lookup shows the hostname resolves to an IP address.
- ? The server is a member of the same security group as the others.
- ? The cloud administrator is able to log in remotely to the other servers without issue.

Which of the following is the MOST likely cause of the server being unavailable?

- A. The network driver updates did not apply successfully, and the interface is in a down state.
- B. The ACL policy for the server was updated as part of the server reboot, preventing login access.
- C. The server was assigned a new IP address, and DNS entry for the server name was not updated.
- D. The update caused an increase in the output to the logs, and the server is too busy to respond.

Answer: A

NEW QUESTION 16

- (Topic 1)

A company has developed a cloud-ready application. Before deployment, an administrator needs to select a deployment technology that provides a high level of portability and is lightweight in terms of footprint and resource requirements.

Which of the following solutions will be BEST to help the administrator achieve the requirements?

- A. Containers
- B. Infrastructure as code
- C. Desktop virtualization
- D. Virtual machines

Answer: A

Explanation:

Containers are a type of deployment technology that packages an application and its dependencies into a lightweight and portable unit that can run on any platform or environment. Containers can provide a high level of portability and are lightweight in terms of footprint and resource requirements, as they do not need a full operating system or hypervisor to run. Containers can also enable faster and easier deployment, scaling, and management of cloud-based applications. Containers are the best solution to help the administrator achieve the requirements for deploying a cloud-ready application. References: CompTIA Cloud+ Certification Exam Objectives, page 11, section 1.6

Reference: <https://blog.netapp.com/blogs/containers-vs-vms/>

NEW QUESTION 18

- (Topic 1)

A company is switching from one cloud provider to another and needs to complete the migration as quickly as possible.

Which of the following is the MOST important consideration to ensure a seamless migration?

- A. The cost of the environment
- B. The I/O of the storage
- C. Feature compatibility
- D. Network utilization

Answer: C

Explanation:

Feature compatibility is the degree to which the features or functionalities of a system or application are compatible or interoperable with another system or application. Feature compatibility is the most important consideration to ensure a seamless migration from one cloud provider to another, as it can affect the performance, reliability, and security of the system or application in the new cloud environment. Feature compatibility can also help complete the migration as quickly as possible, as it can reduce or eliminate the need for reconfiguration, customization, or testing of the system or application after the migration. References: CompTIA Cloud+ Certification Exam Objectives, page 18, section 3.5

NEW QUESTION 21

- (Topic 1)

A systems administrator notices that a piece of networking equipment is about to reach its end of support.

Which of the following actions should the administrator recommend?

- A. Update the firmware
- B. Migrate the equipment to the cloud
- C. Update the OS
- D. Replace the equipment

Answer: D

Explanation:

Replacing the equipment is the best action to take when a piece of networking equipment is about to reach its end of support. End of support means that the vendor or manufacturer will no longer provide technical assistance, updates, patches, or fixes for the equipment, which can affect its functionality, performance, security, and compatibility. Replacing the equipment with a newer model that has ongoing support can prevent any issues or risks associated with using outdated equipment.

References: CompTIA Cloud+ Certification Exam Objectives, page 18, section 3.5

NEW QUESTION 22

- (Topic 1)

A company has deployed a new cloud solution and is required to meet security compliance.

Which of the following will MOST likely be executed in the cloud solution to meet security requirements?

- A. Performance testing
- B. Regression testing
- C. Vulnerability testing
- D. Usability testing

Answer: C

Explanation:

Vulnerability testing is a type of security testing that identifies and evaluates the weaknesses or flaws in a system or service that could be exploited by attackers. Vulnerability testing can help meet security compliance requirements when deploying a new cloud solution, as it can reveal any potential security risks or gaps in the cloud environment and provide recommendations for remediation or mitigation. Vulnerability testing can also help improve security posture and performance, as it can prevent or reduce the impact of cyberattacks, data breaches, or service disruptions.

References: CompTIA Cloud+ Certification Exam Objectives, page 14, section 2.7

NEW QUESTION 23

- (Topic 1)

An organization will be deploying a web application in a public cloud with two web servers, two database servers, and a load balancer that is accessible over a single public IP.

Taking into account the gateway for this subnet and the potential to add two more web servers, which of the following will meet the minimum IP requirement?

- A. 192.168.1.0/26
- B. 192.168.1.0/27
- C. 192.168.1.0/28
- D. 192.168.1.0/29

Answer: C

Explanation:

A /28 subnet is a subnet that has a network prefix of 28 bits and a host prefix of 4 bits. A /28 subnet can support up to 16 hosts (14 usable hosts) and has a subnet mask of 255.255.255.240. Using a /28 subnet can meet the minimum IP requirement for deploying a web application in a public cloud with two web servers, two database servers, and a load balancer that is accessible over a single public IP, taking into account the gateway for this subnet and the potential to add two more web servers. Using a /28 subnet can provide enough host addresses for the current and future web servers, database servers, load balancer, and gateway, as well as allow for some growth or redundancy.

References: CompTIA Cloud+ Certification Exam Objectives, page 15, section 2.8

NEW QUESTION 27

- (Topic 1)

A cloud administrator is designing a multiregion network within an IaaS provider. The business requirements for configuring the network are as follows:

? Use private networking in and between the multisites for data replication.

? Use low latency to avoid performance issues.

Which of the following solutions should the network administrator use within the IaaS provider to connect multiregions?

- A. Peering
- B. Gateways
- C. VPN
- D. Hub and spoke

Answer: A

Explanation:

Peering is a type of network connection that allows two or more networks to exchange traffic directly without using an intermediary or a third-party service. Peering can help connect multiregions within an IaaS provider, as it can enable private networking in and between the multisites for data replication. Peering can also provide low latency, as it can reduce the number of hops and distance between the networks. Peering is the best solution for designing a multiregion network within an IaaS provider to support business requirements. References: CompTIA Cloud+ Certification Exam Objectives, page 15, section 2.8

NEW QUESTION 30

- (Topic 1)

A company that utilizes an IaaS service provider has contracted with a vendor to perform a penetration test on its environment. The vendor is able to exploit the virtualization layer and obtain access to other instances within the cloud provider's environment that do not belong to the company.

Which of the following BEST describes this attack?

- A. VM escape
- B. Directory traversal
- C. Buffer overflow
- D. Heap spraying

Answer: A

Explanation:

VM escape is a type of attack that allows an attacker to break out of a virtual machine (VM) and access the host system or other VMs within the same cloud provider's environment. VM escape can exploit the vulnerabilities in the virtualization layer or hypervisor that separates and isolates the VMs from each other and from the host system. VM escape can result in serious consequences, such as compromising the security and privacy of other customers' data or resources, gaining unauthorized access to the cloud provider's infrastructure or services, or launching further attacks on other systems or networks. VM escape best describes the attack that was performed by a vendor who was able to exploit the virtualization layer and obtain access to other instances within the cloud provider's environment that do not belong to the company. References: CompTIA Cloud+ Certification Exam Objectives, page 19, section 4.1

Reference: <https://whatis.techtarget.com/definition/virtual-machine-escape>

NEW QUESTION 34

- (Topic 1)

A systems administrator needs to configure a set of policies to protect the data to comply with mandatory regulations.

Which of the following should the administrator implement to ensure DLP efficiently prevents the exposure of sensitive data in a cloud environment?

- A. Integrity
- B. Versioning
- C. Classification
- D. Segmentation

Answer: C

Explanation:

Classification is a process of assigning labels or categories to data based on its sensitivity, value, or risk level. Classification can help implement data loss prevention (DLP) policies by identifying which data needs to be protected and how to protect it according to its classification level. Classification can also help comply with mandatory regulations by ensuring that data is handled and stored appropriately based on its legal or contractual requirements. Classification is essential for DLP to efficiently prevent the exposure of sensitive data in a cloud environment. References: CompTIA Cloud+ Certification Exam Objectives, page 14, section 2.7

NEW QUESTION 36

- (Topic 1)

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

Answer: B

Explanation:

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>

NEW QUESTION 39

- (Topic 1)

A systems administrator is troubleshooting performance issues with a Windows VDI environment. Users have reported that VDI performance is very slow at the start of the workday, but the performance is fine during the rest of the day. Which of the following is the MOST likely cause of the issue? (Choose two.)

- A. Disk I/O limits
- B. Affinity rule
- C. CPU oversubscription
- D. RAM usage
- E. Insufficient GPU resources
- F. License issues

Answer: AC

Explanation:

Disk I/O limits are restrictions or controls that limit the amount of disk input/output operations per second (IOPS) that a VM can perform on a storage device or system. CPU oversubscription is a situation where more CPU resources are allocated to VMs than are physically available on the host or server. Disk I/O limits and CPU oversubscription are most likely to cause VDI performance being very slow at the start of the workday, but fine during the rest of the day, as they can create bottlenecks or contention for disk and CPU resources when multiple users log in or launch their VDI sessions at the same time, resulting in increased latency or reduced throughput for VDI operations. References: CompTIA Cloud+ Certification Exam Objectives, page 9, section 1.4

NEW QUESTION 42

- (Topic 1)

A cloud administrator is reviewing a new application implementation document. The administrator needs to make sure all the known bugs and fixes are applied, and unwanted ports and services are disabled.

Which of the following techniques would BEST help the administrator assess these business requirements?

- A. Performance testing
- B. Usability testing
- C. Vulnerability testing
- D. Regression testing

Answer: D

Explanation:

Regression testing is a type of software testing that verifies that existing features or functionalities of a system or application are not affected by any changes or updates made to it. Regression testing can help assess whether all the known bugs and fixes are applied and unwanted ports and services are disabled when reviewing a new application implementation document for a cloud deployment, as it can detect any errors or defects that may have been introduced or re-introduced after applying patches, updates, or configurations to the application. References: CompTIA Cloud+ Certification Exam Objectives, page 19, section 4.1

NEW QUESTION 46

- (Topic 1)

A company has a cloud infrastructure service, and the cloud architect needs to set up a DR site. Which of the following should be configured in between the cloud environment and the DR site?

