



CompTIA

Exam Questions CV0-003

CompTIA Cloud+ Certification Exam

About ExamBible

[Your Partner of IT Exam](#)

Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

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 is running a database application on a SATA disk, and a customer is experiencing slow performance most of the time. Which of the following should be implemented to improve application performance?

- A. Increase disk capacity
- B. Increase the memory and network bandwidth
- C. Upgrade the application
- D. Upgrade the environment and use SSD drives

Answer: D

Explanation:

Upgrading the environment and using solid state drives (SSDs) can improve application performance for a database application that is running on a serial advanced technology attachment (SATA) disk and experiencing slow performance most of the time. Upgrading the environment can involve updating or replacing the hardware, software, or network components that support the application to enhance their functionality, capacity, or compatibility. Using SSDs can provide faster and more reliable data access and storage than SATA disks, as they use flash memory instead of spinning disks to store data. SSDs can also reduce latency, power consumption, and heat generation. References: CompTIA Cloud+ Certification Exam Objectives, page 9, section 1.4

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)

An SQL injection vulnerability was reported on a web application, and the cloud platform team needs to mitigate the vulnerability while it is corrected by the development team. Which of the following controls will BEST mitigate the risk of exploitation?

- A. DLP
- B. HIDS
- C. NAC
- D. WAF

Answer: D

Explanation:

A web application firewall (WAF) is a type of network security device or software that monitors and filters HTTP traffic between a web application and the Internet. A WAF can help mitigate the risk of exploitation of an SQL injection vulnerability reported on a web application while it is corrected by the development team, as it can detect and block any malicious requests or queries that attempt to inject SQL commands into the web application's database. A WAF can also help protect the web application from other common web-based attacks, such as cross-site scripting (XSS), remote file inclusion (RFI), or denial-of-service (DoS). References: CompTIA Cloud+ Certification Exam Objectives, page 14, section 2.7

NEW QUESTION 5

- (Topic 1)

A SAN that holds VM files is running out of storage space.

Which of the following will BEST increase the amount of effective storage on the SAN?

- A. Enable encryption
- B. Increase IOPS
- C. Convert the SAN from RAID 50 to RAID 60
- D. Configure deduplication

Answer: D

Explanation:

Deduplication is a type of data compression technique that eliminates redundant or duplicate data blocks or segments in a storage system or device. Configuring deduplication can help increase the amount of effective storage on a SAN that holds VM files and is running out of storage space, as it can reduce the storage space consumption and increase the storage space utilization by storing only unique data blocks or segments. Configuring deduplication can also improve performance and efficiency, as it can speed up data transfer and backup processes and save network bandwidth and power consumption. References: CompTIA Cloud+ Certification Exam Objectives, page 9, section 1.4

NEW QUESTION 6

- (Topic 1)

After analyzing a web server's logs, a systems administrator sees that users are connecting to the company's application through HTTP instead of HTTPS. The administrator then configures a redirect from HTTP to HTTPS on the web server, and the application responds with a connection time-out message. Which of the following should the administrator verify NEXT?

- A. The TLS certificate
- B. The firewall rules
- C. The concurrent connection limit
- D. The folder permissions

Answer: B

Explanation:

The firewall rules are the set of policies that define which traffic is allowed or denied between different network segments or devices. The firewall rules can affect the redirect from HTTP to HTTPS on the web server, as they can block or allow traffic based on ports and protocols. If the firewall rules are not configured properly to allow HTTPS traffic on port 443, the application may respond with a connection time-out message. The administrator should verify the firewall rules next to ensure that HTTPS traffic is permitted between the web server and its clients. References: CompTIA Cloud+ Certification Exam Objectives, page 15, section 2.8

NEW QUESTION 7

- (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 with 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 8

- (Topic 1)

A company wants to implement business continuity, and the cloud solution architect needs to design the correct solution.

Which of the following will provide the data to measure business continuity? (Choose two.)

- A. A service-level agreement
- B. Automation scripts
- C. Playbooks
- D. A network diagram
- E. A backup and restore
- F. A recovery time objective

Answer: AF

Explanation:

A service-level agreement (SLA) is a contract or document that defines the level of service and performance expected from a service provider or vendor. A recovery time objective (RTO) is a metric that specifies the maximum acceptable time for restoring a system or service after a disruption or outage. Both SLA and RTO can provide the data to measure business continuity, as they can indicate the availability, reliability, and recoverability of a system or service in case of a failure or disaster. SLA and RTO can also help evaluate the effectiveness and efficiency of the business continuity plan and solution. References: CompTIA Cloud+ Certification Exam Objectives, page 20, section 4.2

NEW QUESTION 9

- (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 10

- (Topic 1)

A technician is working with an American company that is using cloud services to provide video-based training for its customers. Recently, due to a surge in demand, customers in Europe are experiencing latency. Which of the following services should the technician deploy to eliminate the latency issue?

- A. Auto-scaling
- B. Cloud bursting
- C. A content delivery network
- D. A new cloud provider

Answer: C

Explanation:

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

"A content delivery network (CDN) refers to a geographically distributed group of servers which work together to provide fast delivery of Internet content."

NEW QUESTION 10

- (Topic 1)

A company wants to check its infrastructure and application for security issues regularly. Which of the following should the company implement?

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

Answer: C

Explanation:

Vulnerability testing is a type of testing that identifies and evaluates the weaknesses or flaws in a system or application that could be exploited by attackers.

Vulnerability testing can help check the infrastructure and application for security issues regularly, as it can reveal the potential risks and exposures that may compromise the confidentiality, integrity, or availability of the system or application. Vulnerability testing can also help remediate or mitigate the vulnerabilities by providing recommendations or solutions to fix or reduce them. References: CompTIA Cloud+ Certification Exam Objectives, page 19, section 4.1

Reference: <https://pure.security/services/technical-assurance/external-penetration-testing/>

NEW QUESTION 12

- (Topic 1)

A systems administrator is troubleshooting performance issues with a Windows VDI environment. Users have reported that VDI performance has been slow since the images were upgraded from Windows 7 to Windows 10.

This VDI environment is used to run simple tasks, such as Microsoft Office. The administrator investigates the virtual machines and finds the following settings:

? 4 vCPU

? 16GB RAM

? 10Gb networking

? 256MB frame buffer

Which of the following MOST likely needs to be upgraded?

- A. vRAM
- B. vCPU
- C. vGPU
- D. vNIC

Answer: C

Explanation:

A virtual graphics processing unit (vGPU) is a type of hardware or software that enables a VM to use the physical GPU resources of the host or server for graphics-intensive tasks. Upgrading the vGPU is most likely to solve the issue of VDI performance being slow since the images were upgraded from Windows 7 to Windows 10, as it can provide more graphics processing power and memory for the VMs. Upgrading the vGPU can also improve the user experience and productivity, as it can enhance the display quality and responsiveness of the VDI environment. References: CompTIA Cloud+ Certification Exam Objectives, page 11, section 1.6

NEW QUESTION 15

- (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 16

- (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 17

- (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 20

- (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 25

- (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 27

- (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 31

- (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 36

- (Topic 2)

A systems administrator has been asked to restore a VM from backup without changing the current VM's operating state. Which of the following restoration methods would BEST fit this scenario?

- A. Alternate location
- B. Rolling
- C. Storage live migration
- D. In-place

Answer: C

Explanation:

Storage live migration is the best restoration method to restore a VM from backup without changing the current VM's operating state. Storage live migration is a process of moving or transferring storage resources or data from one location to another without affecting or interrupting the operation or performance of the VMs that use them. Storage live migration can help to restore a VM from backup by copying the backup data to a new storage location and switching the VM's storage configuration to point to the new location, without requiring any downtime or reboot.

NEW QUESTION 39

- (Topic 2)

A company is currently running a website on site. However, because of a business requirement to reduce current RTO from 12 hours to one hour, and the RPO

from one day to eight hours, the company is considering operating in a hybrid environment. The website uses mostly static files and a small relational database. Which of the following should the cloud architect implement to achieve the objective at the LOWEST cost possible?

- A. Implement a load-balanced environment in the cloud that is equivalent to the current on- premises setup and use DNS to shift the load from on premises to cloud.
- B. Implement backups to cloud storage and infrastructure as code to provision the environment automatically when the on-premises site is down.
- C. Restore the data from the backups.
- D. Implement a website replica in the cloud with auto-scaling using the smallest possible footprint.
- E. Use DNS to shift the load from on premises to the cloud.
- F. Implement a CDN that caches all requests with a higher TTL and deploy the IaaS instances manually in case of disaster.
- G. Upload the backup on demand to the cloud to restore on the new instances.

