CompTIA

Exam Questions CV0-003

CompTIA Cloud+ Certification Exam

NEW QUESTION 1
- (Topic 1)
A systems administrator needs to configure monitoring for a private cloud environment. The administrator has decided to use SNMP for this task.
Which of the following ports should the administrator open on the monitoring server's firewall?

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

Answer: D

Explanation:
Port 161 is the default port used by Simple Network Management Protocol (SNMP) to communicate with network devices and collect information about their status, performance, configuration, and events. Opening port 161 on the monitoring server's firewall will allow SNMP traffic to pass through and enable monitoring for a private cloud environment. If port 161 is closed or blocked, SNMP traffic will be denied or dropped, resulting in a failure to monitor the network devices.
References: CompTIA Cloud+ Certification Exam Objectives, page 15, section 2.8

NEW QUESTION 2
- (Topic 1)
An organization has two businesses that are developing different software products. They are using a single cloud provider with multiple IaaS instances. The organization identifies that the tracking of costs for each business are inaccurate.
Which of the following is the BEST method for resolving this issue?

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

Answer: B

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

NEW QUESTION 3
- (Topic 1)
A cloud administrator is reviewing the authentication and authorization mechanism implemented within the cloud environment. Upon review, the administrator discovers the sales group is part of the finance group, and the sales team members can access the financial application. Single sign-on is also implemented, which makes access much easier.
Which of the following access control rules should be changed?

A. Discretionary-based
B. Attribute-based
C. Mandatory-based
D. Role-based

Answer: D

Explanation:
Role-based access control (RBAC) is a type of access control model that assigns permissions and privileges to users based on their roles or functions within an organization or system. RBAC can help simplify and streamline the management and enforcement of access policies, as it can reduce the complexity and redundancy of assigning permissions to individual users or groups. RBAC can also help improve security and compliance, as it can limit or grant access based on the principle of least privilege and the separation of duties. RBAC is the best access control rule to change when the sales group is part of the finance group and the sales team members can access the financial application due to a single sign-on mechanism being implem
Reference: https://www.ekransystem.com/en/blog/rbac-vs-abac

NEW QUESTION 4
- (Topic 1)
An administrator is performing an in-place upgrade on a quest VM operating system.
Which of the following can be performed as a quick method to roll back to an earlier state, if necessary?

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

Answer: D

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

Reference: https://cloud.google.com/compute/docs/tutorials/performing-in-place-upgrade- windows-server

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

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

Answer: D

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

NEW QUESTION 7
- (Topic 1)
An organization has the following requirements that need to be met when implementing cloud services:
? SSO to cloud infrastructure
? On-premises directory service
? RBAC for IT staff
Which of the following cloud models would meet these requirements?

A. Public
B. Community
C. Hybrid
D. Multitenant

Answer: C

Explanation:
A hybrid cloud is a type of cloud deployment model that combines two or more different types of clouds, such as public, private, or community clouds, into a single integrated environment. A hybrid cloud can meet the requirements for implementing cloud services with SSO to cloud infrastructure, on-premises directory service, and RBAC for IT staff, as it can provide flexibility, scalability, and security for cloud-based and on-premises resources. A hybrid cloud can also enable seamless and secure access to cloud infrastructure using SSO with directory service federation, as well as granular and consistent control over IT staff permissions using RBAC across different cloud environments. References: CompTIA Cloud+ Certification Exam Objectives, page 8, section 1.2

NEW QUESTION 8
- (Topic 1)
A company has decided to get multiple compliance and security certifications for its public cloud environment. However, the company has few staff members to handle the extra workload, and it has limited knowledge of the current infrastructure.
Which of the following will help the company meet the compliance requirements as quickly as possible?

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

Answer: B

Explanation:
A cloud access security broker (CASB) is a type of security solution that acts as a gateway between cloud service users and cloud service providers. A CASB can help a company get multiple compliance and security certifications for its public cloud environment, as it can provide visibility, control, and protection for cloud data

and applications. A CASB can also help the company handle the extra workload and overcome the limited knowledge of the current infrastructure, as it can automate and simplify the enforcement of security policies and compliance requirements across multiple cloud services. References: CompTIA Cloud+ Certification Exam Objectives, page 14, section 2.7

NEW QUESTION 9
- (Topic 1)
A systems administrator is configuring RAID for a new server. This server will host files for users and replicate to an identical server. While redundancy is necessary, the most important need is to maximize storage.
Which of the following RAID types should the administrator choose?

A. 5
B. 6
C. 10
D. 50

Answer: C

Explanation:
RAID 50 is a type of RAID level that combines RAID 5 and RAID 0 to create a nested RAID configuration. RAID 50 consists of two or more RAID 5 arrays that are striped together using RAID 0. RAID 50 can provide redundancy, fault tolerance, and high performance for large data sets. RAID 50 can also maximize storage, as it has a higher usable capacity than other RAID levels with similar features, such as RAID 6 or RAID 10. The administrator should choose RAID 50 to configure a new server that will host files for users and replicate to an identical server, as it can meet the needs of redundancy and storage maximization. References: CompTIA Cloud+ Certification Exam Objectives, page 9, section 1.4

NEW QUESTION 10
- (Topic 1)
A systems administrator is creating a playbook to run tasks against a server on a set schedule.
Which of the following authentication techniques should the systems administrator use within the playbook?