- A. Failback
- B. Playbook
- C. Zoning
- D. Replication

Answer: D

Explanation:

Replication is a process of copying or synchronizing data from one location to another to ensure consistency and availability. Replication can help set up a disaster recovery (DR) site for a cloud environment, as it can enable data backup and recovery in case of a failure or outage in the primary site. Replication can also improve performance and reliability, as it can reduce latency and load by distributing data across multiple sites. Replication should be configured between the cloud environment and the DR site to ensure data protection and continuity. References: CompTIA Cloud+ Certification Exam Objectives, page 10, section 1.5

NEW QUESTION 50

- (Topic 1)

Which of the following is relevant to capacity planning in a SaaS environment?

- A. Licensing
- B. A hypervisor
- C. Clustering
- D. Scalability

Answer: D

Explanation:

Scalability is the ability of a system or service to handle increased workload or demand by adding or removing resources or capacity as needed. Scalability is relevant to capacity planning in a SaaS environment, as it can affect the performance, availability, and cost of the SaaS service. Scalability can help optimize the capacity planning process by ensuring that the SaaS service has enough resources or capacity to meet the current and future needs of the customers without wasting or underutilizing resources or capacity. References: CompTIA Cloud+ Certification Exam Objectives, page 12, section 2.2

NEW QUESTION 53

- (Topic 1)

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

Answer: C

Explanation:

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

NEW QUESTION 58

- (Topic 1)

A media company has made the decision to migrate a physical, internal file server to the cloud and use a web-based interface to access and manage the files. The users must be able to use their current corporate logins. Which of the following is the MOST efficient way to achieve this goal?

- A. Deploy a VM in a cloud, attach storage, and copy the files across
- B. Use a SaaS service with a directory service federation
- C. Deploy a fileshare in a public cloud and copy the files across
- D. Copy the files to the object storage location in a public cloud

Answer: B

Explanation:

Software as a service (SaaS) is a type of cloud service model that provides software applications over the Internet that are hosted and managed by a cloud service provider. Directory service federation is a type of authentication mechanism that allows users to access multiple systems or applications across different domains or organizations with a single login credential. Using a SaaS service with a directory service federation can help migrate an internal file server to the cloud and use a web-based interface to access and manage the files, as it can eliminate the need for maintaining an on-premises file server and enable seamless and secure access to cloud-based files using the same corporate logins. References: CompTIA Cloud+ Certification Exam Objectives, page 8, section 1.2

NEW QUESTION 59

- (Topic 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

Answer: A

Explanation:

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/>

NEW QUESTION 61

- (Topic 1)

A company recently subscribed to a SaaS collaboration service for its business users. The company also has an on-premises collaboration solution and would like users to have a seamless experience regardless of the collaboration solution being used. Which of the following should the administrator implement?

- A. LDAP
- B. WAF
- C. VDI
- D. SSO

Answer: D

Explanation:

Single sign-on (SSO) is a type of authentication mechanism that allows users to access multiple systems or applications with a single login credential. SSO can help users have a seamless experience regardless of the collaboration solution being used, as it can eliminate the need for multiple logins and passwords for different systems or applications. SSO can also improve user convenience, productivity, and security, as it can simplify the login process, reduce login errors, and enhance password management. References: CompTIA Cloud+ Certification Exam Objectives, page 14, section 2.7

NEW QUESTION 65

- (Topic 1)

A systems administrator recently upgraded the processors in a web application host. Upon the next login, the administrator sees a new alert regarding the license being out of compliance. Which of the following licensing models is the application MOST likely using?

- A. Per device
- B. Per user
- C. Core-based
- D. Volume-based

Answer: C

Explanation:

Core-based licensing is a type of licensing model that charges based on the number of processor cores in a system or server. Core-based licensing is often used by software vendors to align their pricing with the performance and capacity of modern hardware. Core-based licensing can also enable customers to optimize their licensing costs by choosing the appropriate hardware configuration for their needs. Upgrading the processors in a web application host can affect the core-based licensing of the application, as it may increase the number of cores that need to be licensed. This can result in an alert regarding the license being out of compliance if the license is not updated accordingly. References: CompTIA Cloud+ Certification Exam Objectives, page 20, section 4.2
Reference: https://download.microsoft.com/download/3/d/4/3d42bdc2-6725-4b29-b75a-a5b04179958b/percorelicensing_definitions_vlbrief.pdf

NEW QUESTION 69

- (Topic 1)

A cloud architect wants to minimize the risk of having systems administrators in an IaaS compute instance perform application code changes. The development group should be the only group allowed to modify files in the directory. Which of the following will accomplish the desired objective?

- A. Remove the file write permissions for the application service account.
- B. Restrict the file write permissions to the development group only.
- C. Add access to the fileshare for the systems administrator's group.
- D. Deny access to all development user accounts

Answer: B

Explanation:

File write permissions are permissions that control who can modify or delete files in a directory or system. Restricting the file write permissions to the development group only can help minimize the risk of having systems administrators in an IaaS compute instance perform application code changes, as it can prevent anyone other than the development group from altering or removing any files in the directory where the application code is stored. Restricting the file write permissions can also help maintain consistency and integrity, as it can ensure that only authorized and qualified users can make changes to the application code. References: CompTIA Cloud+ Certification Exam Objectives, page 14, section 2.7

NEW QUESTION 74

- (Topic 2)

A cloud administrator is managing an organization's infrastructure in a public cloud. All servers are currently located in a single virtual network with a single firewall that all traffic must pass through. Per security requirements, production, QA, and development servers should not be able to communicate directly with each other. Which of the following should an administrator perform to comply with the security requirement?

- A. Create separate virtual networks for production, QA, and development server
- B. Move the servers to the appropriate virtual network. Apply a network security group to each virtual network that denies all traffic except for the firewall.
- C. Create separate network security groups for production, QA, and development server
- D. Apply the network security groups on the appropriate production, QA, and development servers. Peer the networks together.
- E. Create separate virtual networks for production, QA, and development server
- F. Move the servers to the appropriate virtual network. Peer the networks together.
- G. Create separate network security groups for production, QA, and development server
- H. Peer the networks together. Create static routes for each network to the firewall.

Answer: A

Explanation:

These are the actions that the administrator should perform to comply with the security requirement of isolating production, QA, and development servers from each other in a public cloud environment:

? Create separate virtual networks for production, QA, and development servers: A virtual network is a logical isolation of network resources or systems within a cloud environment. Creating separate virtual networks for different types of servers can help to segregate them from each other and prevent direct communication or interference.

? Move the servers to the appropriate virtual network: Moving the servers to the appropriate virtual network can help to assign them to their respective roles and functions, as well as ensure that they follow the network policies and rules of their virtual network.

? Apply a network security group to each virtual network that denies all traffic except for the firewall: A network security group is a set of rules or policies that control and filter inbound and outbound network traffic for a virtual network or system. Applying a network security group to each virtual network that denies all traffic except for the firewall can help to enforce security and compliance by blocking any unauthorized or unwanted traffic between different types of servers, while allowing only necessary traffic through the firewall.

NEW QUESTION 79

- (Topic 2)

A systems administrator is troubleshooting a performance issue with a virtual database server. The administrator has identified the issue as being disk related and believes the cause is a lack of IOPS on the existing spinning disk storage. Which of the following should the administrator do NEXT to resolve this issue?

- A. Upgrade the virtual database server.
- B. Move the virtual machine to flash storage and test again.
- C. Check if other machines on the same storage are having issues.
- D. Document the findings and place them in a shared knowledge base.

Answer: B

Explanation:

Moving the virtual machine to flash storage and testing again is what the administrator should do next to resolve the issue of disk-related performance issue with a virtual database server that has been identified as being caused by a lack of IOPS on the existing spinning disk storage. IOPS (Input/Output Operations Per Second) is a measure of how fast a storage device can read and write data. IOPS can affect performance of a virtual database server by determining how quickly it can access and process data from storage. Spinning disk storage is a type of storage device that uses rotating magnetic disks to store data. Spinning disk storage has lower IOPS than flash storage, which is a type of storage device that uses solid-state memory chips to store data. Flash storage has higher IOPS than spinning disk storage, which means that it can read and write data faster and more efficiently than spinning disk storage. Moving the virtual machine to flash storage and testing again can help to resolve the issue by increasing the IOPS and improving the performance of the virtual database server.

NEW QUESTION 80

- (Topic 2)

A systems administrator is deploying a new cloud application and needs to provision cloud services with minimal effort. The administrator wants to reduce the tasks required for maintenance, such as OS patching, VM and volume provisioning, and autoscaling configurations. Which of the following would be the BEST option to deploy the new application?

- A. A VM cluster
- B. Containers
- C. OS templates
- D. Serverless

Answer: D

Explanation:

Serverless is what would be the best option to deploy a new cloud application and provision cloud services with minimal effort while reducing the tasks required for maintenance such as OS patching, VM and volume provisioning, and autoscaling configurations. Serverless is a cloud service model that provides customers with a platform to run applications or functions without having to manage or provision any underlying infrastructure or resources, such as servers, storage, network, OS, etc. Serverless can provide benefits such as:

? Minimal effort: Serverless can reduce the effort required to deploy a new cloud application and provision cloud services by automating and abstracting away all the infrastructure or resource management or provisioning tasks from customers, and allowing them to focus only on writing code or logic for their applications or functions.

? Reduced maintenance: Serverless can reduce the tasks required for maintenance by handling all the infrastructure or resource maintenance tasks for customers, such as OS patching, VM and volume provisioning, autoscaling configurations, etc., and ensuring that they are always up-to-date and optimized.

NEW QUESTION 85

- (Topic 2)

A cloud administrator wants to have a central repository for all the logs in the company's private cloud. Which of the following should be implemented to BEST meet this requirement?

- A. SNMP
- B. Log scrubbing
- C. CMDB
- D. A syslog server

Answer: D

Explanation:

Reference: <https://www.itpro.com/infrastructure/network-internet/355174/how-to-build-a-dedicated-syslog-server>

A syslog server is what the administrator should implement to have a central repository for all the logs in the company's private cloud. Syslog is a standard protocol that allows network devices and systems to send log messages to a centralized server or collector. Syslog can help to consolidate and manage logs from different sources in one place, which can facilitate monitoring, analysis, troubleshooting, auditing, etc.

NEW QUESTION 90

- (Topic 2)

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.

Answer: C

Explanation:

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.