Answer: C

Explanation:

This is the best solution to achieve the objective of reducing current RTO (Recovery Time Objective) from 12 hours to one hour, and RPO (Recovery Point Objective) from one day to eight hours, at the lowest cost possible, for a website that uses mostly static files and a small relational database. RTO is a metric that measures how quickly a system or service can be restored after a disruption or disaster. 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. To reduce RTO and RPO, the administrator should implement a website replica in the cloud with auto-scaling using the smallest possible footprint. A website replica is a copy or backup of a website that can be used for recovery or failover purposes. Auto-scaling is a feature that allows cloud resources or systems to adjust their capacity and performance according to demand or workload. Using auto-scaling with the smallest possible footprint can minimize costs by using only the necessary resources and scaling up or down as needed. The administrator should also use DNS (Domain Name System) to shift the load from on premises to the cloud. DNS is a service that translates domain names into IP addresses and vice versa. Using DNS, the administrator can redirect traffic from the on-premises website to the cloud replica in case of a disruption or disaster, and vice versa when recovery is complete.

NEW QUESTION 41

- (Topic 2)

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

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

Answer: B

Explanation:

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

NEW QUESTION 42

- (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 45

- (Topic 2)

A systems administrator has finished installing monthly updates to servers in a cloud environment. The administrator notices certain portions of the playbooks are no longer functioning. Executing the playbook commands manually on a server does not work as well. There are no other reports of issues. Which of the following is the MOST likely cause of this issue?

- A. Change management failure
- B. Service overload
- C. Patching failure
- D. Job validation issues
- E. Deprecated features

Answer: E

Explanation:

Deprecated features are features that are no longer supported or recommended by the software vendor or provider. They may be removed or replaced by newer features in future updates or versions. If a playbook relies on deprecated features, it may stop functioning after an update or patch is applied to the software. The administrator should check the release notes or documentation of the software to identify and replace any deprecated features in the playbook.

NEW QUESTION 47

- (Topic 2)

A cloud administrator is upgrading a cloud environment and needs to update the automation script to use a new feature from the cloud provider. After executing the script, the deployment fails. Which of the following is the MOST likely cause?

- A. API incompatibility
- B. Location changes
- C. Account permissions
- D. Network failure

Answer: A

Explanation:

API incompatibility is the most likely cause of the failure of an automation script to use a new feature from the cloud provider. API (Application Programming Interface) is a set of rules or specifications that defines how different software components or systems can communicate and interact with each other. API incompatibility is a situation where an API does not work or function properly with another software component or system due to differences or changes in versions, formats, parameters, etc. API incompatibility can cause errors or issues when using an automation script to deploy or configure cloud resources or services, especially if the script is not updated or modified according to the new API specifications.

NEW QUESTION 52

- (Topic 2)

A systems administrator is trying to establish an RDP session from a desktop to a server in the cloud. However, the connection appears to be refused even though the VM is responding to ICMP echo requests. Which of the following should the administrator check FIRST?

- A. The firewall
- B. The subnet
- C. The gateway
- D. The services

Answer: A

Explanation:

The firewall is the first thing that the administrator should check if an RDP (Remote Desktop Protocol) session from a desktop to a server in the cloud is refused even though the VM is responding to ICMP echo requests. A firewall is a device or software that controls the incoming and outgoing network traffic based on predefined rules or policies. A firewall may block RDP connections by default or require specific ports or rules to be opened or configured.

NEW QUESTION 53

- (Topic 2)

A disaster situation has occurred, and the entire team needs to be informed about the situation. Which of the following documents will help the administrator find the details of the relevant team members for escalation?

- A. Chain of custody
- B. Root cause analysis
- C. Playbook
- D. Call tree

Answer: D

Explanation:

A call tree is what will help the administrator find the details of the relevant team members for escalation after a disaster situation has occurred and the entire team needs to be informed about the situation. A call tree is a document or diagram that shows the hierarchy or sequence of communication or notification among team members in case of an emergency or incident, such as a disaster situation. A call tree can help to find the details of the relevant team members for escalation by providing information such as:

? Name: This indicates who is involved in the communication or notification process, such as team members, managers, stakeholders, etc.

? Role: This indicates what is their function or responsibility in the communication or notification process, such as initiator, receiver, sender, etc.

? Contact: This indicates how they can be reached or contacted in the communication or notification process, such as phone number, email address, etc.

NEW QUESTION 56

- (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 59

- (Topic 2)

A systems administrator is creating a VM and wants to ensure disk space is not allocated to the VM until it is needed. Which of the following techniques should the administrator use to ensure?

- A. Deduplication
- B. Thin provisioning
- C. Software-defined storage
- D. iSCSI storage

Answer: B

Explanation:

Thin provisioning is the technique that ensures disk space is not allocated to the VM until it is needed. Thin provisioning is a storage allocation method that assigns disk space to a VM on demand, rather than in advance. Thin provisioning can improve storage utilization and efficiency by avoiding overprovisioning and wasting disk space. Thin provisioning can also allow for more flexibility and scalability of storage resources.

NEW QUESTION 63

- (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 64

- (Topic 2)

A system administrator supports an application in the cloud, which includes a restful API that receives an encrypted message that is passed to a calculator system. The administrator needs to ensure the proper function of the API using a new automation tool. Which of the following techniques would be BEST for the administrator to use to accomplish this requirement?

- A. Functional testing
- B. Performance testing
- C. Integration testing
- D. Unit testing

Answer: C

Explanation:

Integration testing is the best technique to use to ensure the proper function of an API that receives an encrypted message that is passed to a calculator system. Integration testing is a type of testing that verifies and validates the functionality, performance, and reliability of different components or modules of a system or application when they are combined or integrated together. Integration testing can help to ensure the API can communicate and interact with the calculator system correctly and securely, as well as identify any errors or issues that may arise from the integration.

NEW QUESTION 69

- (Topic 2)

A systems administrator is deploying a VM and would like to minimize storage utilization by ensuring the VM uses only the storage if needs. Which of the following will BEST achieve this goal?

- A. Compression
- B. Deduplication
- C. RAID
- D. Thin provisioning

Answer: D

Explanation:

Reference: https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.vm_admin.doc/GUID-4C0F4D73-82F2-4B81-8AA7-1DD752A8A5AC.html
Thin provisioning is the technique that will minimize storage utilization by ensuring the VM uses only the storage it needs. Thin provisioning is a storage allocation method that assigns disk space to a VM on demand, rather than in advance. Thin provisioning can improve storage utilization and efficiency by avoiding overprovisioning and wasting disk space. Thin provisioning can also allow for more flexibility and scalability of storage resources.

NEW QUESTION 70

- (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 72

- (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 76

- (Topic 2)

An administrator recently provisioned a file server in the cloud. Based on financial considerations, the administrator has a limited amount of disk space. Which of the following will help control the amount of space that is being used?

- A. Thick provisioning
- B. Software-defined storage
- C. User quotas
- D. Network file system

Answer: C

Explanation:

User quotas are what will help control the amount of space that is being used by a file server in the cloud that has a limited amount of disk space due to financial considerations. User quotas are the limits or restrictions that are imposed on the amount of space that each user can use or consume on a file server or storage device. User quotas can help to control the amount of space that is being used by:

? Preventing or reducing wastage or overuse of space by users who may store unnecessary or redundant files or data on the file server or storage device.

? Ensuring fair and equal distribution or allocation of space among users who may have different needs or demands for space on the file server or storage device.

? Monitoring and managing the usage or consumption of space by users who may need to be notified or alerted when they reach or exceed their quota on the file server or storage device.

NEW QUESTION 79

- (Topic 2)

Users of a public website that is hosted on a cloud platform are receiving a message indicating the connection is not secure when landing on the website. The administrator has found that only a single protocol is opened to the service and accessed through the URL <https://www.comptiasite.com>. Which of the following would MOST likely resolve the issue?

- A. Renewing the expired certificate
- B. Updating the web-server software
- C. Changing the crypto settings on the web server
- D. Upgrading the users' browser to the latest version

Answer: A

Explanation:

Renewing the expired certificate is what would most likely resolve the issue of users receiving a message indicating the connection is not secure when landing on

a website that is hosted on a cloud platform and accessed through <https://www.comptiasite.com>. A certificate is a digital document that contains information such as identity, public key, expiration date, etc., that can be used to prove one's identity and establish secure communication over a network. A certificate can expire when it reaches its validity period and needs to be renewed or replaced. An expired certificate can cause users to receive a message indicating the connection is not secure by indicating that the website's identity or security cannot be verified or trusted. Renewing the expired certificate can resolve the issue by extending its validity period and restoring its identity or security verification or trust.

NEW QUESTION 84

- (Topic 2)

A cloud engineer is responsible for managing a public cloud environment. There is currently one virtual network that is used to host the servers in the cloud environment. The environment is rapidly growing, and the network does not have any more available IP addresses. Which of the following should the engineer do to accommodate additional servers in this environment?

- A. Create a VPC and peer the networks.
- B. Implement dynamic routing.
- C. Enable DHCP on the networks.
- D. Obtain a new IPAM subscription.