A. Use the server's root credentials
B. Hard-code the password within the playbook
C. Create a service account on the server
D. Use the administrator's SSO credentials

Answer: C

Explanation:
A service account is a type of user account that is created for a specific service or application to run on a server or system. Creating a service account on the server is the best authentication technique to use within the playbook to run tasks against the server on a set schedule, as it can provide secure and consistent access to the server without exposing or hard-coding any sensitive credentials within the playbook. Creating a service account can also help manage and monitor the tasks and activities performed by the service or application on the server. References: CompTIA Cloud+ Certification Exam Objectives, page 14, section 2.7

NEW QUESTION 10
- (Topic 1)
A company has deployed a new cloud solution and is required to meet security compliance.
Which of the following will MOST likely be executed in the cloud solution to meet security requirements?

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

Answer: C

Explanation:
Vulnerability testing is a type of security testing that identifies and evaluates the weaknesses or flaws in a system or service that could be exploited by attackers. Vulnerability testing can help meet security compliance requirements when deploying a new cloud solution, as it can reveal any potential security risks or gaps in the cloud environment and provide recommendations for remediation or mitigation. Vulnerability testing can also help improve security posture and performance, as it can prevent or reduce the impact of cyberattacks, data breaches, or service disruptions.
References: CompTIA Cloud+ Certification Exam Objectives, page 14, section 2.7

NEW QUESTION 14
- (Topic 1)
Which of the following is relevant to capacity planning in a SaaS environment?

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

Answer: D

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

NEW QUESTION 18
- (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 20
- (Topic 2)
A systems administrator is deploying a new cloud application and needs to provision cloud services with minimal effort. The administrator wants to reduce the tasks required for maintenance, such as OS patching, VM and volume provisioning, and autoscaling configurations. Which of the following would be the BEST option to deploy the new application?

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

Answer: D

Explanation:
Serverless is what would be the best option to deploy a new cloud application and provision cloud services with minimal effort while reducing the tasks required for maintenance such as OS patching, VM and volume provisioning, and autoscaling configurations. Serverless is a cloud service model that provides customers with a platform to run applications or functions without having to manage or provision any underlying infrastructure or resources, such as servers, storage, network, OS, etc. Serverless can provide benefits such as:
? Minimal effort: Serverless can reduce the effort required to deploy a new cloud application and provision cloud services by automating and abstracting away all the infrastructure or resource management or provisioning tasks from customers, and allowing them to focus only on writing code or logic for their applications or functions.
? Reduced maintenance: Serverless can reduce the tasks required for maintenance by handling all the infrastructure or resource maintenance tasks for customers, such as OS patching, VM and volume provisioning, autoscaling configurations, etc., and ensuring that they are always up-to-date and optimized.

NEW QUESTION 23
- (Topic 2)
A cloud administrator wants to have a central repository for all the logs in the company's private cloud. Which of the following should be implemented to BEST meet this requirement?

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

Answer: D

Explanation:
Reference: https://www.itpro.com/infrastructure/network-internet/355174/how-to-build-a- dedicated-syslog-server
A syslog server is what the administrator should implement to have a central repository for all the logs in the company's private cloud. Syslog is a standard protocol that allows network devices and systems to send log messages to a centralized server or collector. Syslog can help to consolidate and manage logs from different sources in one place, which can facilitate monitoring, analysis, troubleshooting, auditing, etc.

NEW QUESTION 27
- (Topic 2)
A cloud administrator is building a new VM for machine-learning training. The developer requesting the VM has stated that the machine will need a full GPU dedicated to it.
Which of the following configuration options would BEST meet this requirement?

A. Virtual GPU
B. External GPU
C. Passthrough GPU
D. Shared GPU

Answer: C

Explanation:
Reference: https://blogs.vmware.com/apps/2018/09/using-gpus-with-virtual-machines-on- vsphere-part-2-vmdirectpath-i-o.html
Passthrough GPU is a configuration option that allows a VM to access a physical GPU directly without any virtualization layer or sharing mechanism. This provides the VM with full and exclusive access to the GPU resources and performance. Passthrough GPU is suitable for applications that require intensive graphics processing or machine learning training.

NEW QUESTION 30
- (Topic 2)
A database analyst reports it takes two hours to perform a scheduled job after onboarding 10,000 new users to the system. The analyst made no changes to the scheduled job before or after onboarding the users. The database is hosted in an IaaS instance on a cloud provider. Which of the following should the cloud administrator evaluate to troubleshoot the performance of the job?