NEW QUESTION 93

- (Topic 2)

A cloud solutions architect needs to determine the best strategy to deploy an application environment in production, given the following requirements:

No downtime

Instant switch to a new version using traffic control for all users

Which of the following deployment strategies would be the BEST solution?

- A. Hot site
- B. Blue-green
- C. Canary
- D. Rolling

Answer: B

Explanation:

Reference: <https://thenewstack.io/deployment-strategies/>

Blue-green is the best deployment strategy to deploy an application environment in production, given the requirements of no downtime and instant switch to a new version using traffic control for all users. Blue-green is a deployment strategy that involves having two identical environments, one running the current version of the application (blue) and one running the new version of the application (green). The traffic is directed to the blue environment by default, while the green environment is tested and verified. When the new version is ready to go live, the traffic is switched to the green environment using a router or load balancer, without any downtime or interruption. The blue environment can be kept as a backup or updated with the new version for future deployments.

NEW QUESTION 94

- (Topic 2)

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

Answer: A

Explanation:

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.

NEW QUESTION 97

- (Topic 2)

A cloud administrator is reviewing the annual contracts for all hosted solutions. Upon review of the contract for the hosted mail solution, the administrator notes the monthly subscription rate has increased every year. The provider has been in place for ten years, and there is a large amount of data being hosted. Which of the following is a barrier to switching providers?

- A. Service-level agreement
- B. Vendor lock-in
- C. Memorandum of understanding
- D. Encrypted data

Answer: B

Explanation:

Vendor lock-in is a barrier to switching providers for a hosted mail solution that has increased its monthly subscription rate every year. Vendor lock-in is a situation where a customer becomes dependent on a vendor or provider for a product or service and faces difficulties or costs in switching to another vendor or provider. Vendor lock-in can occur due to various factors, such as proprietary technology, contractual obligations, data migration challenges, compatibility issues, etc. In this case, the customer may face vendor lock-in due to the large amount of data being hosted by the mail provider and the potential challenges or costs of transferring or migrating the data to another provider.

NEW QUESTION 98

- (Topic 2)

A cloud administrator has been using a custom VM deployment script. After three months of use, the script no longer joins the LDAP domain. The cloud administrator verifies the account has the correct permissions. Which of the following is the MOST likely cause of the failure?

- A. Incorrect encryption ciphers
- B. Broken trust relationship
- C. Invalid certificates
- D. Expired password

Answer: D

Explanation:

An expired password is the most likely cause of the failure of a custom VM deployment script that no longer joins the LDAP domain. LDAP (Lightweight Directory Access Protocol) is a protocol that allows access and management of directory services, such as user accounts, groups, permissions, etc., over a network. LDAP can be used to authenticate and authorize users or devices to access network resources or systems. An expired password is a password that has reached its validity period and needs to be changed or renewed. An expired password can prevent users or devices from joining or accessing an LDAP domain, as it may indicate that the account is inactive, compromised, or outdated.

NEW QUESTION 100

- (Topic 2)

An update is being deployed to a web application, and a systems administrator notices the cloud SQL database has stopped running. The VM is responding to pings, and there were not any configuration changes scheduled for the VM. Which of the following should the administrator check NEXT?

- A. Logs on the VM
- B. Firewall on the VM
- C. Memory on the VM
- D. vGPU performance on the VM

Answer: A

Explanation:

Checking the logs on the VM is the next step that the administrator should take if the cloud SQL database has stopped running after an update deployment. Logs are records of events and activities that occur on a system or application. Logs can provide useful information for troubleshooting and identifying the root cause of an issue. The administrator should look for any errors, warnings, or messages that indicate what happened to the SQL database service and why it stopped running.

NEW QUESTION 104

- (Topic 2)

A private IaaS administrator is receiving reports that all newly provisioned Linux VMs are running an earlier version of the OS than they should be. The administrator reviews the automation scripts to troubleshoot the issue and determines the scripts ran successfully. Which of the following is the MOST likely cause of the issue?

- A. API version incompatibility
- B. Misconfigured script account
- C. Wrong template selection
- D. Incorrect provisioning script indentation

Answer: C

Explanation:

The wrong template selection is the most likely cause of the issue of newly provisioned Linux VMs running an earlier version of OS than they should be in a private IaaS environment. A template is a preconfigured image or blueprint of a VM that contains an OS, applications, settings, etc., that can be used to create new VMs quickly and consistently. A template may have different versions or updates depending on when it was created or modified. If a template is selected incorrectly or not updated properly, it may result in creating VMs with an older or different version of OS than expected.

NEW QUESTION 107

- (Topic 2)

A technician just received the lessons learned from some recent data that was lost due to an on-premises file-server crash. The action point is to change the backup strategy to minimize manual intervention. Which of the following is the BEST approach for the technician to implement?

- A. Backup as a service
- B. RAID 1
- C. Long-term storage
- D. New backup devices

Answer: A

Explanation:

Backup as a service (BaaS) is the best approach for changing the backup strategy to minimize manual intervention after a data loss due to an on-premises file-server crash. BaaS is a cloud-based service that provides backup and recovery solutions for customers' data and systems. BaaS can automate and simplify backup processes by using cloud storage, encryption, deduplication, compression, scheduling, etc., without requiring customers to purchase or maintain backup hardware or software.

NEW QUESTION 111

- (Topic 2)

A system administrator is migrating a bare-metal server to the cloud. Which of the following types of migration should the systems administrator perform to accomplish this task?

- A. V2V
- B. V2P
- C. P2P
- D. P2V

Answer: D

Explanation:

P2V (Physical to Virtual) is a type of migration that converts a physical server into a virtual machine (VM). P2V migration can help to move a bare-metal server to the cloud by creating an image of its disk and configuration and uploading it to a cloud platform that supports VM creation from custom images.

NEW QUESTION 112

- (Topic 2)

A cloud administrator would like to deploy a cloud solution to its provider using automation techniques. Which of the following must be used? (Choose two.)

- A. Auto-scaling
- B. Tagging
- C. Playbook
- D. Templates
- E. Containers
- F. Serverless

Answer: CD

Explanation:

Playbook and templates are two things that must be used to deploy a cloud solution to its provider using automation techniques. A playbook is a file or script that defines a set of tasks or actions to be executed on one or more cloud resources or systems. A playbook can automate and standardize the deployment and configuration of cloud solutions using tools such as Ansible, Chef, Puppet, etc. A template is a preconfigured image or blueprint of a cloud resource or system that contains an OS, applications, settings, etc., that can be used to create new resources or systems quickly and consistently. A template can simplify and speed up the deployment of cloud solutions using tools such as AWS CloudFormation, Azure Resource Manager, Google Cloud Deployment Manager, etc.

NEW QUESTION 113

- (Topic 2)

A technician needs to deploy two virtual machines in preparation for the configuration of a financial application next week. Which of the following cloud deployment models should the technician use?

- A. XaaS
- B. IaaS
- C. PaaS
- D. SaaS

Answer: B

Explanation:

IaaS (Infrastructure as a Service) is the cloud deployment model that the technician should use to deploy two virtual machines in preparation for the configuration of a financial application next week. IaaS is a cloud service model that provides basic computing resources such as servers, storage, network, etc., to the customers. The customers have full control and flexibility over these resources and can install and configure any software they need on them. IaaS is suitable for deploying virtual machines, as it allows the customers to choose their preferred OS, applications, settings, etc., and customize them according to their needs.

NEW QUESTION 118

- (Topic 2)

An organization is using multiple SaaS-based business applications, and the systems administrator is unable to monitor and control the use of these subscriptions. The administrator needs to implement a solution that will help the organization apply security policies and monitor each individual SaaS subscription. Which of the following should be deployed to achieve these requirements?

- A. DLP
- B. CASB
- C. IPS
- D. HIDS

Answer: B

Explanation:

CASB (Cloud Access Security Broker) is what should be deployed to monitor and control the use of multiple SaaS-based business applications in a cloud environment. SaaS (Software as a Service) is a cloud service model that provides customers with access to software applications hosted on remote servers over a network or internet connection. SaaS can provide customers with convenience, flexibility, and scalability, but it may also introduce security risks such as data breaches, leaks, losses, etc., especially if customers have multiple SaaS subscriptions from different providers. CASB is a tool or service that acts as an intermediary between customers and SaaS providers. CASB can help to monitor and control the use of multiple SaaS subscriptions by providing features such as:

? Visibility: CASB can provide visibility into what SaaS applications are being used, by whom, when, where, how, etc., as well as identify any unauthorized or suspicious activities.

? Compliance: CASB can provide compliance with various laws, regulations, standards, policies, etc., that apply to SaaS applications and data, such as GDPR, HIPAA, PCI DSS, etc., as well as enforce them using rules or actions.

? Security: CASB can provide security for SaaS applications and data by detecting and preventing any threats or attacks, such as malware, phishing, ransomware, etc., as well as protecting them using encryption, authentication, authorization, etc.

NEW QUESTION 122

- (Topic 2)

After a few new web servers were deployed, the storage team began receiving incidents in their queue about the web servers. The storage administrator wants to verify the incident tickets that should have gone to the web server team. Which of the following is the MOST likely cause of the issue?

- A. Incorrect assignment group in service management
- B. Incorrect IP address configuration
- C. Incorrect syslog configuration on the web servers
- D. Incorrect SNMP settings

Answer: C

Explanation:

Incorrect syslog configuration on the web servers is the most likely cause of the issue of storage team receiving incidents in their queue about web servers after new web servers were deployed in a cloud environment. Syslog is a standard protocol that allows network devices and systems to send log messages to a centralized server or collector. Syslog can help to consolidate and manage logs from different sources in one place, which can facilitate monitoring, analysis, troubleshooting, auditing, etc. Incorrect syslog configuration on the web servers can cause them to send log messages to the wrong destination or queue, such as the storage team's queue, rather than the web server team's queue.

NEW QUESTION 127

- (Topic 2)

A DevOps administrator is designing a new machine-learning platform. The application needs to be portable between public and private clouds and should be kept as small as possible. Which of the following approaches would BEST meet these requirements?