Answer: A

Explanation:

Creating a VPC (Virtual Private Cloud) and peering the networks is the best option to accommodate additional servers in a public cloud environment that has run out of IP addresses. A VPC is a logically isolated section of a cloud provider's network that allows customers to launch and configure their own virtual network resources. Peering is a process of connecting two VPCs together so that they can communicate with each other as if they were in the same network.

NEW QUESTION 85

- (Topic 2)

A cloud administrator set up a link between the private and public cloud through a VPN tunnel. As part of the migration, a large set of files will be copied. Which of the following network ports are required from a security perspective?

- A. 22, 53, 445
- B. 22, 443, 445
- C. 25, 123, 443
- D. 137, 139, 445

Answer: B

Explanation:

These are the network ports that are required from a security perspective to copy a large set of files between the private and public cloud through a VPN tunnel. A VPN (Virtual Private Network) tunnel is a secure and encrypted connection that allows data to be transferred between two networks or locations over the public internet. To copy files between the private and public cloud, the following ports are needed:

? Port 22: This is the port used by SSH (Secure Shell) protocol, which is a method of remotely accessing and managing cloud resources or systems using a command-line interface. SSH can also be used to securely transfer files using SCP (Secure Copy Protocol) or SFTP (SSH File Transfer Protocol).

? Port 443: This is the port used by HTTPS (Hypertext Transfer Protocol Secure), which is a protocol that encrypts and secures web traffic. HTTPS can also be used to transfer files using web browsers or tools such as curl or wget.

? Port 445: This is the port used by SMB (Server Message Block) protocol, which is a protocol that allows file sharing and access over a network. SMB can also be used to transfer files using tools such as robocopy or rsync.

NEW QUESTION 90

- (Topic 1)

Company A has acquired Company B and is in the process of integrating their cloud resources. Company B needs access to Company A's cloud resources while retaining its IAM solution.

Which of the following should be implemented?

- A. Multifactor authentication
- B. Single sign-on
- C. Identity federation
- D. Directory service

Answer: C

Explanation:

Identity 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. Identity federation can help integrate the cloud resources of Company A and Company B after Company A has acquired Company B, as it can enable seamless and secure access to both companies' cloud resources using the same IAM solution. Identity federation 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

Reference: <https://medium.com/@dinika.15/identity-federation-a-brief-introduction-f2f823f8795a>

NEW QUESTION 93

- (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 96

- (Topic 1)

A cloud architect is designing the VPCs for a new hybrid cloud deployment. The business requires the following:

? High availability

? Horizontal auto-scaling

? 60 nodes peak capacity per region

? Five reserved network IP addresses per subnet

? /24 range

Which of the following would BEST meet the above requirements?

A. Create two /25 subnets in different regions

B. Create three /25 subnets in different regions

C. Create two /26 subnets in different regions

D. Create three /26 subnets in different regions

E. Create two /27 subnets in different regions

F. Create three /27 subnets in different regions

Answer: C

Explanation:

A /26 subnet is a subnet that has a network prefix of 26 bits and a host prefix of 6 bits. A /26 subnet can support up to 64 hosts (62 usable hosts) and has a subnet mask of 255.255.255.192. Creating two /26 subnets in different regions can best meet the business requirements for deploying a high availability, horizontally auto-scaling solution that has a peak capacity of 60 nodes per region and five reserved network IP addresses per subnet. Creating two /26 subnets can provide enough host addresses for the peak capacity and the reserved addresses, as well as allow for some growth or redundancy. Creating the subnets in different regions can provide high availability and horizontal auto-scaling, as it can distribute the workload across multiple locations and scale out or in based on demand. References: CompTIA Cloud+ Certification Exam Objectives, page 15, section 2.8

NEW QUESTION 99

- (Topic 1)

A storage array that is used exclusively for datastores is being decommissioned, and a new array has been installed. Now the private cloud administrator needs to migrate the data.

Which of the following migration methods would be the BEST to use?

A. Conduct a V2V migration

B. Perform a storage live migration

C. Rsync the data between arrays

D. Use a storage vendor migration appliance

Answer: B

Explanation:

A storage live migration is a process of moving or transferring data or files from one storage system or device to another without interrupting or affecting the availability or performance of the VMs or applications that use them. Performing a storage live migration can help migrate the data from a SAN that is being decommissioned to a new array, as it can ensure that there is no downtime or disruption for the VMs or applications that rely on the data or files stored on the SAN. Performing a storage live migration can also help maintain consistency and integrity, as it can synchronize and verify the data or files between the source and destination storage systems or devices.

References: CompTIA Cloud+ Certification Exam Objectives, page 10, section 1.5

NEW QUESTION 100

- (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 104

- (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 109

- (Topic 1)

A systems administrator would like to reduce the network delay between two servers. Which of the following will reduce the network delay without taxing other system resources?

- A. Decrease the MTU size on both servers
- B. Adjust the CPU resources on both servers
- C. Enable compression between the servers
- D. Configure a VPN tunnel between the servers

Answer: A

Explanation:

The maximum transmission unit (MTU) is the largest size of a packet or frame that can be sent over a network. Decreasing the MTU size on both servers can reduce the network delay between them, as it can reduce the fragmentation and reassembly of packets, improve the transmission efficiency, and avoid packet loss or errors. Decreasing the MTU size can also avoid taxing other system resources, as it does not require additional CPU, memory, or disk resources. References: CompTIA Cloud+ Certification Exam Objectives, page 16, section 3.2
Reference: <https://cseweb.ucsd.edu/~calder/papers/HPDC-01-DynComp.pdf>

NEW QUESTION 113

- (Topic 1)

A cloud administrator has finished setting up an application that will use RDP to connect. During testing, users experience a connection timeout error. Which of the following will MOST likely solve the issue?

- A. Checking user passwords
- B. Configuring QoS rules
- C. Enforcing TLS authentication
- D. Opening TCP port 3389

Answer: D

Explanation:

TCP port 3389 is the default port used by Remote Desktop Protocol (RDP) to connect to a remote system or application over a network. Opening TCP port 3389 on the firewall or network device will most likely solve the issue of users experiencing a connection timeout error when trying to use RDP to connect to an application, as it will allow RDP traffic to pass through. If TCP port 3389 is closed or blocked, RDP traffic will be denied or dropped, resulting in a connection timeout error. References: CompTIA Cloud+ Certification Exam Objectives, page 15, section 2.8
Reference: <https://docs.microsoft.com/en-us/windows-server/remote/remote-desktop-services/troubleshoot/rdp-error-general-troubleshooting>

NEW QUESTION 114

- (Topic 1)

A systems administrator in a large enterprise needs to alter the configuration of one of the finance department's database servers. Which of the following should the administrator perform FIRST?

- A. Capacity planning
- B. Change management
- C. Backups
- D. Patching

Answer: B

Explanation:

The SA would do the other three regardless of the need to alter configurations. In this situation, the SA would have to present the change to the CCB in order to do the alteration.

There is no clarification on whether the change management process has been gone through. Any changes, regardless of how small or big, must go through the change management process. This allows proposals to be heard by end-users, management, and possibly stockholders. From there, it will be reviewed and either approved or denied, with reasons specified. From there, the administrator(s) can do whatever processes are necessary.

Change management is a process or procedure that defines the steps, roles, and responsibilities for implementing, documenting, and communicating any changes or updates to a system or service. Change management can help ensure that any changes or updates are done in a controlled and consistent manner, minimizing any risks or impacts to the system or service. Performing change management is the first thing that a systems administrator should do before altering the

configuration of one of the finance department's database servers, as it can ensure that the change request is approved, authorized, tested, and verified before applying it to the database server. References: CompTIA Cloud+ Certification Exam Objectives, page 13, section 2.5

NEW QUESTION 118

- (Topic 1)

A SaaS provider wants to maintain maximum availability for its service. Which of the following should be implemented to attain the maximum SLA?

- A. A hot site
- B. An active-active site
- C. A warm site
- D. A cold site

Answer: B

Explanation:

An active-active site is a type of disaster recovery (DR) site that runs simultaneously with the primary site and handles part of the normal workload or traffic. An active-active site can help maintain maximum availability for a SaaS service, as it can provide load balancing, redundancy, and failover capabilities for the SaaS service in case of an outage or disruption at the primary site. An active-active site can also improve performance and scalability, as it can distribute the workload or traffic across multiple sites and handle increased demand or peak periods. References: CompTIA Cloud+ Certification Exam Objectives, page 10, section 1.5

NEW QUESTION 122

- (Topic 1)

A systems administrator for an e-commerce company will be migrating the company's main website to a cloud provider. The principal requirement is that the website must be highly available. Which of the following will BEST address this requirement?