A. The laaS compute configurations, the capacity trend analysis reports, and the storage IOPS
B. The hypervisor logs, the memory utilization of the hypervisor host, and the network throughput of the hypervisor
C. The scheduled job logs for successes and failures, the time taken to execute the job, and the job schedule
D. Migrating from laaS to on premises, the network traffic between on-premises users and the laaS instance, and the CPU utilization of the hypervisor host

Answer: A

Explanation:
To troubleshoot the performance of a scheduled job that takes two hours to run after onboarding 10,000 new users to a cloud-based system, the administrator should evaluate the IaaS compute configurations, the capacity trend analysis reports, and the storage IOPS. These factors can affect the performance of a database job in an IaaS instance on a cloud provider. The IaaS compute configurations include the CPU, memory, and network resources assigned to the instance. The capacity trend analysis reports show the historical and projected usage and demand of the resources. The storage IOPS (Input/Output Operations Per Second) measure the speed and performance of the disk storage. The administrator should check if these factors are sufficient, optimal, or need to be adjusted to improve the performance of the job.

NEW QUESTION 31
- (Topic 2)
All of a company's servers are currently hosted in one cloud MSP. The company created a new cloud environment with a different MSP. A cloud engineer is now tasked with preparing for server migrations and establishing connectivity between clouds. Which of the following should the engineer perform FIRST?

A. Peer all the networks from each cloud environment.
B. Migrate the servers.
C. Create a VPN tunnel.
D. Configure network access control lists.

Answer: C

Explanation:
Creating a VPN tunnel is the first action that the engineer should perform to
prepare for server migrations and establish connectivity between clouds. 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. Creating a VPN tunnel can enable communication and interoperability between different cloud environments, as well as protect data from interception or modification during migration.

NEW QUESTION 35
- (Topic 2)
A private IaaS administrator is receiving reports that all newly provisioned Linux VMs are running an earlier version of the OS than they should be. The administrator reviews the automation scripts to troubleshoot the issue and determines the scripts ran successfully. Which of the following is the MOST likely cause of the issue?

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

Answer: C

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

NEW QUESTION 36
- (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 39
- (Topic 2)
A cloud administrator is responsible for managing a cloud-based content management solution. According to the security policy, any data that is hosted in the cloud must be protected against data exfiltration. Which of the following solutions should the administrator implement?

A. HIDS
B. FIM
C. DLP
D. WAF

Answer: C

Explanation:
DLP (Data Loss Prevention) is what the administrator should implement to protect data against data exfiltration in a cloud-based content management solution. Data exfiltration is a process of transferring or stealing data from a system or network without authorization or permission. Data exfiltration can cause data breaches, leaks, or losses that may affect confidentiality, integrity, or availability of data. DLP is a tool or service that monitors and controls data movement and usage within a system or network. DLP can help to prevent data exfiltration by detecting and blocking any unauthorized or suspicious data transfers or activities, as well as enforcing policies and rules for data classification, encryption, access, etc.

NEW QUESTION 44
- (Topic 2)
After a few new web servers were deployed, the storage team began receiving incidents in their queue about the web servers. The storage administrator wants to verify the incident tickets that should have gone to the web server team. Which of the following is the MOST likely cause of the issue?

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

Answer: C

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

NEW QUESTION 45
- (Topic 2)
A technician is trying to delete six decommissioned VMs. Four VMs were deleted without issue. However, two of the VMs cannot be deleted due to an error. Which of the following would MOST likely enable the technician to delete the VMs?

A. Remove the snapshots
B. Remove the VMs' IP addresses
C. Remove the VMs from the resource group
D. Remove the lock from the two VMs

Answer: D

Explanation:
Removing the lock from the two VMs is what would most likely enable the technician to delete the VMs that cannot be deleted due to an error. A lock is a feature that prevents certain actions or operations from being performed on a resource or service, such as deleting, modifying, moving, etc. A lock can help to protect a resource or service from accidental or unwanted changes or removals. Removing the lock from the two VMs can enable the technician to delete them by allowing the delete action or operation to be performed on them.

NEW QUESTION 49
- (Topic 2)
A company wants to move its environment from on premises to the cloud without vendor lock-in. Which of the following would BEST meet this requirement?

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

Answer: C

Explanation:
IaaS (Infrastructure as a Service) is what would best meet the requirement of moving an environment from on premises to the cloud without vendor lock-in. Vendor lock- in is a situation where customers become dependent on or tied to a specific vendor or provider for their products or services, and face difficulties

NEW QUESTION 51
- (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 56
- (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 60
- (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 65
- (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 70
- (Topic 2)
A company needs to access the cloud administration console using its corporate identity. Which of the following actions would MOST likely meet the requirements?

A. Implement SSH key-based authentication.
B. Implement cloud authentication with local LDAP.
C. Implement multifactor authentication.
D. Implement client-based certificate authentication.