- A. Virtual machines
- B. Software as a service
- C. Serverless computing
- D. Containers

Answer: D

Explanation:

Containers are the best approach to design a new machine-learning platform that needs to be portable between public and private clouds and should be kept as small as possible. Containers are isolated environments that can run applications and their dependencies without interfering with other processes or systems. Containers are lightweight, portable, and scalable, which makes them ideal for machine-learning applications. Containers can be moved easily between public and private clouds without requiring any changes or modifications. Containers can also reduce the size and complexity of applications by using only the necessary components and libraries.

NEW QUESTION 128

- (Topic 2)

Which of the following service models would be used for a database in the cloud?

- A. PaaS
- B. IaaS
- C. CaaS
- D. SaaS

Answer: A

Explanation:

PaaS (Platform as a Service) is a cloud service model that provides a platform for developing, testing, deploying, and managing applications in the cloud. PaaS includes the underlying infrastructure (servers, storage, network, etc.) as well as the middleware, databases, tools, frameworks, and APIs that are required for application development and delivery. Examples of PaaS are AWS Elastic Beanstalk, Azure App Service, Google App Engine, etc.

NEW QUESTION 129

- (Topic 2)

A company needs a solution to find content in images. Which of the following technologies, when used in conjunction with cloud services, would facilitate the BEST solution?

- A. Internet of Things
- B. Digital transformation
- C. Artificial intelligence
- D. DNS over TLS

Answer: C

Explanation:

Artificial intelligence (AI) is the technology that, when used in conjunction with cloud services, would facilitate the best solution for finding content in images. AI is a branch of computer science that aims to create machines or systems that can perform tasks that normally require human intelligence, such as reasoning, learning, decision making, etc. AI can be used to analyze images and extract information such as objects, faces, text, emotions, etc., using techniques such as computer vision, machine learning, natural language processing, etc. AI can help to find content in images faster, more accurately, and more efficiently than manual methods.

NEW QUESTION 132

- (Topic 2)

A systems administrator is examining a managed hosting agreement and wants to determine how much data would be lost if a server had to be restored from backups. To which of the following metrics should the administrator refer?

- A. RTO
- B. MTBF
- C. RPO
- D. MTTR

Answer: C

Explanation:

RPO (Recovery Point Objective) is the metric that the administrator should refer to determine how much data would be lost if a server had to be restored from backups. RPO is a metric that measures how much data can be lost or how far back in time a recovery point can be without causing significant impact or damage. RPO can help to determine how much data would be lost by comparing the time of the disruption or disaster with the time of the last backup or snapshot. RPO can also help to determine how frequently backups or snapshots should be performed to minimize data loss.

NEW QUESTION 133

- (Topic 2)

An organization suffered a critical failure of its primary datacenter and made the decision to switch to the DR site. After one week of using the DR site, the primary datacenter is now ready to resume operations.

Which of the following is the MOST efficient way to bring the block storage in the primary datacenter up to date with the DR site?

- A. Set up replication.
- B. Copy the data across both sites.
- C. Restore incremental backups.
- D. Restore full backups.

Answer: A

Explanation:

Reference: <https://www.ibm.com/docs/en/cloud-pak-system-w3550/2.3.3?topic=system-administering-block-storage-replication>

Setting up replication is the most efficient way to bring the block storage in the primary datacenter up to date with the DR site after a critical failure. Replication is a process of copying data from one location to another in real-time or near real-time. Replication can be synchronous or asynchronous, depending on the latency and bandwidth requirements. Replication can ensure data consistency and availability across multiple sites and facilitate faster recovery.

NEW QUESTION 138

- (Topic 2)

A systems administrator is deploying a solution that includes multiple network I/O-intensive VMs. The solution design requires that vNICs of the VMs provide low-latency, near-native performance of a physical NIC and data protection between the VMs. Which of the following would BEST satisfy these requirements?

- A. SR-IOV
- B. GENEVE
- C. SDN
- D. VLAN

Answer: A

Explanation:

SR-IOV (Single Root Input/Output Virtualization) is what would best satisfy the requirements of low-latency, near-native performance of a physical NIC and data protection between VMs for multiple network I/O-intensive VMs. SR-IOV is a technology that allows a physical NIC to be partitioned into multiple virtual NICs that can be assigned to different VMs. SR-IOV can provide the following benefits:

? Low-latency: SR-IOV can reduce latency by bypassing the hypervisor and allowing direct communication between the VMs and the physical NIC, without any overhead or interference.

? Near-native performance: SR-IOV can provide near-native performance by allowing the VMs to use the full capacity and functionality of the physical NIC, without any emulation or translation.

? Data protection: SR-IOV can provide data protection by isolating and securing the network traffic between the VMs and the physical NIC, without any exposure or leakage.

NEW QUESTION 140

- (Topic 2)

A Chief Information Security Officer (CISO) is evaluating the company's security management program. The CISO needs to locate all the assets with identified deviations and mitigation measures. Which of the following would help the CISO with these requirements?

- A. An SLA document
- B. ADR plan
- C. SOC procedures
- D. A risk register

Answer: D

Explanation:

A risk register is a document that records all the identified risks, their causes, impacts, probabilities, mitigation measures, and status for a project or an organization. A risk register helps to manage and monitor risks throughout their lifecycle and ensure they are addressed appropriately. A risk register would help the CISO to locate all the assets with identified deviations and mitigation measures.

NEW QUESTION 143

- (Topic 2)

An engineer is responsible for configuring a new firewall solution that will be deployed in a new public cloud environment. All traffic must pass through the firewall. The SLA for the firewall is 99.999%. Which of the following should be deployed?

- A. Two load balancers behind a single firewall
- B. Firewalls in a blue-green configuration
- C. Two firewalls in a HA configuration
- D. A web application firewall

Answer: C

Explanation:

Deploying two firewalls in a HA (High Availability) configuration is the best option to ensure all traffic passes through the firewall and meets the SLA (Service Level Agreement) of 99.999%. HA is a design principle that aims to minimize downtime and ensure continuous operation of a system or service. HA can be achieved by using redundancy, failover, load balancing, clustering, etc. Two firewalls in a HA configuration can provide redundancy and failover in case one firewall fails or becomes overloaded.

NEW QUESTION 144

- (Topic 2)

A company is preparing a hypervisor environment to implement a database cluster. One of the requirements is to share the disks between the nodes of the cluster to access the same LUN. Which of the following protocols should the company use? (Choose two.)

- A. CIFS
- B. FTP
- C. iSCSI
- D. RAID 10
- E. NFS
- F. FC

Answer: CF

Explanation:

These are the protocols that should be used to share the disks between the nodes of a database cluster to access the same LUN (Logical Unit Number). A LUN is an identifier that represents a logical unit of storage, such as a disk, partition, volume, etc., that can be accessed by a host system or device. To share the disks between the nodes of a cluster, the following protocols can be used:

? iSCSI (Internet Small Computer System Interface): This is a protocol that allows SCSI commands to be sent over IP networks. iSCSI can enable block-level storage access over a network, which means that the host system or device can access the storage as if it were a local disk.

? FC (Fibre Channel): This is a protocol that provides high-speed and low-latency data transfer over optical fiber cables. FC can also enable block-level storage access over a network, which means that the host system or device can access the storage as if it were a local disk.

NEW QUESTION 146

- (Topic 2)

A company needs to migrate the storage system and batch jobs from the local storage system to a public cloud provider. Which of the following accounts will MOST likely be created to run the batch processes?

- A. User
- B. LDAP
- C. Role-based
- D. Service

Answer: D

Explanation:

A service account is what will most likely be created to run the batch processes that migrate the storage system and batch jobs from the local storage system to a public cloud provider. A service account is a special type of account that is used to perform automated tasks or operations on a system or service, such as running scripts, applications, or processes. A service account can provide benefits such as:

? Security: A service account can have limited or specific permissions and roles that are required to perform the tasks or operations, which can prevent unauthorized or malicious access or actions.

? Efficiency: A service account can run the tasks or operations without any human intervention or interaction, which can save time and effort.

? Reliability: A service account can run the tasks or operations consistently and accurately, which can reduce errors or failures.

NEW QUESTION 148

- (Topic 2)

An administrator is securing a private cloud environment and wants to ensure only approved systems can connect to switches. Which of the following would be MOST useful to accomplish this task?

- A. VLAN
- B. NIPS
- C. WAF
- D. NAC

Answer: D

Explanation:

Reference: <https://www.cisco.com/c/en/us/products/security/what-is-network-access-control-nac.html>

NAC (Network Access Control) is what the administrator should implement to ensure only approved systems can connect to switches in a private cloud environment. NAC is a security technique that controls and restricts access to network resources based on predefined policies or rules. NAC can verify and authenticate users or devices before granting them access to switches or other network devices. NAC can also enforce compliance and security standards on users or devices before allowing them to connect to switches.

NEW QUESTION 150

- (Topic 2)

A company recently experienced a power outage that lasted 30 minutes. During this time, a whole rack of servers was inaccessible, even though the servers did not lose power.

Which of the following should be investigated FIRST?

- A. Server power
- B. Rack power
- C. Switch power
- D. SAN power

Answer: C

Explanation:

If a whole rack of servers was inaccessible during a power outage, even though the servers did not lose power, it is likely that the switch that connects them to the network lost power. Without network connectivity, the servers would not be able to communicate with other devices or services. The administrator should investigate the switch power source and ensure it has a backup power supply or UPS.

NEW QUESTION 151

- (Topic 2)

A cloud security analyst needs to ensure the web servers in the public subnet allow only secure communications and must remediate any possible issue. The stateful configuration for the public web servers is as follows:

ID	Direction	Protocol	Port	Source	Action
1	inbound	TCP	80	any	allow
2	inbound	TCP	443	any	allow
3	inbound	TCP	3306	any	allow
4	inbound	TCP	3389	any	allow
5	outbound	UDP	53	any	allow
*	both	any	any	any	deny

Which of the following actions should the analyst take to accomplish the objective?

- A. Remove rules 1, 2, and 5.
- B. Remove rules 1, 3, and 4.
- C. Remove rules 2, 3, and 4.
- D. Remove rules 3, 4, and 5.