- A. Vertical scaling
- B. A server cluster
- C. Redundant switches
- D. A next-generation firewall

Answer: B

Explanation:

A server cluster is a group of servers that work together to provide high availability, load balancing, and scalability for applications or services. A server cluster can help ensure the high availability requirement for migrating an e-commerce company's main website to a cloud provider, as it can prevent downtime or disruption in case of a server failure or outage by automatically switching the workload to another server in the cluster. A server cluster can also improve performance and reliability, as it can distribute the workload across multiple servers and handle increased traffic or demand. References: CompTIA Cloud+ Certification Exam Objectives, page 10, section 1.5

NEW QUESTION 124

- (Topic 1)

A marketing team is using a SaaS-based service to send emails to large groups of potential customers. The internally managed CRM system is configured to generate a list of target customers automatically on a weekly basis, and then use that list to send emails to each customer as part of a marketing campaign. Last week, the first email campaign sent emails successfully to 3,000 potential customers. This week, the email campaign attempted to send out 50,000 emails, but only 10,000 were sent.

Which of the following is the MOST likely reason for not sending all the emails?

- A. API request limit
- B. Incorrect billing account
- C. Misconfigured auto-scaling
- D. Bandwidth limitation

Answer: A

Explanation:

An API request limit 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 request limits are often used by SaaS-based services to control the usage and traffic of their customers and prevent overloading or abuse of their resources. An API request limit can cause a failure to send all the emails if the marketing team exceeds the number of requests allowed by the SaaS-based service in a week. The service may reject or block any requests that go beyond the limit, resulting in fewer emails being sent than expected. References: CompTIA Cloud+ Certification Exam Objectives, page 13, section 2.5

Reference: <https://developers.google.com/analytics/devguides/config/mgmt/v3/limits-quotas>

NEW QUESTION 126

- (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 129

- (Topic 1)

An organization is required to set a custom registry key on the guest operating system. Which of the following should the organization implement to facilitate this requirement?

- A. A configuration management solution
- B. A log and event monitoring solution
- C. A file integrity check solution
- D. An operating system ACL

Answer: A

Explanation:

A configuration management solution is a type of tool or system that automates and standardizes the configuration and deployment of cloud resources or services according to predefined policies or rules. A configuration management solution can help set a custom registry key on the guest operating system in an IaaS instance, as it can apply the desired registry setting to one or more virtual machines (VMs) without manual intervention or scripting. A configuration management solution can also help maintain consistency, compliance, and security of cloud configurations by monitoring and enforcing the desired state. References: CompTIA Cloud+ Certification Exam Objectives, page 13, section 2.5

NEW QUESTION 131

- (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 134

- (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 138

- (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 139

- (Topic 4)

A systems administrator is reviewing the logs from a company's IDS and notices a large amount of outgoing traffic from a particular server. The administrator then runs a scan on the server, which detects malware that cannot be removed. Which of the following should the administrator do first?

- A. Determine the root cause.
- B. Disconnect the server from the network.
- C. Perform a more intrusive scan.
- D. Restore the server from a backup.

Answer: B

Explanation:

The first step in any incident response procedure is to contain the incident and prevent it from spreading or causing more damage. In this scenario, the systems administrator is reviewing the logs from a company's IDS and notices a large amount of outgoing traffic from a particular server. The administrator then runs a scan on the server, which detects malware that cannot be removed. This indicates that the server is compromised and may be sending malicious or sensitive data to an external source. Therefore, the best thing to do first is to disconnect the server from the network, which will isolate it from the rest of the system and stop the data exfiltration. Determining the root cause, performing a more intrusive scan, and restoring the server from a backup are all important steps, but they should be done after the server is disconnected from the network. References: CompTIA Cloud+ CV0-003 Certification Study Guide, Chapter 10, Incident Response Procedures, page 1771.

NEW QUESTION 141

- (Topic 4)

A company is concerned it will run out of VLANs on its private cloud platform in the next couple months, and the product currently offered to customers requires the company to allocate three dedicated, segmented tiers. Which of the following can the company implement to continue adding new customers and to maintain the required level of isolation from other tenants?

- A. GRE
- B. SR-IOV
- C. VXLAN
- D. IPSec

Answer: C

Explanation:

One possible solution for the company to continue adding new customers and to maintain the required level of isolation from other tenants is to implement VXLAN. VXLAN is a network virtualization technology that can extend VLAN by adding a 24-bit segment ID, which allows up to 16 million unique virtual segments. VXLAN can encapsulate layer 2 Ethernet frames within layer 3 IP packets, and tunnel them across the underlying network. VXLAN can provide logical isolation and security for different tenants, as well as scalability and flexibility for large cloud computing environments¹.

NEW QUESTION 144

- (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 148

- (Topic 4)

A cloud administrator is having difficulty correlating logs for multiple servers. Upon inspection, the administrator finds that the time-zone settings are mismatched throughout the deployment. Which of the following solutions can help maintain time synchronization between all the resources?

- A. DNS
- B. IPAM
- C. NTP
- D. SNMP

Answer: C

Explanation:

The correct answer is C. NTP.

NTP stands for Network Time Protocol, which is a standard protocol for synchronizing the clocks of computers over a network. NTP uses a hierarchical, client-server architecture, where a client requests the current time from a server, and the server responds with a timestamp. The client then adjusts its own clock to match the server's time, taking into account the network delay and clock drift. NTP can achieve sub-millisecond accuracy over local area networks and a few milliseconds over the internet¹².

NTP can help maintain time synchronization between all the resources in a distributed cloud environment, as it allows each resource to get the accurate time from a reliable source. This can help with correlating logs, auditing, security, and other time-sensitive operations. NTP can also handle different time zones, as it uses Coordinated Universal Time (UTC) as the reference time, and each resource can convert UTC to its local time zone¹².

DNS stands for Domain Name System, which is a protocol for resolving domain names into IP addresses. DNS does not provide any functionality for time synchronization³.

IPAM stands for IP Address Management, which is a method for planning, tracking, and managing the IP address space used in a network. IPAM does not provide any functionality for time synchronization.

SNMP stands for Simple Network Management Protocol, which is a protocol for collecting and organizing information about managed devices on a network. SNMP can be used to monitor the performance, availability, configuration, and security of network devices, but it does not provide any functionality for time synchronization.

NEW QUESTION 152

- (Topic 4)

A company has a web application running in an on-premises environment that needs to be migrated to the cloud. The company wants to implement a solution that maximizes scalability, availability, and security, while requiring no infrastructure administration. Which of the following services would be BEST to meet this goal?

- A. A PaaS solution
- B. A hybrid solution
- C. An IaaS solution
- D. A SaaS solution

Answer: A

Explanation:

A PaaS solution, or platform as a service, is a cloud computing service that provides a complete, ready-to-use, cloud-hosted platform for developing, running, maintaining and managing applications¹. A PaaS solution would meet the company's goal of maximizing scalability, availability, and security, while requiring no infrastructure administration, because:

Scalability: A PaaS solution can automatically scale up or down the resources needed to run the application based on the demand and traffic. The company does not need to worry about provisioning or managing servers, storage, network, or load balancers²³.

Availability: A PaaS solution can ensure high availability and reliability of the application by replicating it across multiple regions and zones. The company does not need to worry about backup, recovery, or failover²³.

Security: A PaaS solution can provide built-in security features such as encryption, authentication, authorization, and firewall. The company does not need to worry about installing or updating security patches or software²³.

No infrastructure administration: A PaaS solution can abstract away the underlying infrastructure and hardware from the company. The company only needs to focus on developing and deploying the application code and data. The PaaS provider takes care of the rest²³.

A hybrid solution (B) is a cloud computing service that combines on-premises and cloud resources. It may offer some benefits such as flexibility and cost optimization, but it would not meet the company's goal of requiring no infrastructure administration. The company would still need to manage and maintain the on-premises part of the solution⁴.

An IaaS solution ©, or infrastructure as a service, is a

NEW QUESTION 157

- (Topic 4)

A systems administrator is planning to migrate to a cloud solution with volume-based licensing. Which of the following is most important when considering licensing costs?

- A. The number of cores
- B. The number of threads
- C. The number of machines
- D. The number of sockets

Answer: C

Explanation:

Volume-based licensing is a model where the cost of the software is based on the number of licenses purchased¹. This model is commonly used for software that is installed on a specific number of devices, such as antivirus software or office productivity suites¹. Therefore, the number of machines is the most important factor when considering licensing costs in this model.

References: CompTIA Cloud+ CV0-003 Exam Objectives, Objective 1.2: Given a scenario, compare and contrast various cloud service models ; Cloud+ Exam CV0-003: CompTIA Cloud+ Licensing Models¹

NEW QUESTION 159

- (Topic 4)

Based on the shared responsibility model, which of the following solutions passes the responsibility of patching the OS to the customer?