Answer: D

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

NEW QUESTION 71
- (Topic 2)
A cloud security analyst needs to ensure the web servers in the public subnet allow only secure communications and must remediate any possible issue. The stateful configuration for the public web servers is as follows:

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

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

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

Answer: A

Explanation:
To ensure the web servers in the public subnet allow only secure communications and remediate any possible issue, the analyst should remove rules 1, 2, and 5 from the stateful configuration. These rules are allowing insecure or unnecessary traffic to or from the web servers, which may pose security risks or performance issues. The rules are:
? Rule 1: This rule allows inbound traffic on port 80 (HTTP) from any source to any destination. HTTP is an unencrypted and insecure protocol that can expose web traffic to interception, modification, or spoofing. The analyst should remove this rule and use HTTPS (port 443) instead, which encrypts and secures web traffic.
? Rule 2: This rule allows outbound traffic on port 25 (SMTP) from any source to any destination. SMTP is a protocol that is used to send email messages. The web servers in the public subnet do not need to send email messages, as this is not their function. The analyst should remove this rule and block outbound SMTP traffic, which may prevent spamming or phishing attacks from compromised web servers.
? Rule 5: This rule allows inbound traffic on port 22 (SSH) from any source to any destination. SSH is a protocol that allows remote access and management of systems or devices using a command-line interface. The web servers in the public subnet do not need to allow SSH access from any source, as this may expose them to unauthorized or malicious access. The analyst should remove this rule and restrict SSH access to specific sources, such as the administrator's workstation or a bastion host.

NEW QUESTION 75
- (Topic 1)
A web server has been deployed in a public IaaS provider and has been assigned the public IP address of 72.135.10.100. Users are now reporting that when they browse to the website, they receive a message indicating the service is unavailable. The cloud administrator logs into the server, runs a netstat command, and notices the following relevant output:

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

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

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

Answer: D

Explanation:
Updating the gateway on the web server to use 72.135.10.1 is the best action to take to resolve the issue of the web server being unavailable after being deployed in a public IaaS provider and assigned the public IP address of 72.135.10.100. Updating the gateway can ensure that the web server can communicate with the

Internet and other networks by using the correct router or device that connects the web server's network to other networks. Updating the gateway can also improve performance and reliability, as it can avoid any routing errors or conflicts that may prevent the web server from responding to remote login requests.
References: CompTIA Cloud+ Certification Exam Objectives, page 15, section 2.8

NEW QUESTION 80
- (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 81
- (Topic 1)
A systems administrator is troubleshooting network throughput issues following a deployment. The network is currently being overwhelmed by the amount of traffic between the database and the web servers in the environment.
Which of the following should the administrator do to resolve this issue?

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

Answer: C

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

NEW QUESTION 83
- (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 84
- (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 85
- (Topic 1)
Which of the following will mitigate the risk of users who have access to an instance modifying the system configurations?

A. Implement whole-disk encryption
B. Deploy the latest OS patches
C. Deploy an anti-malware solution
D. Implement mandatory access control

Answer: D

Explanation:
Mandatory access control (MAC) is a type of access control model that enforces strict security policies based on predefined rules and labels. MAC assigns security labels to subjects (users or processes) and objects (files or resources) and allows access only if the subject has the appropriate clearance and need-to-know for the object. MAC can mitigate the risk of users who have access to an instance modifying the system configurations, as it can prevent unauthorized or accidental changes to critical files or settings by restricting access based on predefined rules and labels. References: CompTIA Cloud+ Certification Exam Objectives, page 14, section 2.7

NEW QUESTION 88
- (Topic 1)
Lateral-moving malware has infected the server infrastructure.
Which of the following network changes would MOST effectively prevent lateral movement in the future?

A. Implement DNSSEC in all DNS servers
B. Segment the physical network using a VLAN
C. Implement microsegmentation on the network
D. Implement 802.1X in the network infrastructure

Answer: C

Explanation:
Microsegmentation is a type of network security technique that divides a network into smaller logical segments or zones based on workload or application characteristics and applies granular policies and rules to control and isolate traffic within each segment or zone. Implementing microsegmentation on the network can help prevent lateral movement in the future after lateral-moving malware has infected the server infrastructure, as it can limit the exposure and spread of malware by restricting access and communication between different segments or zones based on predefined criteria such as identity, role, or behavior. References: CompTIA Cloud+ Certification Exam Objectives, page 14, section 2.7

NEW QUESTION 92
- (Topic 1)
A company developed a product using a cloud provider’s PaaS platform and many of the platform-based components within the application environment.
Which of the following would the company MOST likely be concerned about when utilizing a multicloud strategy or migrating to another cloud provider?

A. Licensing
B. Authentication providers
C. Service-level agreement
D. Vendor lock-in

Answer: D

Explanation:
Vendor lock-in is a situation where a customer becomes dependent on a specific vendor for products or services and faces high switching costs or barriers when trying to change vendors. Vendor lock-in is most likely to be a concern for a company that developed a product using a cloud provider’s PaaS platform and many of the platform- based components within the application environment when utilizing a multicloud strategy or migrating to another cloud provider, as it can limit the flexibility, scalability, and portability of the product and increase the complexity, risk, and cost of moving or integrating with other cloud platforms or providers. References: CompTIA Cloud+ Certification Exam Objectives, page 8, section 1.2

NEW QUESTION 96
- (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 99
- (Topic 4)
A cloud administrator is evaluating a solution that will limit access to authorized individuals. The solution also needs to ensure the system that connects to the environment meets patching, antivirus, and configuration requirements. Which of the following technologies would BEST meet these requirements?