Answer: A

Explanation:

To ensure the web servers in the public subnet allow only secure communications and remediate any possible issue, the analyst should remove rules 1, 2, and 5 from the stateful configuration. These rules are allowing insecure or unnecessary traffic to or from the web servers, which may pose security risks or performance issues. The rules are:

? Rule 1: This rule allows inbound traffic on port 80 (HTTP) from any source to any destination. HTTP is an unencrypted and insecure protocol that can expose web traffic to interception, modification, or spoofing. The analyst should remove this rule and use HTTPS (port 443) instead, which encrypts and secures web traffic.

? Rule 2: This rule allows outbound traffic on port 25 (SMTP) from any source to any destination. SMTP is a protocol that is used to send email messages. The web servers in the public subnet do not need to send email messages, as this is not their function. The analyst should remove this rule and block outbound SMTP traffic, which may prevent spamming or phishing attacks from compromised web servers.

? Rule 5: This rule allows inbound traffic on port 22 (SSH) from any source to any destination. SSH is a protocol that allows remote access and management of systems or devices using a command-line interface. The web servers in the public subnet do not need to allow SSH access from any source, as this may expose them to unauthorized or malicious access. The analyst should remove this rule and restrict SSH access to specific sources, such as the administrator's workstation or a bastion host.

NEW QUESTION 153

- (Topic 2)

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.

Answer: B

Explanation:

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.

NEW QUESTION 156

- (Topic 1)

A web server has been deployed in a public IaaS provider and has been assigned the public IP address of 72.135.10.100. Users are now reporting that when they browse to the website, they receive a message indicating the service is unavailable. The cloud administrator logs into the server, runs a netstat command, and notices the following relevant output:

```
TCP 17.3.130.3:0 72.135.10.100:5500 TIME_WAIT
TCP 17.3.130.3:0 72.135.10.100:5501 TIME_WAIT
TCP 17.3.130.3:0 72.135.10.100:5502 TIME_WAIT
TCP 17.3.130.3:0 72.135.10.100:5503 TIME_WAIT
TCP 17.3.130.3:0 72.135.10.100:5504 TIME_WAIT
```

Which of the following actions should the cloud administrator take to resolve the issue?

- A. Assign a new IP address of 192.168.100.10 to the web server
- B. Modify the firewall on 72.135.10.100 to allow only UDP
- C. Configure the WAF to filter requests from 17.3.130.3
- D. Update the gateway on the web server to use 72.135.10.1

Answer: D

Explanation:

Updating the gateway on the web server to use 72.135.10.1 is the best action to take to resolve the issue of the web server being unavailable after being deployed in a public IaaS provider and assigned the public IP address of 72.135.10.100. Updating the gateway can ensure that the web server can communicate with the Internet and other networks by using the correct router or device that connects the web server's network to other networks. Updating the gateway can also improve performance and reliability, as it can avoid any routing errors or conflicts that may prevent the web server from responding to remote login requests. References: CompTIA Cloud+ Certification Exam Objectives, page 15, section 2.8

NEW QUESTION 160

- (Topic 1)

A cloud engineer is responsible for managing two cloud environments from different MSPs. The security department would like to inspect all traffic from the two cloud environments.

Which of the following network topology solutions should the cloud engineer implement to reduce long-term maintenance?

- A. Chain
- B. Star
- C. Mesh
- D. Hub and spoke

Answer: D

Explanation:

Hub and spoke is a type of network topology that consists of a central node or device (hub) that connects to multiple peripheral nodes or devices (spokes). Hub and spoke can help reduce long-term maintenance for managing two cloud environments from different MSPs, as it can simplify and centralize the network configuration and management by using the hub as a single point of contact and control for the spokes. Hub and spoke can also improve network performance and security, as it can reduce latency, bandwidth consumption, and network congestion by routing traffic through the hub. References: CompTIA Cloud+ Certification Exam Objectives, page 15, section 2.8

NEW QUESTION 165

- (Topic 1)

A developer is no longer able to access a public cloud API deployment, which was working ten minutes prior.

Which of the following is MOST likely the cause?

- A. API provider rate limiting
- B. Invalid API token
- C. Depleted network bandwidth
- D. Invalid API request

Answer: A

Explanation:

API provider rate limiting is a restriction on the number of requests that can be made to a web service or application programming interface (API) within a certain time period. API provider rate limiting can cause a failure to access a public cloud API deployment, as it can reject or block any requests that exceed the limit. API provider rate limiting can be used by cloud providers to control the usage and traffic of their customers and prevent overloading or abuse of their resources. API provider rate limiting is the most likely cause for the developer being unable to access a public cloud API deployment that was working ten minutes prior. References: CompTIA Cloud+ Certification Exam Objectives, page 13, section 2.5

NEW QUESTION 167

- (Topic 1)

A systems administrator is troubleshooting network throughput issues following a deployment. The network is currently being overwhelmed by the amount of traffic between the database and the web servers in the environment.

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

- A. Set up affinity rules to keep web and database servers on the same hypervisor
- B. Enable jumbo frames on the gateway
- C. Move the web and database servers onto the same VXLAN
- D. Move the servers onto thick-provisioned storage

Answer: C

Explanation:

A virtual extensible local area network (VXLAN) is a type of network virtualization technology that creates logical networks or segments that span across multiple physical networks or locations. Moving the web and database servers onto the same VXLAN can help resolve the network throughput issues following a deployment, as it can reduce the network traffic between the database and the web servers by using a common virtual network identifier (VNI) and encapsulating the traffic within UDP packets. Moving the web and database servers onto the same VXLAN can also improve performance and security, as it can provide higher scalability, isolation, and encryption for the network traffic. References: CompTIA Cloud+ Certification Exam Objectives, page 15, section 2.8

NEW QUESTION 171

- (Topic 1)

A systems administrator is deploying a solution that requires a virtual network in a private cloud environment. The solution design requires the virtual network to transport multiple payload types.

Which of the following network virtualization options would BEST satisfy the requirement?

- A. VXLAN
- B. STT
- C. NVGRE
- D. GENEVE

Answer: D

Explanation:

Generic Network Virtualization Encapsulation (GENEVE) is a type of network virtualization technology that creates logical networks or segments that span across multiple physical networks or locations. GENEVE can satisfy the requirement of transporting multiple payload types in a virtual network in a private cloud environment, as it can support various network protocols and services by using a flexible and extensible header format that can encapsulate different types of payloads within UDP packets. GENEVE can also provide interoperability and compatibility, as it can integrate with existing network virtualization technologies such as VXLAN, STT, or NVGRE. References: CompTIA Cloud+ Certification Exam Objectives, page 15, section 2.8

NEW QUESTION 174

- (Topic 1)

A systems administrator is building a new virtualization cluster. The cluster consists of five virtual hosts, which each have flash and spinning disks. This storage is shared among all the virtual hosts, where a virtual machine running on one host may store data on another host.

This is an example of:

- A. a storage area network
- B. a network file system
- C. hyperconverged storage
- D. thick-provisioned disks

Answer: C

Explanation:

Hyperconverged storage is a type of storage architecture that combines compute, storage, and network resources into a single system or appliance. Hyperconverged storage uses software-defined storage (SDS) to pool and share the local storage of each node in the cluster, creating a distributed storage system that can be accessed by any node or virtual machine in the cluster. Hyperconverged storage can provide high performance, scalability, and efficiency for virtualized environments. The scenario of building a new virtualization cluster with five virtual hosts that share their flash and spinning disks among all the virtual hosts is an example of hyperconverged storage. References: [CompTIA Cloud+ Certification Exam Objectives], page 9, section 1.4

NEW QUESTION 177

- (Topic 1)

A systems administrator wants to have near-real-time information on the volume of data being exchanged between an application server and its clients on the Internet.

Which of the following should the systems administrator implement to achieve this objective?

- A. A stateful firewall
- B. DLP
- C. DNSSEC
- D. Network flows

Answer: D

Explanation:

Network flows are records of network traffic that capture information such as source and destination IP addresses, ports, protocols, timestamps, and byte and packet counts. Network flows can provide near-real-time information on the volume of data being exchanged between a system and its clients on the Internet, as they can measure and monitor the amount and rate of network traffic for each connection or session. Network flows can also help analyze network performance, troubleshoot network issues, and detect network anomalies or security incidents. A systems administrator should implement network flows to achieve the objective of having near-real-time information on the volume of data being exchanged between an application server and its clients on the Internet. References: CompTIA Cloud+ Certification Exam Objectives, page 16,

section 3.2

NEW QUESTION 179

- (Topic 1)

A systems administrator is deploying a new storage array for backups. The array provides 1PB of raw disk space and uses 14TB nearline SAS drives. The solution must tolerate at least two failed drives in a single RAID set.

Which of the following RAID levels satisfies this requirement?

- A. RAID 0
- B. RAID 1
- C. RAID 5
- D. RAID 6
- E. RAID 10

Answer: D

Explanation:

RAID 6 is a type of RAID level that uses block-level striping with two parity blocks distributed across all member disks. RAID 6 can provide redundancy and fault tolerance, as it can survive the failure of up to two disks without losing any data. RAID 6 can also support large data sets and high-capacity disks, as it can offer more usable space and better performance than other RAID levels with similar features, such as RAID 5 or RAID 10. RAID 6 is the best RAID level for a systems administrator to use when deploying a new

storage array for backups that provides 1PB of raw disk space and uses 14TB nearline SAS drives and must tolerate at least two failed drives in a single RAID set.

References: CompTIA Cloud+ Certification Exam Objectives, page 9, section 1.4

NEW QUESTION 180

- (Topic 1)

A cloud administrator recently noticed that a number of files stored at a SaaS provider's file-sharing service were deleted. As part of the root cause analysis, the administrator noticed the parent folder permissions were modified last week. The administrator then used a test user account and determined the permissions on the files allowed everyone to have write access.

Which of the following is the best step for the administrator to take NEXT?

- A. Identify the changes to the file-sharing service and document
- B. Acquire a third-party DLP solution to implement and manage access
- C. Test the current access permissions to the file-sharing service
- D. Define and configure the proper permissions for the file-sharing service

Answer: D

Explanation:

Permissions are rules or settings that determine what actions users can perform on files or resources in a system or service. Permissions can help control and restrict access to files or resources based on various criteria, such as user identity, role, group, or ownership. Defining and configuring the proper permissions for the file-sharing service is the best step for the administrator to take next after discovering that sales group members can access the financial application due to being part of the finance group and having write access to all files in the file-sharing service. Defining and configuring the proper permissions can prevent unauthorized or accidental access or modification of files or resources by limiting or granting access based on specific criteria.