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

Answer: C

Explanation:

IaaS stands for Infrastructure as a Service, and it is a cloud service model that provides customers with access to virtualized computing resources, such as servers, storage, and networks. In the IaaS model, the customer is responsible for patching the operating system (OS) of the virtual machines, as well as installing and managing the applications and data. The cloud service provider (CSP) is responsible for maintaining the physical infrastructure, such as the hardware, power, cooling, and security. Therefore, IaaS passes the responsibility of patching the OS to the customer, unlike PaaS, DBaaS, or SaaS, where the CSP handles the OS patching and updates. References: CompTIA Cloud+ CV0-003 Certification Study Guide, Chapter 2, Objective 2.1: Given a scenario, deploy cloud services and solutions.

NEW QUESTION 160

- (Topic 4)

A cloud administrator received a request to provision a set of cloud resources in an effort to switch to infrastructure as code to automate and optimize operations. The administrator decides to try to run some tests with the following definition:

```
#Cloud provider
provider "Cloud" {
  cloud_api_key = "${var.cloud_api_key}"
  region       = "us-north"
}

#Resources
resource "key_is_ssh_key" "ssh_public" {
  name      = "testssh"
  public_key = var.ssh_public_key
}

resource "virtual-server" "vml" {
  name      = "vml"
  image     = "${var.image}"
  keys      = [key_is_ssh_key.ssh_public]
}

variable "ssh_public_key" {
  default = "test.pub"
}
```

However, the test fails with the following error:

```
Error: [DEBUG] Create SSH key illegal base64 data at input
```

Which of the following is the most likely cause of the issue?

- A. The cloud provider is expecting the private key.
- B. The incorrect resource name was used.
- C. The environment variable for the public key path has not been set.
- D. An unexpected variable was provided.

Answer: C

Explanation:

The error message indicates that the cloud provider is unable to find the public key file that is specified in the definition. The definition uses an environment variable called PUBLIC_KEY_PATH to refer to the location of the public key file. However, if this environment variable has not been set or exported in the shell, the cloud provider will not be able to resolve it and will fail to provision the resources. To fix this issue, the cloud administrator should set and export the environment variable for the public key path before running the definition. References: [CompTIA Cloud+ CV0-003 Certification Study Guide], Chapter 8, Objective 8.1: Given a scenario, implement cloud automation and orchestration.

NEW QUESTION 163

- (Topic 4)

During a security incident on an IaaS platform, which of the following actions will a systems administrator most likely take as part of the containment procedure?

- A. Connect to an instance for triage.
- B. Add a deny rule to the network ACL.
- C. Mirror the traffic to perform a traffic capture.
- D. Perform a memory acquisition.

Answer: B

Explanation:

A network access control list (ACL) is a set of rules that controls the inbound and outbound traffic for a network interface or a subnet. A deny rule can be used to block or filter the traffic from a specific source or destination, such as an IP address, a port number, or a protocol. By adding a deny rule to the network ACL, a systems administrator can prevent the communication between the compromised instance and the attacker, or between the compromised instance and other instances or servers. This can help to contain the security incident and limit the potential damage or data loss. A deny rule can also be used to isolate the compromised instance for further investigation or remediation. References: CompTIA Cloud+ CV0-003 Study Guide, Chapter 5: Maintaining a Cloud Environment, page 222-223; What is a network access control list (ACL)?.

NEW QUESTION 165

- (Topic 4)

A systems administrator is planning to deploy a database cluster in a virtualization environment. The administrator needs to ensure the database nodes do not exist on the same physical host. Which of the following would best meet this requirement?

- A. Oversubscription
- B. Anti-affinity
- C. A firewall
- D. A separate cluster

Answer: B

Explanation:

Anti-affinity is a rule that specifies that certain virtual machines should not run on the same physical host. This can help to improve availability and performance by avoiding single points of failure and resource contention. For example, if the database nodes are running on the same host and the host fails, the entire database cluster will be unavailable. By using anti-affinity rules, the systems administrator can ensure the database nodes are distributed across different hosts in the virtualization environment. References: CompTIA Cloud+ CV0-003 Study Guide, Chapter 2: Deploying a Cloud Environment, page 76.

NEW QUESTION 170

- (Topic 4)

A systems administrator has a redundant backup system in place. Which of the following should the systems administrator perform to maintain efficient operation and comply with the global standard in the corporate backup policies?

- A. Modify RTO policies.
- B. Confirm completion of the backups.
- C. Test the backups.
- D. Modify RPO policies.

Answer: C

NEW QUESTION 172

- (Topic 4)

Different healthcare organizations have agreed to collaborate and build a cloud infrastructure that should minimize compliance costs and provide a high degree of security and privacy, as per regulatory requirements. This is an example of a:

- A. private cloud.
- B. community cloud.
- C. hybrid cloud.
- D. public cloud.

Answer: B

Explanation:

The correct answer is B. Community cloud.

A community cloud is a cloud deployment model that involves a shared infrastructure among several organizations that have common interests, goals, or requirements. A community cloud can provide a high degree of security, privacy, and compliance, as well as cost savings and efficiency, for the participating

organizations. A community cloud can be managed by one or more of the organizations, or by a third-party service provider .

A private cloud is a cloud deployment model that involves a dedicated infrastructure for a single organization. A private cloud can provide a high degree of control, customization, and security for the organization, but it may also incur higher costs and complexity. A private cloud can be managed by the organization itself, or by a third-party service provider.

A hybrid cloud is a cloud deployment model that involves a combination of two or more different cloud models, such as private, public, or community clouds. A hybrid cloud can provide the benefits of both models, such as scalability, flexibility, and cost-effectiveness, as well as address the challenges of each model, such as security, compliance, and performance. A hybrid cloud can be managed by the organization itself, or by one or more service providers .

A public cloud is a cloud deployment model that involves a shared infrastructure for multiple organizations or individuals. A public cloud can provide a high degree of scalability, accessibility, and affordability for the users, but it may also pose some risks in terms of security, privacy, and compliance. A public cloud is managed by a third-party service provider .

NEW QUESTION 176

- (Topic 4)

A cloud administrator created four VLANs to autoscale the container environment. Two of the VLANs are on premises, while two VLANs are on a public cloud provider with a direct link between them. Firewalls are between the links with an additional subnet for communication, which is 192.168.5.0/24.

The on-premises gateways are:

* 192.168.1.1/24

* 192.168.2.1/24

The cloud gateways are:

* 192.168.3.1/24

* 192.168.4.1/24

The orchestrator is unable to communicate with the cloud subnets. Which Of the following should the administrator do to resolve the issue?

A. Allow firewall traffic to 192.168.5.0/24.

B. Set both firewall interfaces to 192.168.5.1/24.

C. Add interface 192.168.3.1/24 on the local firewall.

D. Add interface 192.168.1.1/24 on the cloud firewall.

Answer: A

Explanation:

To allow communication between the on-premises and cloud subnets, the firewall traffic should be allowed to pass through the additional subnet for communication, which is 192.168.5.0/24. This subnet acts as a bridge between the two networks and should have firewall rules that permit traffic from and to both sides.

References: [CompTIA Cloud+ Study Guide], page 181.

NEW QUESTION 180

- (Topic 4)

An IT professional is selecting the appropriate cloud storage solution for an application that has the following requirements:

· The owner of the objects should be the object writer.

· The storage system must enforce TLS encryption.

Which of the following should the IT professional configure?

A. A bucket

B. A CIFS endpoint

C. A SAN

D. An NFS mount

Answer: A

Explanation:

A bucket is a cloud storage solution that allows users to store and access objects, such as files, images, videos, etc. A bucket is typically associated with object storage services, such as Amazon S3, Google Cloud Storage, or Microsoft Azure Blob Storage¹²³. A bucket has the following characteristics that match the requirements of the application:

? The owner of the objects is the object writer. This means that the user who uploads or writes an object to the bucket becomes the owner of that object and can control its access permissions⁴⁵⁶.

? The storage system enforces TLS encryption. This means that the data in transit between the client and the bucket is encrypted using the Transport Layer Security (TLS) protocol, which provides security and privacy for the communication . A CIFS endpoint, a SAN, and an NFS mount are not cloud storage solutions, but rather network protocols or architectures that enable access to storage devices

NEW QUESTION 182

- (Topic 4)

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

A. per gigabyte

B. per seat

C. Per user

D. Per device

Answer: A

Explanation:

The correct answer is A. per gigabyte.

A cost model for a DBaaS is a way of determining how much the user pays for the database service. Different cost models may have different pricing factors, such as storage usage, data transfer, compute resources, and additional services.

A per gigabyte cost model is best for a cloud solution because it allows the user to pay only for the amount of storage space they use for their database. This way, the user can scale up or down their storage needs as per their requirements and budget. A per gigabyte cost model also reflects the actual cost of the infrastructure, software licenses, and maintenance that the service provider incurs to host and operate the database¹.

A per seat cost model is not suitable for a cloud solution because it charges the user based on the number of seats or licenses they purchase for the database service. This means that the user may end up paying for more seats than they actually use, or not have enough seats to accommodate their users. A per seat cost

model also does not account for the storage usage or performance of the database.