A. NAC
B. EDR
C. IDS
D. HIPS

Answer: A

Explanation:

NAC (Network Access Control) is a technology that will limit access to authorized individuals and ensure the system that connects to the environment meets patching, antivirus, and configuration requirements. NAC can enforce policies and rules that define who, what, when, where, and how a device or a user can access a network or a cloud environment. NAC can also inspect and evaluate the security posture and compliance status of a device or a user before granting or denying access. For example, NAC can check if the device has the latest patches, antivirus software, and configuration settings, and if not, it can quarantine, remediate, or reject the device. NAC can also monitor and audit the ongoing network activity and behavior of the devices and users, and take actions if any violations or anomalies are detected.

NEW QUESTION 101
- (Topic 4)
As a result of an IT audit, a customer has decided to move some applications from an old legacy system to a private cloud. The current server location is remote with low bandwidth. Which of the following is the best migration strategy to use for this deployment?

A. P2V with physical data transport
B. P2P with remote data copy
C. V2V with physical data transport
D. V2P with physical data transport
E. V2P with remote data copy

Answer: A

Explanation:
P2V stands for physical to virtual, which is the process of converting a physical server into a virtual machine. This is a common migration strategy for moving legacy systems to the cloud, as it preserves the existing configuration and data of the server. Physical data transport means using a physical device, such as a hard disk drive or a USB flash drive, to transfer the data from the source location to the destination location. This method is suitable for remote locations with low bandwidth, as it avoids the network latency and congestion that may occur with remote data copy. P2P, V2V, and V2P are other types of migration strategies, but they are not applicable for this scenario. P2P stands for physical to physical, which is the process of moving a physical server to another physical server. V2V stands for virtual to virtual, which is the process of moving a virtual machine to another virtual machine. V2P stands for virtual to physical, which is the process of converting a virtual machine into a physical server. Remote data copy means using a network connection, such as FTP or SCP, to transfer the data from the source location to the destination location. This method is suitable for locations with high bandwidth and reliable network connectivity. References: CompTIA Cloud+ CV0-003 Certification Study Guide, Chapter 21, Cloud Migration, page 3371.

NEW QUESTION 106
- (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 109
- (Topic 4)

A company is using IaaS services from two different providers: one for its primary site, and the other for a secondary site. The primary site is completely inaccessible, and the management team has decided to run through the BCP procedures. Which of the following will provide the complete asset information?

A. DR replication document
B. DR playbook
C. DR policies and procedures document
D. DR network diagram

Answer: B

Explanation:
According to the CompTIA Cloud+ CV0-003 Certification Study Guide1, the answer is B. DR playbook. A DR playbook is a document that contains the detailed steps and procedures to recover from a disaster scenario. It includes the asset information, such as the cloud resources, configurations, and dependencies, that are needed to restore the normal operations of the business. A DR replication document is a document that describes how the data and applications are replicated between the primary and secondary sites. A DR policies and procedures document is a document that defines the roles and responsibilities of the staff, the communication channels, and the objectives and scope of the DR plan. A DR network diagram is a visual representation of the network topology and connectivity between the primary and secondary sites.

NEW QUESTION 112
- (Topic 4)
A systems administrator needs to connect the companys network to a public cloud services provider. Which of the following will BEST ensure encryption in transit for data transfers?

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

Answer: B

Explanation:
The answer is A. SAML. SAML (Security Assertion Markup Language) is a standard for exchanging authentication and authorization data between different parties, such as a user and a service provider. In a federated cluster, SAML can be used to enable single sign-on (SSO) for users across multiple clusters or cloud providers. SAML relies on the exchange of XML-based assertions that contain information about the user's identity, attributes, and entitlements. If the users' API access tokens have become invalid, it could be because the SAML assertions have expired, been revoked, or corrupted. The administrator should check the SAML configuration and logs to determine the cause of this issue.
Some possible sources of information about SAML and federated clusters are:
? Authenticating | Kubernetes: This page provides an overview of authenticating users in Kubernetes, including using SAML for federated identity.
? Authenticating to the Kubernetes API server - Google Cloud: This page explains how to authenticate to the Kubernetes API server on Google Cloud, including using SAML for federated identity with Google Cloud Identity Platform.
? Error 403 User not authorized when trying to access Azure Databricks API through Active Directory - Stack Overflow: This page discusses a similar issue of users getting an error when trying to access Azure Databricks API using SAML and Active Directory.

NEW QUESTION 113
- (Topic 4)
A cloud administrator receives an email stating the following:
"Clients are receiving emails from our web application with non-encrypted links."
The administrator notices that links generated from the web application are opening in http://. Which of the following should be configured to redirect the traffic to https://?