References: CompTIA Cloud+ Certification Exam Objectives, page 14, section 2.7

NEW QUESTION 183

- (Topic 1)

An organization's web server farm, which is hosted in the cloud with DNS load balancing, is experiencing a spike in network traffic. This has caused an outage of the organization's web server infrastructure.

Which of the following should be implemented to prevent this in the future as a mitigation method?

- A. Enable DLP
- B. Configure microsegmentation
- C. Enable DNSSEC
- D. Deploy a vADC appliance

Answer: D

Explanation:

A virtual application delivery controller (vADC) is a type of network device or software that provides load balancing, security, and optimization for web applications or services. Deploying a vADC appliance can help prevent an outage of the organization's web server infrastructure due to a spike in network traffic, as it can distribute the traffic across multiple web servers and improve the performance and availability of web applications or services. Deploying a vADC appliance can also provide mitigation methods such as DDoS protection, SSL offloading, and caching to enhance the security and efficiency of web traffic delivery.

References: CompTIA Cloud+ Certification Exam Objectives, page 15, section 2.8

NEW QUESTION 186

- (Topic 1)

A systems administrator is using VMs to deploy a new solution that contains a number of application VMs.

Which of the following would provide high availability to the application environment in case of hypervisor failure?

- A. Anti-affinity rules
- B. Cold migration
- C. Live migration
- D. Affinity rules

Answer: A

Explanation:

Anti-affinity rules are rules or policies that prevent two or more VMs from running on the same host or cluster in a cloud environment. Anti-affinity rules can provide high availability to an application environment in case of hypervisor failure, as they can distribute or separate the application VMs across different hosts or clusters and avoid having a single point of failure. Anti-affinity rules can also improve performance and reliability, as they can reduce contention and load by balancing the resource utilization across multiple hosts or clusters. References: CompTIA Cloud+ Certification Exam Objectives, page 10, section 1.5
 Reference: <https://www.vmware.com/products/vsphere/high-availability.html>

NEW QUESTION 189

- (Topic 1)

After accidentally uploading a password for an IAM user in plain text, which of the following should a cloud administrator do FIRST? (Choose two.)

- A. Identify the resources that are accessible to the affected IAM user
- B. Remove the published plain-text password
- C. Notify users that a data breach has occurred
- D. Change the affected IAM user's password
- E. Delete the affected IAM user

Answer: BD

Explanation:

Removing the published plain-text password and changing the affected IAM user's password are the first actions that a cloud administrator should take after accidentally uploading a password for an IAM user in plain text, as they can prevent or limit any unauthorized or malicious access to the cloud resources or services using the compromised password. Removing the published plain-text password can ensure that the password is not exposed or available to anyone who may access or view the uploaded file. Changing the affected IAM user's password can ensure that the password is updated and secured using encryption or hashing techniques. References: CompTIA Cloud+ Certification Exam Objectives, page 14, section 2.7

NEW QUESTION 191

- (Topic 1)

An organization has multiple VLANs configured to segregate the network traffic. Following is the breakdown of the network segmentation:

- ? Production traffic (10.10.0.0/24)
- ? Network backup (10.20.0.0/25)
- ? Virtual IP network (10.20.0.128/25)

The following configuration exists on the server:

Server name	Interface	IP address	Gateway
COMPSRV01	Production	10.10.0.12/24	10.10.0.1
COMPSRV01	Network backup	10.20.0.12/25	10.10.0.1

The backup administrator observes that the weekly backup is failing for this server. Which of the following commands should the administrator run to identify the issue?

- A. ROUTE PRINT
- B. NETSTAT -A
- C. IPCONFIG /ALL
- D. NET SM

Answer: A

Explanation:

ROUTE PRINT is a command that displays the routing table of a system, which shows the destination network, the gateway, the interface, and the metric for each route. ROUTE PRINT can help identify the issue of the weekly backup failing for this server, as it can show if there is a valid route to the network backup segment (10.20.0.0/25) from the production traffic segment (10.10.0.0/24). If there is no route or an incorrect route, the backup will fail to reach the destination. The administrator can use ROUTE PRINT to verify and troubleshoot the routing configuration of the server. References: CompTIA Cloud+ Certification Exam Objectives, page 16, section 3.2
 Reference: <https://www.toolbox.com/tech/operating-systems/blogs/using-the-route-print-command-in-windows-7-022310/>

NEW QUESTION 195

- (Topic 1)

A cloud administrator is planning to migrate a globally accessed application to the cloud.

Which of the following should the cloud administrator implement to BEST reduce latency for all users?

- A. Regions
- B. Auto-scaling
- C. Clustering
- D. Cloud bursting

Answer: A

Explanation:

Regions are geographical locations or areas where cloud service providers have data centers or facilities that host their cloud resources or services. Regions can help reduce latency for all users when deploying a globally accessed application to the cloud, as they can enable faster and closer access to the cloud resources or services based on the user's physical location. Regions can also improve performance and availability, as they can provide redundancy and load balancing by distributing the workload across multiple locations. References: CompTIA Cloud+ Certification Exam Objectives, page 15, section 2.8

NEW QUESTION 196

- (Topic 4)

A cloud engineer is deploying a server in a cloud platform. The engineer reviews a security scan report. Which of the following recommended services should be disabled? (Select two).

- A. Telnet

- B. FTP
- C. Remote log-in
- D. DNS
- E. DHCP
- F. LDAP

Answer: AB

Explanation:

Telnet and FTP are recommended services to be disabled when deploying a server in a cloud platform, as they are insecure protocols that transmit data in plain text and expose credentials and sensitive information to potential attackers¹². Remote log-in, DNS, DHCP, and LDAP are not necessarily recommended to be disabled, as they may provide useful functionality for the server and the cloud environment. However, they should be configured properly and secured with encryption, authentication, and authorization mechanisms³⁴.

References: CompTIA Cloud+ CV0-003 Exam Objectives, Objective 4.2: Given a scenario, apply security configurations and compliance controls ; CompTIA Quick Start Guide to Tackling Cloud Security Concerns³

NEW QUESTION 201

- (Topic 4)

A systems administrator is trying to connect to a remote KVM host. The command line appears as follows:

```
serveradmin@localhost:~$ virsh remotehost
Error: daemon not running on remote host.
```

After logging in to the remote server, the administrator verifies the daemon is running. Which of the following should the administrator try NEXT?

- A. Opening port 22 on the firewall
- B. Running the command with elevated privileges
- C. Checking if the SSH password is correct
- D. Ensuring the private key was properly imported

Answer: B

Explanation:

The answer is B. Running the command with elevated privileges. According to the web search results, the error message “End of file while reading data: sh: 1: nc: not found: Input/output error” indicates that the remote host does not have the nc (netcat) command installed or available in the PATH¹². The nc command is used by libvirt to establish a connection between the client and the server. To fix this error, the administrator should install nc on the remote host or ensure that it is in the PATH. However, to do this, the administrator needs to have elevated privileges, such as sudo or root, on the remote host. Therefore, the administrator should try running the command with elevated privileges, such as sudo virsh remotehost or su -c ‘virsh remotehost’. This will allow the administrator to install nc or modify the PATH on the remote host and then connect to it using libvirt.

NEW QUESTION 204

- (Topic 4)

A systems administrator is deploying a new version of a website. The website is deployed in the cloud using a VM cluster. The administrator must then deploy the new version into one VM first. After a period of time, if there are no issues detected, a second VM will be updated. This process must continue until all the VMS are updated. Which of the following upgrade methods is being implemented?

- A. Canary
- B. Blue-green
- C. Rolling
- D. Staging

Answer: C

Explanation:

The upgrade method that is being implemented by the systems administrator is rolling. A rolling upgrade is a type of upgrade that applies the new version of a software or service to a subset of nodes or instances at a time, while the rest of the nodes or instances continue to run the old version. This way, the upgrade can be performed gradually and incrementally, without causing downtime or disruption to the entire system. A rolling upgrade can also help to monitor and test the new version for any issues or errors, and roll back to the old version if needed¹².

A canary upgrade is a type of upgrade that applies the new version of a software or service to a small and selected group of users or customers, before rolling it out to the rest of the population. This way, the upgrade can be evaluated for its performance, functionality, and feedback, and any problems or bugs can be fixed before affecting the majority of users or customers³⁴.

A blue-green upgrade is a type of upgrade that involves having two identical environments, one running the old version (blue) and one running the new version (green) of a software or service. The traffic is switched from the blue environment to the green environment once the new version is ready and tested. This way, the upgrade can be performed quickly and seamlessly, without any downtime or risk of failure. The blue environment can also serve as a backup in case of any issues with the green environment⁵.

A staging upgrade is a type of upgrade that involves having a separate environment that mimics the production environment, where the new version of a software or service is deployed and tested before moving it to the production environment. This way, the upgrade can be verified and validated for its compatibility, security, and quality, and any defects or errors can be resolved before affecting the live system.

NEW QUESTION 208

- (Topic 4)

A cloud administrator created a developer desktop image and added it to the VDI farm in a private cloud environment. One of the developers opened a VDI session and noticed that compiling the code was taking up to one hour to complete. However, when the developer compiles the code on a local machine, the job completes in less than five minutes. Which of the following sizing techniques would be best to use to improve the performance of the compile job?

- A. Add more servers to the VDI environment.
- B. Increase the CPU and the memory on the VDI template.
- C. Configure the VDI environment to increase sessions automatically.

D. Migrate code compile jobs to a public cloud provider.

Answer: B

Explanation:

The most likely cause of the poor performance of the compile job is that the VDI template does not have enough CPU and memory resources to handle the task efficiently. Compiling code is a CPU-intensive and memory-intensive process that requires sufficient computing power to run smoothly. By increasing the CPU and memory on the VDI template, the cloud administrator can improve the performance of the compile job and reduce the time it takes to complete. Adding more servers to the VDI environment or configuring the VDI environment to increase sessions automatically would not help, as they would only affect the scalability and availability of the VDI farm, not the performance of individual sessions. Migrating code compile jobs to a public cloud provider would incur additional costs and complexity, and may not be feasible or desirable for the organization. References: The Official CompTIA Cloud+ Self-Paced Study Guide (CV0-003) eBook, Chapter 3, Section 3.3, page 971

NEW QUESTION 212

- (Topic 4)

Which of the following enables CSPs to offer unlimited capacity to customers?