A per user cost model is also not suitable for a cloud solution because it charges the user

based on the number of users who access the database service. This means that the user may have to pay more if they have a large number of users, or less if they have a small number of users. A per user cost model also does not account for the storage usage or performance of the database.

A per device cost model is also not suitable for a cloud solution because it charges the user based on the number of devices that connect to the database service. This means that the user may have to pay more if they have multiple devices per user, or less if they have one device per user. A per device cost model also does not account for the storage usage or performance of the database.

NEW QUESTION 183

- (Topic 4)

A cloud administrator is reviewing the current private cloud and public IaaS environment, and is building an optimization plan. Portability is of great concern for the administrator so resources can be easily moved from one environment to another.

Which of the following should the administrator implement?

- A. Serverless
- B. CDN
- C. Containers
- D. Deduplication

Answer: C

Explanation:

Containers are packages of software that contain all of the necessary elements to run in any environment. Containers virtualize the operating system and run anywhere, from a private data center to the public cloud or even on a developer's personal laptop. Containers provide an isolated environment for running applications, sharing the host OS kernel but isolating processes, file systems, and network resources. Containers package applications and their dependencies together, ensuring they run consistently across different environments, from development to production. Containers are lightweight, resource-efficient, fast, and immutable, making them ideal for portability and scalability. By using containers, a cloud administrator can easily move resources from one environment to another without changing the code or configuration of the applications. References: CompTIA Cloud+ CV0-003 Study Guide, Chapter 2: Deploying a Cloud Environment, page 75-76; What are containers?; Portability in the Cloud: Cloud Native and Containers.

NEW QUESTION 186

- (Topic 4)

A cloud engineer is troubleshooting RSA key-based authentication from a local computer to a cloud-based server, which is running SSH service on a default port.

The following file permissions are set on the authorized keys file:

-rw-rw-rw-1 ubuntu ubuntu 391 Mar 5 01:36 authorized _ keys

Which Of the following security practices are the required actions the engineer Should take to gain access to the server? (Select TWO).

- A. Fix the file permissions with execute permissions to the owner of the file.
- B. Open port 21 access for the computer's public IP address.
- C. Fix the file permissions with read-only access to the owner Of the file.
- D. Open port 22 access for the computer's public IP address.
- E. Open port 21 access for 0.0.0.0/0 CIDR.
- F. open port 22 access for 0.0.0.0/0 CIDR.

Answer: CD

Explanation:

The correct answer is C and D.

* C. Fix the file permissions with read-only access to the owner of the file.

* D. Open port 22 access for the computer's public IP address.

The authorized_keys file on the server should have read-only access for the owner of the file, and no access for anyone else. This ensures that only the owner can read the public keys that are authorized to log in, and no one can modify or delete them. The file permissions can be fixed with the command `chmod 400 ~/.ssh/authorized_keys` on the server. This is a recommended security practice for SSH key-based authentication¹²³. The computer that wants to log in to the server using SSH key-based authentication needs to have access to port 22 on the server, which is the default port for SSH service. This can be done by opening port 22 access for the computer's public IP address on the server's firewall or security group settings. This allows the computer to initiate an SSH connection to the server and authenticate with its private key. Opening port 21, which is used for FTP service, is not relevant or secure for SSH key-based authentication¹.

NEW QUESTION 187

- (Topic 4)

A cloud administrator used a deployment script to recreate a number of servers hosted in a public-cloud provider. However, after the script completes, the administrator receives the following error when attempting to connect to one of the servers Via SSH from the administrators workstation: CHANGED. Which of the following IS the MOST likely cause of the issue?

- A. The DNS records need to be updated
- B. The cloud provider assigned a new IP address to the server.
- C. The fingerprint on the server's RSA key is different
- D. The administrator has not copied the public key to the server.

Answer: C

Explanation:

This error indicates that the SSH client has detected a change in the server's RSA key, which is used to authenticate the server and establish a secure connection. The SSH client stores the fingerprints of the servers it has previously connected to in a file called known_hosts, which is usually located in the ~/.ssh directory. When the SSH client tries to connect to a server, it compares the fingerprint of the server's RSA key with the one stored in the known_hosts file. If they match, the connection proceeds. If they do not match, the SSH client warns the user of a possible man-in-the-middle attack or a host key change, and aborts the connection.

The most likely cause of this error is that the deployment script has recreated the server with a new RSA key, which does not match the one stored in the known_hosts file. This can happen when a server is reinstalled, cloned, or migrated. To resolve this error, the administrator needs to remove or update the old fingerprint from the known_hosts file, and accept the new fingerprint when connecting to the server again. Alternatively, the administrator can use a tool or service that can synchronize or manage the RSA keys

across multiple servers, such as AWS Key Management Service (AWS KMS) 1, Azure Key Vault 2, or HashiCorp Vault 3.

NEW QUESTION 191

- (Topic 4)

A DevOps team needs to provide a solution that offers isolation, portability, and scalability. Which of the following would BEST meet these requirements?

- A. Virtual machines
- B. Containers
- C. Appliances
- D. Clusters

Answer: B

Explanation:

Containers are a solution that offers isolation, portability, and scalability for software development and deployment. Containers are lightweight and self-contained units of software that package up the application code and all its dependencies, such as libraries, frameworks, and configuration files. Containers run on a container platform, such as Docker or Kubernetes, that provides the runtime environment and orchestration for the containers.

Containers offer isolation, as they run independently from each other and from the underlying host system. Each container has its own namespace, filesystem, network, and resources, and does not interfere with other containers or processes. Containers also offer portability, as they can run on any system that supports the container platform, regardless of the hardware or operating system differences. Containers can be easily moved, copied, or deployed across different environments, such as development, testing, or production. Containers also offer scalability, as they can be dynamically created, destroyed, or replicated to meet the changing demand for the application. Containers can also leverage the distributed computing power of clusters, which are groups of servers that work together to provide high availability and performance.

NEW QUESTION 194

- (Topic 4)

A systems administrator needs to implement a way for users to verify software integrity. Which of the following tools would BEST meet the administrator's needs?

- A. TLS 1.3
- B. CRC32
- C. AES-256
- D. SHA-512

Answer: D

Explanation:

SHA-512 is a tool that can generate a cryptographic hash value for any given data. A cryptographic hash value is a fixed-length string of bits that uniquely and irreversibly represents the data. SHA-512 is one of the variants of the Secure Hash Algorithm 2 (SHA-2) family, which is a widely used and standardized hash function.

SHA-512 can help users to verify software integrity by comparing the hash values of the software before and after downloading, installing, or transferring. If the hash values match, it means that the software has not been altered, corrupted, or tampered with. If the hash values differ, it means that the software may have been compromised, infected, or damaged.

NEW QUESTION 199

- (Topic 4)

A Cloud administrator needs to reduce storage costs. Which of the following would BEST help the administrator reach that goal?

- A. Enabling compression
- B. Implementing deduplication
- C. Using containers
- D. Rightsizing the VMS

Answer: B

Explanation:

The correct answer is B. Implementing deduplication would best help the administrator reduce storage costs.

Deduplication is a technique that eliminates redundant copies of data and stores only one unique instance of the data. This can reduce the amount of storage space required and lower the storage costs. Deduplication can be applied at different levels, such as file-level, block-level, or object-level. Deduplication can also improve the performance and efficiency of backup and recovery operations.

Enabling compression is another technique that can reduce storage costs, but it may not be as effective as deduplication, depending on the type and amount of data. Compression reduces the size of data by applying algorithms that remove or replace redundant or unnecessary bits. Compression can also affect the quality and accessibility of the data, depending on the compression ratio and method.

Using containers and rightsizing the VMs are techniques that can reduce compute costs, but not necessarily storage costs. Containers are lightweight and portable units of software that run on a shared operating system and include only the necessary dependencies and libraries. Containers can reduce the overhead and resource consumption of virtual machines (VMs), which require a full operating system for each instance. Rightsizing the VMs means adjusting the CPU, memory, disk, and network resources of the VMs to match their workload requirements. Rightsizing the VMs can optimize their performance and utilization, and avoid overprovisioning or underprovisioning.

NEW QUESTION 201

- (Topic 4)

A systems administrator notices several VMS are constantly ballooning, while the memory usage of several other VMS is significantly lower than their resource allocation. Which of the following will MOST likely solve the issue?

- A. Rightsizing
- B. Bandwidth increase
- C. Cluster placement
- D. Storage tiers

Answer: A

Explanation:

The best answer is A. Rightsizing.

Rightsizing is the process of restructuring a company so it can make a profit more efficiently and meet updated business objectives¹. Organizations will usually rightsize their business by reducing their workforce, reorganizing upper management, cutting costs, and changing job roles².