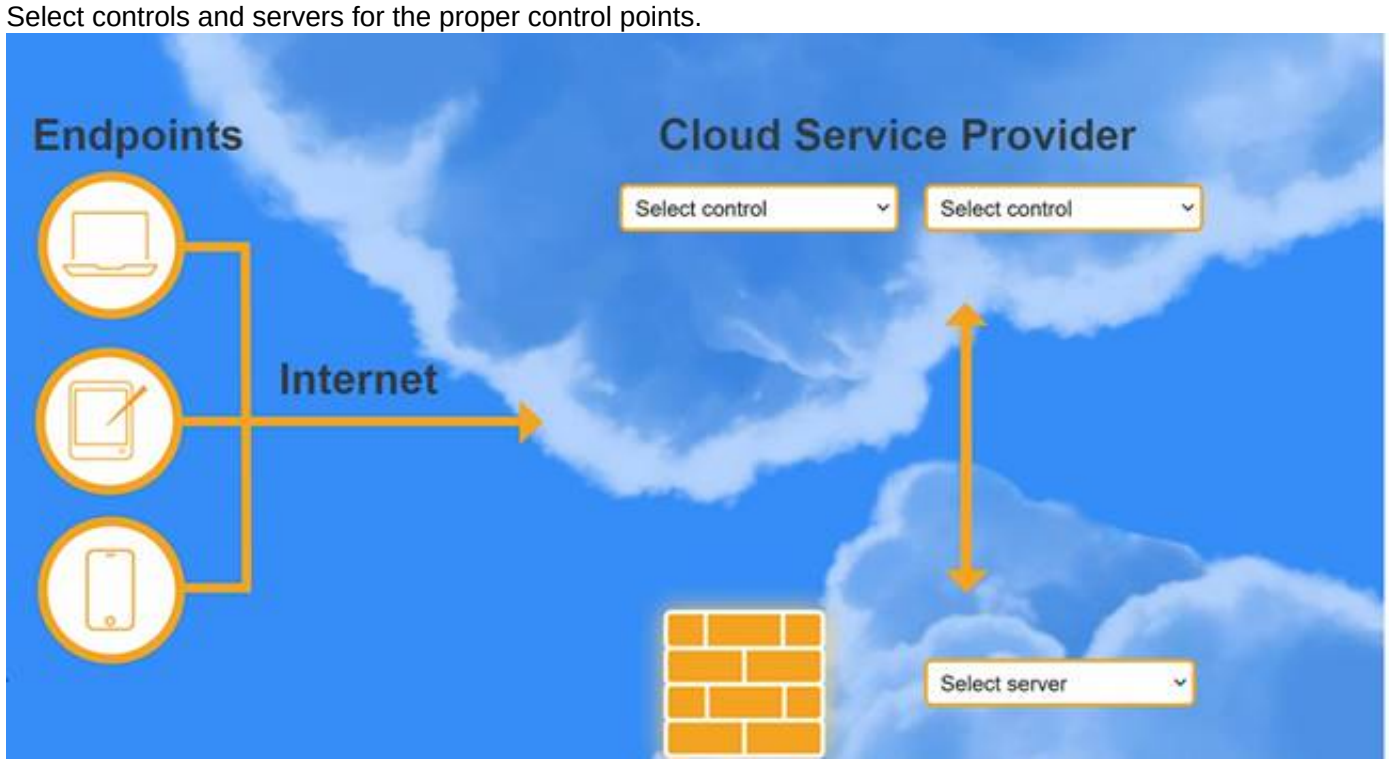
A. User account access
B. Programming code
C. Web server configuration
D. Load balancer setting