- A. Adequate budget
- B. Global data center distribution
- C. Economies of scale
- D. Agile project management

Answer: C

Explanation:

The correct answer is C. Economies of scale.

Economies of scale are the cost advantages that CSPs can achieve by increasing the size and scale of their operations. By spreading the fixed costs of infrastructure, software, and personnel over a larger customer base and data volume, CSPs can reduce the average cost per unit of service and offer unlimited capacity to customers at competitive prices¹. Adequate budget is not a sufficient condition for offering unlimited capacity, as CSPs still need to optimize their resource utilization and efficiency to meet the growing demand for data storage and processing.

Global data center distribution is a strategy that CSPs use to improve their service availability, reliability, and performance by locating their servers closer to their customers and reducing network latency. However, this does not necessarily imply unlimited capacity, as CSPs still need to manage the trade-offs between data center size, cost, and power consumption.

Agile project management is a methodology that CSPs use to deliver their services faster, better, and cheaper by adopting iterative, incremental, and collaborative approaches. However, this does not directly affect their capacity, as CSPs still need to scale their infrastructure and software to handle the increasing data load.

NEW QUESTION 216

- (Topic 4)

A cloud administrator must ensure all servers are in compliance with the company's security policy Which of the following should the administrator check FIRST?

- A. The application version
- B. The OS version
- C. Hardened baselines
- D. Password policies

Answer: C

Explanation:

Hardened baselines are a set of security best practices that reduce the vulnerability of a system to exploits by reducing its attack surface¹. They are also known as security configurations or benchmarks, and they provide a standard level of system hardening for an organization²³.

Checking the hardened baselines of the servers is the first step that a cloud administrator should take to ensure compliance with the company's security policy.

This is because hardened baselines can help to:

Identify and eliminate common vulnerabilities and exposures (CVEs) that attackers can exploit¹.

Remove unnecessary or unused services, accounts, software, and ports that can increase the attack surface²³.

Apply appropriate settings and controls for encryption, authentication, authorization, firewall, and logging²³.

Streamline audits and testing by reducing complexity and providing a reliable benchmark²³.

NEW QUESTION 221

- (Topic 4)

A cloud engineer is migrating a customer's web servers from a hypervisor platform to a CSP environment. The engineer needs to decouple the infrastructure and components during the migration to reduce the single points of failure. Which of the following storage options should the cloud engineer migrate the content to in order to improve availability?

- A. Block
- B. File
- C. Object
- D. iSCSI
- E. NFS

Answer: C

Explanation:

Object storage is a storage option that stores data as discrete units called objects, which are identified by a unique identifier and can have metadata attached to them. Object storage can help the cloud engineer migrate the content to improve availability by decoupling the data from the underlying infrastructure and components. Object storage can also provide high scalability, durability, and redundancy for the data, as well as support for multiple protocols and access methods. Object storage can be accessed through APIs, web interfaces, or gateways that can emulate file or block storage. Object storage is suitable for storing unstructured or static data, such as web content, images, videos, or documents. References: CompTIA Cloud+ CV0-003 Certification Study Guide, Chapter 4, Objective 4.1: Given a scenario, implement cloud storage solutions.

NEW QUESTION 224

- (Topic 4)

A systems administrator is attempting to gather information about services and resource utilization on VMS in a cloud environment. Which of the following will BEST accomplish this objective?

- A. Syslog
- B. SNMP
- C. CMDB
- D. Service management
- E. Performance monitoring

Answer: E

Explanation:

Performance monitoring is the process of collecting and analyzing metrics related to the performance and availability of resources in a cloud environment¹. Performance monitoring can help a systems administrator to gather information about services and resource utilization on VMs in a cloud environment by providing the following benefits²:

- ? Identify and troubleshoot performance issues and bottlenecks before they affect the end users or business operations.
- ? Optimize the resource allocation and configuration to meet the performance requirements and SLAs of the services.
- ? Plan for future capacity and scalability needs based on the historical trends and patterns of resource utilization.
- ? Compare the performance and costs of different cloud service providers, regions, and SKUs.

Some of the tools and services that can help with performance monitoring in a cloud environment are³:

- ? Azure Monitor: A comprehensive service that provides a unified view of the health, performance, and availability of your Azure resources, applications, and services. Azure Monitor collects metrics, logs, and traces from various sources and provides analysis, visualization, alerting, and automation capabilities.
- ? Azure Advisor: A personalized service that provides recommendations to optimize your Azure resources for performance, security, cost, reliability, and operational excellence. Azure Advisor analyzes your resource configuration and usage data and suggests best practices to improve your cloud environment.
- ? Azure Application Insights: A service that monitors the performance and usage of your web applications and services. Application Insights collects telemetry data such as requests, dependencies, exceptions, page views, custom events, and metrics from your application code and provides powerful analytics, diagnostics, and alerting features.
- ? Azure Log Analytics: A service that collects and analyzes data from various sources such as Azure Monitor, Azure services, VMs, containers, applications, and other cloud or on-premises systems. Log Analytics enables you to query, visualize, and correlate log data using the Kusto Query Language (KQL) and create custom dashboards and reports.

Syslog is a standard protocol for sending log messages from network devices to a central server. Syslog can help with logging and auditing activities in a cloud environment, but it does not provide performance monitoring capabilities. Therefore, option A is incorrect. SNMP (Simple Network Management Protocol) is a protocol for collecting and organizing information about managed devices on a network. SNMP can help with network management and monitoring in a cloud environment, but it does not provide comprehensive performance monitoring for VMs and services. Therefore, option B is incorrect.

CMDB (Configuration Management Database) is a database that stores information about the configuration items (CIs) in an IT environment. CMDB can help with configuration management and change management in a cloud environment, but it does not provide performance monitoring capabilities. Therefore, option C is incorrect.

Service management is a set of processes and practices that aim to deliver value to customers by providing quality services that meet their needs and expectations. Service management can help with service design, delivery, support, and improvement in a cloud environment, but it does not provide performance monitoring capabilities. Therefore, option D is incorrect.

NEW QUESTION 229

- (Topic 4)

A cloud administrator needs to deploy a security virtual appliance in a private cloud environment, but this appliance will not be part of the standard catalog of items for other users to request. Which of the following is the BEST way to accomplish this task?

- A. Create an empty V
- B. import the hard disk of the virtual applianc
- C. and configure the CPU and memory.
- D. Acquire the build scripts from the vendor and recreate the appliance using the baseline templates
- E. Import the virtual appliance into the environment and deploy it as a VM
- F. Convert the virtual appliance to a template and deploy a new VM using the template.

Answer: C

Explanation:

The correct answer is C. Import the virtual appliance into the environment and deploy it as a VM.

A virtual appliance is a pre-packaged and pre-configured software solution that runs on a virtual machine (VM). A virtual appliance typically consists of an operating system, an application, and any required dependencies, and is designed to provide a specific function or service. A virtual appliance can be distributed as a single file or a set of files that can be imported into a virtualization platform, such as VMware, Hyper-V, or KVM .

A cloud administrator can deploy a security virtual appliance in a private cloud environment by importing the virtual appliance into the environment and deploying it as a VM. This is the best way to accomplish this task because it preserves the original configuration and functionality of the virtual appliance, and does not require any additional installation or customization. The cloud administrator can also control the access and visibility of the virtual appliance, and prevent other users from requesting it from the standard catalog of items .

Creating an empty VM, importing the hard disk of the virtual appliance, and configuring the CPU and memory is not the best way to accomplish this task because it involves more steps and complexity than importing the virtual appliance as a whole. It also introduces the risk of losing or corrupting some data or settings during the import process, or misconfiguring the CPU and memory for the virtual appliance.

Acquiring the build scripts from the vendor and recreating the appliance using the baseline templates is not the best way to accomplish this task because it involves more time and effort than importing the virtual appliance directly. It also depends on whether the vendor provides the build scripts or not, and whether they are compatible with the baseline templates or not.

Converting the virtual appliance to a template and deploying a new VM using the template is not the best way to accomplish this task because it adds an unnecessary step of creating a template from the virtual appliance. It also does not prevent other users from accessing or requesting the template from the catalog of items.

NEW QUESTION 230

- (Topic 4)

A systems administrator needs to connect the companys network to a public cloud services provider. Which of the following will BEST ensure encryption in transit for data transfers?

- A. Identity federation
- B. A VPN tunnel
- C. A proxy solution
- D. A web application firewall

Answer: B

Explanation:

The answer is A. SAML. SAML (Security Assertion Markup Language) is a standard for exchanging authentication and authorization data between different parties, such as a user and a service provider. In a federated cluster, SAML can be used to enable single sign-on (SSO) for users across multiple clusters or cloud providers. SAML relies on the exchange of XML-based assertions that contain information about the user's identity, attributes, and entitlements. If the users' API access tokens have become invalid, it could be because the SAML assertions have expired, been revoked, or corrupted. The administrator should check the SAML configuration and logs to determine the cause of this issue.

Some possible sources of information about SAML and federated clusters are:

? Authenticating | Kubernetes: This page provides an overview of authenticating users in Kubernetes, including using SAML for federated identity.

? Authenticating to the Kubernetes API server - Google Cloud: This page explains how to authenticate to the Kubernetes API server on Google Cloud, including using SAML for federated identity with Google Cloud Identity Platform.

? Error 403 User not authorized when trying to access Azure Databricks API through Active Directory - Stack Overflow: This page discusses a similar issue of users getting an error when trying to access Azure Databricks API using SAML and Active Directory.

NEW QUESTION 232

- (Topic 4)

A cloud security analyst needs to ensure the web servers in the public subnet allow only secure communications and must remediate any possible issue. The stateful configuration for the public web servers is as follows:

ID	Direction	Protocol	Port	Source	Action
1	inbound	TCP	80	any	allow
2	inbound	TCP	443	any	allow
3	inbound	TCP	3306	any	allow
4	inbound	TCP	3389	any	allow
5	outbound	UDP	53	any	allow
*	both	any	any	any	deny

Which Of the following actions Should the analyst take to accomplish the Objective?