Rightsizing can help solve the issue of VMs constantly ballooning, while the memory usage of several other VMs is significantly lower than their resource allocation. Ballooning is a memory reclamation technique used when ESXi host runs out of memory. It involves a balloon driver that consumes unused memory within the VM's address space and makes it available for other uses by the host machine³. However, ballooning can also degrade the performance of the VMs and cause swapping or paging⁴.

By rightsizing the VMs, the systems administrator can adjust the memory allocation according to the actual demand and usage of each VM. This can prevent overprovisioning or underprovisioning of memory resources and improve the efficiency and profitability of the company. Rightsizing can also help avoid redundancies, streamline workflows, and make better hiring decisions¹.

NEW QUESTION 202

- (Topic 4)

A systems administrator is implementing a new version of a company's primary human- resources application. An upgrade will be performed on the production server, as there is no development environment. The administrator needs to have a plan in case something goes wrong with the upgrade. Which of the following will work best to ensure a quick rollback in case an issue arises?

- A. An application-level backup
- B. A production snapshot
- C. A full backup
- D. A differential backup

Answer: B

Explanation:

A production snapshot is a point-in-time copy of the state and data of a production server or instance. It can be used to restore the server or instance to the exact state it was in when the snapshot was taken, in case of a failure, error, or corruption. A production snapshot can help to ensure a quick rollback in case an issue arises during an application upgrade, as it can revert the changes made by the upgrade and restore the previous version of the application. A production snapshot can also preserve the configuration and settings of the server or instance, as well as the application data and dependencies. A production snapshot is different from a backup, which is a copy of the data only, and may not include the state or configuration of the server or instance. References: CompTIA Cloud+ CV0-003 Study Guide, Chapter 2: Deploying a Cloud Environment, page 75-76; Snapshots vs Backups: Key Differences and Similarities.

NEW QUESTION 203

- (Topic 4)

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

- A. Scaling of the environment after work hours
- B. Implementing access control after work hours
- C. Shutting down the environment after work hours
- D. Blocking external access to the environment after work hours

Answer: C

Explanation:

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

NEW QUESTION 208

- (Topic 4)

A systems administrator is performing an OS upgrade on a production VM. Which of the following actions should the administrator take before the upgrade to ensure the FASTEST recovery of the system in case the upgrade fails in an unrecoverable way?

- A. Submit the upgrade to the CAB.
- B. Perform a full backup.
- C. Take a snapshot of the system.
- D. Test the upgrade in a preproduction environment.

Answer: C

Explanation:

A snapshot is an image of your system/volume at a specific point in time. It captures the entire file system as it was when the snapshot was taken. When a snapshot is used to restore the system, the system will revert to exactly how it was at the time of the snapshot¹. Snapshots are designed for short-term storage and fast recovery. They do not need a lot of storage space or time to create copies²³⁴.

Taking a snapshot of the system before the OS upgrade would ensure the fastest recovery of the system in case the upgrade fails in an unrecoverable way. The administrator could simply restore the system from the snapshot and avoid any data loss or corruption. This would be much faster and easier than performing a full backup or testing the upgrade in a preproduction environment.

NEW QUESTION 212

- (Topic 4)

A cloud engineer recently used a deployment script template to implement changes on a cloud-hosted web application. The web application communicates with a managed database on the back end. The engineer later notices the web application is no longer receiving data from the managed database. Which of the following is the most likely cause of the issue?

- A. Misconfiguration in the user permissions
- B. Misconfiguration in the routing traffic

- C. Misconfiguration in the network ACL
- D. Misconfiguration in the firewall

Answer: D

Explanation:

A misconfiguration in the firewall can block the communication between the web application and the managed database, preventing the web application from receiving data. A firewall is a network security device that monitors and controls incoming and outgoing network traffic based on predefined rules¹. A deployment script template is a way to automate the deployment of resources and configurations in Azure Resource Manager¹. If the script template contains incorrect or conflicting rules for the firewall, it can cause the issue.

References: CompTIA Cloud+ CV0-003 Exam Objectives, Objective 2.2: Given a scenario, deploy and test a cloud solution ; Use deployment scripts in templates - Azure Resource Manager¹

NEW QUESTION 215

- (Topic 4)

An organization is developing a new online product. The product must:

- Minimize organizational infrastructure and comply with security standards.
- Minimize organizational compliance efforts.
- Focus on application development and increase speed to market.

Which of the following should the organization consider, given the requirements listed above?

- A. Use cloud-native serverless services.
- B. Implement automated compliance scanning tools.
- C. Harden servers using repeatable compliance templates.
- D. Deploy compliance linters in the CI/CD pipeline.

Answer: A

Explanation:

One possible answer is:

A. Use cloud-native serverless services.

Cloud-native serverless services are a type of cloud computing that allows developers to build and run applications without having to manage servers, infrastructure, or scaling. Cloud-native serverless services can help the organization meet the requirements listed above, as they can:

? Minimize organizational infrastructure and comply with security standards. Cloud-native serverless services are fully managed by the cloud provider, which means the organization does not have to provision, configure, or maintain any servers or infrastructure. The cloud provider also handles the security aspects of the serverless environment, such as encryption, authentication, authorization, patching, and monitoring. The organization can focus on developing the application logic and rely on the cloud provider to meet the security standards¹².

? Minimize organizational compliance efforts. Cloud-native serverless services can also help the organization reduce the compliance burden, as they can leverage the compliance certifications and attestations of the cloud provider. The cloud provider can ensure that the serverless environment complies with various regulations and standards, such as PCI DSS, HIPAA, GDPR, ISO 27001, etc. The organization can inherit the compliance posture of the cloud provider and avoid the hassle of auditing and validating their own infrastructure¹².

? Focus on application development and increase speed to market. Cloud-native serverless services can also enable the organization to accelerate the development and delivery of their online product, as they can write code using their preferred programming languages and frameworks, and deploy it quickly and easily to the serverless environment. The serverless environment can automatically scale up or down based on the demand, ensuring high availability and performance. The organization can also integrate serverless services with other cloud services, such as databases, storage, analytics, etc., to create a full-stack application¹².

NEW QUESTION 217

- (Topic 4)

A cloud administrator is investigating slow VM performance. The administrator has checked the physical server performance and has identified the host is under stress due to a peak usage workload. Which of the following is the NEXT step the administrator should complete?

- A. Perform a root cause analysis
- B. Migrate the VM to a different host.
- C. Document the findings.
- D. Perform a system restart.

Answer: B

Explanation:

Migrating the VM to a different host is a common technique to improve the performance of a VM that is suffering from resource contention or contention on the physical server. By moving the VM to a different host, the administrator can:

Reduce the stress and load on the original host, which may be under stress due to a peak usage workload.

Increase the availability and reliability of the VM, which may be experiencing slow performance due to resource contention or contention on the original host.

Balance the workload and resource utilization across multiple hosts, which may improve the overall performance and efficiency of the cloud environment.

Migrating the VM to a different host can be done manually or automatically, depending on the configuration and capabilities of the cloud platform. Some cloud platforms support live migration, which allows moving a VM to a different host without interrupting its operation or service. Other cloud platforms require shutting down or pausing the VM before migrating it to a different host .

NEW QUESTION 218

- (Topic 4)

During a security incident on an IaaS platform, which of the following actions will a systems administrator most likely take as part of the containment procedure?

- A. Connect to an instance for triage.
- B. Add a deny rule to the network ACL.
- C. Mirror the traffic to perform a traffic capture.
- D. Perform a memory acquisition.

Answer: B

Explanation:

Adding a deny rule to the network ACL is a common containment procedure for a security incident on an IaaS platform, as it can isolate the affected instance from the rest of the network and prevent further compromise or data exfiltration. Connecting to an instance for triage, mirroring the traffic to perform a traffic capture, and performing a memory acquisition are more likely to be part of the analysis or evidence collection procedures, not the containment procedure.

References: CompTIA Cloud+ CV0-003 Exam Objectives, Objective 4.2: Given a scenario, apply security configurations and compliance controls ; Cloud Security Mitigation | Cloud Computing | CompTIA1

NEW QUESTION 222

- (Topic 3)

A cloud administrator would like to maintain file integrity checks through hashing on a cloud object store. Which of the following is MOST suitable from a performance perspective?

- A. SHA-256
- B. SHA-512
- C. MD5
- D. AES

Answer: C

Explanation:

The most suitable hashing algorithm from a performance perspective to maintain file integrity checks on a cloud object store is MD5 (Message Digest 5). MD5 is a hashing algorithm that generates a 128-bit hash value for any given input data. MD5 is faster and more efficient than other hashing algorithms, such as SHA-256 or SHA-512, which generate longer hash values and require more computational resources. MD5 can be used to verify the integrity of files by comparing their hash values before and after transmission or storage. Reference: CompTIA Cloud+ Certification Exam Objectives, Domain 2.0 Security, Objective 2.5 Given a scenario, apply data security techniques in the cloud.