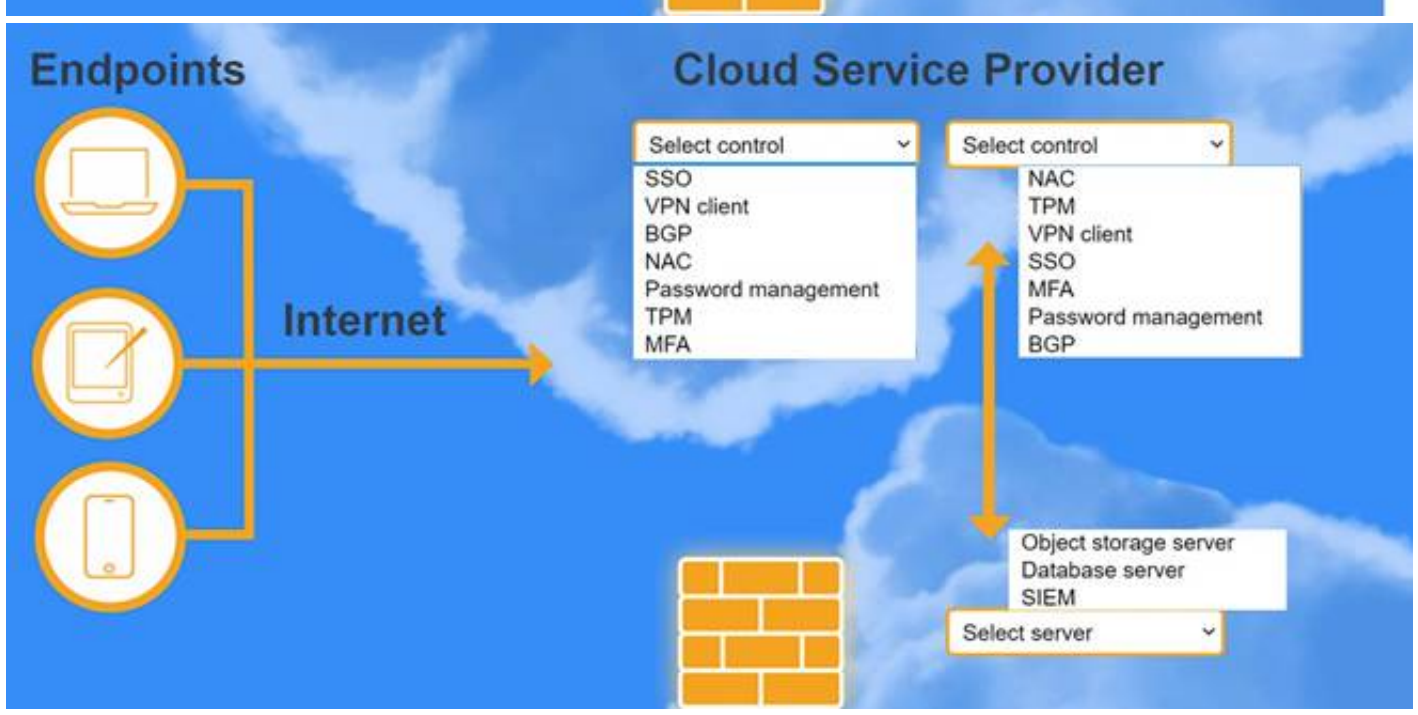
Answer: C

Explanation:
To redirect the traffic from HTTP to HTTPS, the web server configuration should be modified to include a rule that forces the HTTP requests to be redirected to HTTPS. This can be done by using the web server's configuration file or a .htaccess file. The exact syntax may vary depending on the web server software, but the general idea is to use a rewrite rule that matches the HTTP protocol and changes it to HTTPS. For example, on Apache web server, the following code can be added to the .htaccess file: RewriteEngine On
RewriteCond %{HTTPS} off
RewriteRule ^(.*)$ https://%{HTTP_HOST}%{REQUEST_URI} [L,R=301]
This code will check if the HTTPS is off, and if so, it will rewrite the URL to use HTTPS and redirect the client with a 301 status code, which means permanent redirection. This way, the clients will always use HTTPS to access the web application, and the links generated from the web application will be encrypted.
User account access (A) is not relevant to the redirection of HTTP to HTTPS, as it only controls who can access the web application. Programming code (B) may be used to generate the links with HTTPS, but it will not redirect the existing HTTP requests to HTTPS. Load balancer setting (D) may also be used to redirect the traffic to HTTPS, but it is not the most efficient or secure way, as it will add an extra layer of processing and expose the HTTP traffic to the load balancer. Therefore, web server configuration © is the best option to redirect the traffic to HTTPS.
Reference: The Official CompTIA Cloud+ Student Guide (Exam CV0-003), Chapter 4:
Cloud Security, Section 4.3: Secure Cloud Services, p. 4-23.

NEW QUESTION 118
HOTSPOT - (Topic 4)
A highly regulated business is required to work remotely, and the risk tolerance is very low. You are tasked with providing an identity solution to the company cloud that includes the following:
? secure connectivity that minimizes user login
? tracks user activity and monitors for anomalous activity
? requires secondary authentication

INSTRUCTIONS
Select controls and servers for the proper control points.