- A. Remove rules 1, 2, and 5.
- B. Remove rules 1, 3, and 4.
- C. Remove rules 2,3, and 4.
- D. Remove rules 3,4, and 5.

Answer: B

Explanation:

The correct answer is B. Remove rules 1, 3, and 4.

The objective is to ensure the web servers in the public subnet allow only secure communications. This means that only HTTPS traffic should be allowed on port 443, which is the standard port for secure web connections. HTTPS traffic uses the TCP protocol and encrypts the data between the client and the server.

Rule 1 allows all TCP traffic on any port from any source. This is too permissive and exposes the web servers to potential attacks or unauthorized access. Rule 1 should be removed to restrict the TCP traffic to only port 443.

Rule 3 allows all UDP traffic on any port from any source. UDP is a connectionless protocol that does not guarantee reliable or secure delivery of data. UDP is typically used for streaming media, voice over IP (VoIP), or online gaming, but not for web servers. Rule 3 should be removed to prevent unnecessary or malicious UDP traffic.

Rule 4 allows all ICMP traffic from any source. ICMP is a protocol that is used for diagnostic or control purposes, such as ping or traceroute. ICMP traffic can be used by attackers to scan or probe the network for vulnerabilities or information. Rule 4 should be removed to block ICMP traffic and reduce the attack surface.

Rule 2 allows TCP traffic on port 443 from any source. This is the desired rule that allows secure web communications using HTTPS. Rule 2 should be kept.

Rule 5 denies all other traffic that does not match any of the previous rules. This is the default rule that provides a catch-all protection for the web servers. Rule 5 should be kept. Therefore, the analyst should remove rules 1, 3, and 4 to accomplish the objective.

NEW QUESTION 236

- (Topic 4)

A systems administrator deployed a new web application in a public cloud and would like to test it, but the company's network firewall is only allowing outside connections to the cloud provider network using TCP port 22. While waiting for the network administrator to open the required ports, which of the following actions should the systems administrator take to test the new application? (Select two).

- A. Create an IPSec tunnel.
- B. Create a VPN tunnel.
- C. Open a browser using the default gateway IP address.
- D. Open a browser using the localhost IP address.
- E. Create a GRE tunnel.
- F. Create a SSH tunnel.

Answer: BF

Explanation:

To test the new web application in the public cloud, the systems administrator should create a replica database, synchronize the data, and switch to the new instance, and create a SSH tunnel. Creating a replica database can help minimize the downtime and ensure data consistency during the migration. Synchronizing the data can help keep the replica database up to date with the original database. Switching to the new instance can help activate the new web application in the public cloud. Creating a SSH tunnel can help bypass the network firewall and access the web application using TCP port 22. SSH is a secure protocol that can create encrypted tunnels between the local and remote hosts. By creating a SSH tunnel, the systems administrator can forward the web application traffic through the tunnel and test it using a web browser. References: [CompTIA Cloud+ CV0-003 Certification Study Guide], Chapter 7, Objective 7.1: Given a scenario, migrate applications and data to the cloud.

NEW QUESTION 239

- (Topic 4)

A company would like to move all its on-premises platforms to the cloud. The company has enough skilled Linux and web-server engineers but only a couple of skilled database administrators. It also has little expertise in managing email services. Which of the following solutions would BEST match the skill sets of available personnel?

- A. Run the web servers in PaaS, and run the databases and email in SaaS.
- B. Run the web servers, databases, and email in SaaS.
- C. Run the web servers in IaaS, the databases in PaaS, and the email in SaaS.
- D. Run the web servers, databases, and email in IaaS.

Answer: C

Explanation:

To answer this question, we need to understand the different types of cloud computing models and how they suit the skill sets of the available personnel. According to Google Cloud, there are three main models for cloud computing: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). Each model provides different levels of control, flexibility, and management over the cloud resources and services¹.

? IaaS: This model provides access to networking features, computers (virtual or on dedicated hardware), and data storage space. It gives the highest level of flexibility and management control over the IT resources and is most similar to existing IT resources that many IT departments and developers are familiar with².

? PaaS: This model provides a complete cloud platform for developing, running, and managing applications without the cost, complexity, and inflexibility of building and maintaining the underlying infrastructure. It removes the need for organizations to manage the hardware and operating systems and allows them to focus on the deployment and management of their applications².

? SaaS: This model provides a completed product that is run and managed by the service provider. It does not require any installation, maintenance, or configuration by the customers. It is typically used for end-user applications that are accessed through a web browser or a mobile app².

Based on these definitions, we can evaluate each option:

? Option A: Run the web servers in PaaS, and run the databases and email in SaaS. This option is not the best match for the skill sets of the available personnel because it does not leverage their expertise in Linux and web-server engineering. Running the web servers in PaaS means that they will have less control and customization over the web server environment and will have to rely on the service provider's platform features. Running the databases and email in SaaS means that they will not need any database administration or email management skills, but they will also have less flexibility and security over their data and communication.

? Option B: Run the web servers, databases, and email in SaaS. This option is not a good match for the skill sets of the available personnel because it does not utilize their skills at all. Running everything in SaaS means that they will have no control or responsibility over any aspect of their cloud environment and will have to depend entirely on the service provider's products. This option may be suitable for some small businesses or non-technical users who do not have any IT skills or resources, but not for a company that has skilled Linux and web-server engineers.

? Option C: Run the web servers in IaaS, the databases in PaaS, and the email in SaaS. This option is the best match for the skill sets of the available personnel because it balances their strengths and weaknesses. Running the web servers in IaaS means that they can use their Linux and web-server engineering skills to configure, manage, and optimize their web server infrastructure according to their needs. Running the databases in PaaS means that they can leverage the service provider's platform features to simplify their database development and administration tasks without having to worry about the underlying hardware and operating systems. Running the email in SaaS means that they can outsource their email services to a reliable and secure service provider without having to invest in or manage their own email infrastructure.

? Option D: Run the web servers, databases, and email in IaaS. This option is not a good match for the skill sets of the available personnel because it puts too much burden on them. Running everything in IaaS means that they will have to handle all aspects of their cloud environment, including networking, computing, storage, security, backup, scaling, patching, etc. This option may be suitable for some large enterprises or highly technical users who have full control and customization over their cloud environment, but not for a company that has only a couple of skilled database administrators and little expertise in managing email services.

Therefore, option C is the correct answer.

NEW QUESTION 244

- (Topic 4)

A systems administrator is responsible for upgrading operating systems on VMs that are hosted in a cloud environment. The systems administrator wants to ensure the VMs receive updates for as long as possible. Which of the following should the systems administrator choose?

- A. Stable
- B. Nightly
- C. LTS
- D. Canary
- E. EDR

Answer: C

Explanation:

LTS stands for Long Term Support, and it is a term that refers to a version of an operating system that receives updates and security patches for a longer period of time than other versions. LTS versions are usually more stable and reliable than other versions, and they are suitable for users who want to avoid frequent changes or compatibility issues. By choosing LTS versions for the VMs that are hosted in a cloud environment, the systems administrator can ensure that the VMs receive updates for as long as possible, and benefit from the enhanced security and performance of the operating system. LTS versions are typically released every few years, and they are supported for several years after their release. For example, Ubuntu 20.04 LTS is supported until April 2025, while Ubuntu 21.04 is supported until January 2022. References: CompTIA Cloud+ CV0-003 Certification Study Guide, Chapter 5, Objective 5.2: Given a scenario, troubleshoot common cloud resource and service issues.

NEW QUESTION 248

- (Topic 4)

A cloud engineer is deploying a server in a cloud platform. The engineer reviews a security scan report. Which of the following recommended services should be disabled? (Select TWO).

- A. Telnet
- B. FTP
- C. Remote login
- D. DNS
- E. DHCP
- F. LDAP

Answer: AB

Explanation:

Telnet and FTP are two services that should be disabled on a cloud server because they are insecure and vulnerable to attacks. Telnet and FTP use plain text to transmit data over the network, which means that anyone who can intercept the traffic can read or modify the data, including usernames, passwords, commands, files, etc. This can lead to data breaches, unauthorized access, or malicious actions on the server¹.

Instead of Telnet and FTP, more secure alternatives should be used, such as SSH (Secure Shell) and SFTP (Secure File Transfer Protocol). SSH and SFTP use encryption to protect the data in transit and provide authentication and integrity checks for the communication. SSH and SFTP can prevent eavesdropping, tampering, or spoofing of the data and ensure the confidentiality and privacy of the server².

The other options are not services that should be disabled on a cloud server:

? Option C: Remote login. Remote login is a service that allows users to access a remote server from another location using a network connection. Remote login can be useful for managing, configuring, or troubleshooting a cloud server without having to physically access it. Remote login can be secured by using encryption, authentication, authorization, and logging mechanisms³.

? Option D: DNS (Domain Name System). DNS is a service that translates human-friendly domain names into IP addresses that can be used to communicate over the Internet. DNS is essential for resolving the names of the cloud resources and services that are hosted on the cloud platform. DNS can be secured by using DNSSEC (DNS Security Extensions), which add digital signatures to DNS records to verify their authenticity and integrity.

? Option E: DHCP (Dynamic Host Configuration Protocol). DHCP is a service that assigns IP addresses and other network configuration parameters to devices on a network. DHCP can simplify the management of IP addresses and avoid conflicts or errors in the network. DHCP can be secured by using DHCP snooping, which filters out unauthorized DHCP messages and prevents rogue DHCP servers from assigning IP addresses.

? Option F: LDAP (Lightweight Directory Access Protocol). LDAP is a service that stores and organizes information about users, devices, and resources on a network. LDAP can provide identity management and access control for the cloud environment. LDAP can be secured by using LDAPS (LDAP over SSL/TLS), which encrypts the LDAP traffic and provides authentication and integrity checks.

NEW QUESTION 252

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

CV0-003 Practice Exam Features:

- * CV0-003 Questions and Answers Updated Frequently
- * CV0-003 Practice Questions Verified by Expert Senior Certified Staff
- * CV0-003 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * CV0-003 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The CV0-003 Practice Test Here](#)