NEW QUESTION 226

- (Topic 3)

A product-based company wants to transition to a method that provides the capability to enhance the product seamlessly and keep the development iterations to a shorter time frame. Which of the following would BEST meet these requirements?

- A. Implement a secret management solution.
- B. Create autoscaling capabilities.
- C. Develop CI/CD tools.
- D. Deploy a CMDB tool.

Answer: C

Explanation:

CI/CD tools are software tools that enable continuous integration and continuous delivery or deployment, which are methods to frequently deliver software products to customers by introducing automation into the stages of software development. CI/CD tools can help a product-based company to transition to a method that provides the capability to enhance the product seamlessly and keep the development iterations to a shorter time frame, as they can offer the following benefits:

? Faster and more reliable delivery of software products, as CI/CD tools can automate the processes of building, testing, and deploying code changes, reducing manual errors and delays.

? Higher quality and performance of software products, as CI/CD tools can facilitate ongoing feedback, monitoring, and improvement of the code, ensuring that it meets the customer expectations and requirements.

? Greater collaboration and communication among the development teams, as CI/CD tools can integrate with various tools and platforms, such as version control systems, code repositories, testing frameworks, and cloud services, enabling a seamless workflow and visibility across the software lifecycle.

Some examples of popular CI/CD tools are Jenkins¹, CircleCI², GitLab CI/CD³, and AWS CodeBuild⁴.

NEW QUESTION 231

- (Topic 3)

A cloud administrator needs to control the connections between a group of web servers and database servers as part of the financial application security review. Which of the following would be the BEST way to achieve this objective?

- A. Create a directory security group.
- B. Create a resource group.
- C. Create separate VLANs.
- D. Create a network security group.

Answer: D

Explanation:

A network security group is a service that allows the cloud administrator to filter and control the network traffic between different resources in a cloud environment. A network security group contains security rules that specify the source, destination, protocol, port, and direction of the traffic, and whether to allow or deny it. A network security group can be associated with a subnet or a network interface in a virtual machine, and it can apply to inbound or outbound traffic. A network security group would be the best way to achieve the objective of controlling the connections between a group of web servers and database servers as part of the financial application security review, as it can provide granular and flexible control over the network access and security of the servers.

NEW QUESTION 234

- (Topic 3)

A systems administrator is troubleshooting issues with network slowness. Traffic analysis shows that uplink bandwidth on the core switch is often sustained at 125Mbps due to a combination of production traffic from other sources. Which of the following would BEST resolve the issue?

- A. Turn off the servers that use the most bandwidth.
- B. Enable QoS to prioritize production traffic.
- C. Increase the buffer size on the core switch.

D. Reboot the core switch.

Answer: B

Explanation:

The best solution to resolve the issue of network slowness caused by high uplink bandwidth utilization on the core switch is to enable quality of service (QoS) to prioritize production traffic over other types of traffic. QoS is a mechanism that allows network administrators to classify and manage network traffic according to its importance, latency, bandwidth, and reliability requirements. By enabling QoS, the core switch can allocate more resources and guarantee better performance for production traffic, while limiting or dropping less critical traffic. Reference: CompTIA Cloud+ Certification Exam Objectives, Domain 4.0 Troubleshooting, Objective 4.1 Given a scenario, troubleshoot connectivity issues related to cloud implementations.

NEW QUESTION 239

- (Topic 3)

A cloud administrator has created a new asynchronous workflow to deploy VMs to the cloud in bulk. When the workflow is tested for a single VM, it completes successfully. However, if the workflow is used to create 50 VMs at once, the job fails. Which of the following is the MOST likely cause of the issue? (Choose two.)

- A. Incorrect permissions
- B. Insufficient storage
- C. Billing issues with the cloud provider
- D. No connectivity to the public cloud
- E. Expired API token
- F. Disabled autoscaling

Answer: BE

Explanation:

The most likely causes of the issue where the new asynchronous workflow fails to create 50 VMs at once in the public cloud are insufficient storage and expired API token. Insufficient storage means that there is not enough disk space available in the public cloud to accommodate all the VMs that are being created simultaneously. This could result in errors or failures during the provisioning process. Expired API token means that the authentication credential that is used by the workflow to communicate with the public cloud service has expired or become invalid. This could result in errors or failures during the API calls or requests. Reference: CompTIA Cloud+ Certification Exam Objectives, Domain 4.0 Troubleshooting, Objective 4.5 Given a scenario, troubleshoot automation/orchestration issues.

NEW QUESTION 244

- (Topic 3)

A security team is conducting an audit of the security group configurations for the Linux servers that are hosted in a public IaaS. The team identifies the following rule as a potential

Protocol	Port	Source	Description
TCP	22	0.0.0.0/0	Allow SSH access

A cloud administrator, who is working remotely, logs in to the cloud management console and modifies the rule to set the source to "My IP". Shortly after deploying the rule, an internal developer receives the following error message when attempting to log in to the server using SSH: Network error: connection timed out.

However, the administrator is able to connect successfully to the same server using SSH. Which of the following is the BEST option for both the developer and the administrator to access the server from their locations?

- A. Modify the outbound rule to allow the company's external IP address as a source.
- B. Add an inbound rule to use the IP address for the company's main office as a source.
- C. Modify the inbound rule to allow the company's external IP address as a source.
- D. Delete the inbound rule to allow the company's external IP address as a source.

Answer: C

Explanation:

The inbound rule that the security team identified as a potential vulnerability is the one that allows SSH access (port 22) from any source (0.0.0.0/0). This means that anyone on the internet can try to connect to the Linux servers using SSH, which poses a risk of unauthorized access or brute-force attacks. The cloud administrator, who is working remotely, logs in to the cloud management console and modifies the rule to set the source to "My IP". This means that only the administrator's IP address can connect to the Linux servers using SSH, which improves the security of the servers. However, this also prevents other authorized users, such as the internal developer, from accessing the servers using SSH, as they have different IP addresses than the administrator. Therefore, the administrator needs to modify the rule again to allow more sources for SSH access.

The best option for both the developer and the administrator to access the server from their locations is to modify the inbound rule to allow the company's external IP address as a source. This means that only the IP addresses that belong to the company's network can connect to the Linux servers using SSH, which reduces the attack surface and ensures that only authorized users can access the servers. The company's external IP address can be obtained by using a web service such as [What Is My IP Address?] or [IP Location]. The administrator can then enter this IP address or its CIDR notation in the source field of the inbound rule.

NEW QUESTION 249

- (Topic 3)

A company is performing a DR drill and is looking to validate its documentation. Which of the following metrics will determine the service recovery duration?

- A. MTTF
- B. SLA
- C. RTO
- D. RPO

Answer: C

Explanation:

RTO (Recovery Time Objective) is a metric that determines the maximum amount of time that a service can be unavailable or disrupted before it causes unacceptable consequences for the business. RTO is normally measured in minutes, hours, or days, and it is based on the criticality and priority of the service. RTO is one of the key metrics that can determine the service recovery duration, as it defines the target time frame for restoring the service to normal operations after a disaster. For example, if a company has an RTO of four hours for its email service, it means that it aims to recover the email service within four hours after a disaster, such as a server failure or a network outage.

NEW QUESTION 251

- (Topic 3)

A company has hired a security firm to perform a vulnerability assessment of its environment. In the first phase, an engineer needs to scan the network services exposed by the hosts. Which of the following will help achieve this with the LEAST privileges?

- A. An agent-based scan
- B. A credentialed scan
- C. A network-based scan
- D. An application scan

Answer: C

Explanation:

A network-based scan is a type of vulnerability assessment that scans the network services exposed by the hosts without requiring any credentials or agents. This type of scan will help achieve the objective of scanning the network services with the least privileges, as it does not need any access to the hosts or their internal configurations. A network-based scan can identify open ports, running services, and potential vulnerabilities on the hosts. Reference: CompTIA Cloud+ Certification Exam Objectives, Domain 2.0 Security, Objective 2.4 Given a scenario, implement security automation and orchestration in a cloud environment.

NEW QUESTION 253

- (Topic 3)

A company that requires full administrative control at the OS level is considering the use of public cloud services. Which of the following service models would BEST fit the company's requirements?

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

Answer: D

Explanation:

IaaS (Infrastructure as a Service) is a public cloud service model that provides access to fundamental compute, network, and storage resources on demand over the public Internet or through dedicated connections. Customers can provision and configure these resources according to their needs, and they have full administrative control at the OS level. This means that customers can install, update, and manage any software or applications they want on the cloud servers, as well as apply their own security and compliance policies. IaaS is suitable for companies that require high flexibility and customization of their cloud infrastructure, as well as scalability and cost-efficiency.

NEW QUESTION 257

.....

Relate Links

100% Pass Your CV0-003 Exam with ExamBible Prep Materials

<https://www.exambible.com/CV0-003-exam/>

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>