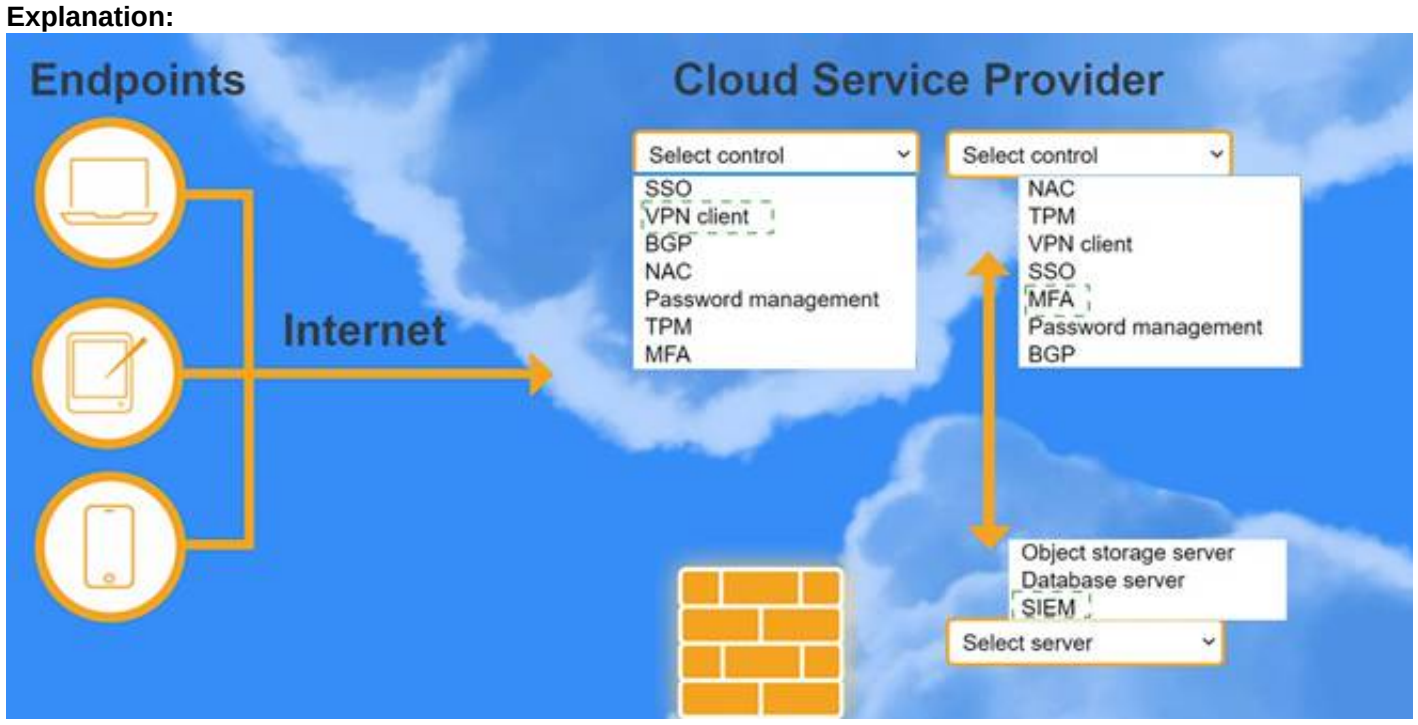




A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 123
- (Topic 4)
An organization hosts an ERP database in on-premises infrastructure. A recommendation has been made to migrate the ERP solution to reduce operational overhead in the maintenance of the data center. Which of the following should be considered when migrating this on-premises database to DBaaS?
? • Database application version compatibility
• Database IOPS values
• Database storage utilization
? • Physical database server CPU cache value
• Physical database server DAS type
• Physical database server network I/O

? • Database total user count
• Database total number of tables
• Database total number of storage procedures
• Physical database server memory configuration
• Physical database server CPU frequency

A. • Physical database server operating system

Answer: A

Explanation:
When migrating an on-premises database to DBaaS, it is important to consider the database application version compatibility, the database IOPS values, and the database storage utilization. These factors can affect the performance, functionality, and cost of the migration. Database application version compatibility refers to the ability of the DBaaS provider to support the same or compatible version of the database software as the on- premises database. This can ensure that the database features, syntax, and behavior are consistent and compatible across the environments. Database IOPS values refer to the input/output operations per second that the database performs. This can indicate the workload and throughput of the database, and help determine the appropriate size and configuration of the DBaaS instance. Database storage utilization refers to the amount of disk space that the database consumes. This can affect the cost and scalability of the DBaaS service, and help optimize the storage allocation and backup
strategies. References := CompTIA Cloud+ source documents or study guide
? CompTIA Cloud+ Certification Exam Objectives, Domain 2.0: Deployment, Objective 2.1: Given a scenario, execute and implement solutions using appropriate cloud migration tools and methods.
? Migrate your relational databases to Azure - .NET | Microsoft Learn, Migrate On- premises Tablespaces to DBaaS Database Using Cross-Platform Tablespace Transport
? Migrating On-Premises Databases to the DBaaS Database Using RMAN - Oracle, Overview

NEW QUESTION 127
- (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 128
- (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 131
- (Topic 4)
A cloud administrator deployed new hosts in a private cloud. After a few months elapsed, some of the hypervisor features did not seem to be working. Which of the following was MOST likely causing the issue?

A. Incorrect permissions
B. Missing license
C. Incorrect tags
D. Oversubscription

Answer: B

Explanation:
The correct answer is B. Missing license.
Some hypervisor features may require a valid license to work properly. If the license is missing, expired, or invalid, the hypervisor may not be able to use those features or may operate in a reduced functionality mode. For example, some features of Hyper-V, such as live migration, replication, and failover clustering, require a license for Windows Server or Windows 10 Enterprise1. Similarly, some features of VMware ESXi, such as vMotion, Storage vMotion, and Fault Tolerance,

require a license for VMware vSphere2. Therefore, if a cloud administrator deployed new hosts in a private cloud and found that some of the hypervisor features did not seem to be working after a few months elapsed, the most likely cause was a missing license. The administrator should check the license status of the hypervisor and renew or activate the license if needed.
Incorrect permissions are not a likely cause of the issue, as they would affect the access to the hypervisor or its resources, not the functionality of the hypervisor itself. Incorrect tags are also not a likely cause of the issue, as they are used for identification and classification of resources, not for enabling or disabling features. Oversubscription is not a likely cause of the issue either, as it would affect the performance or availability of the resources, not the functionality of the hypervisor itself.

NEW QUESTION 132
- (Topic 4)
A new development team requires workstations hosted in a PaaS to develop a new website. Members of the team also require remote access to the workstations using their corporate email addresses. Which of the following solutions will BEST meet these requirements? (Select TWO).

A. Deploy new virtual machines.
B. Configure email account replication.
C. Integrate identity services.
D. Implement a VDI solution.
E. Migrate local VHD workstations.
F. Create a new directory service.

Answer: AC

Explanation:
A Platform-as-a-Service (PaaS) is a cloud computing model that provides customers a complete cloud platform—hardware, software, and infrastructure—for developing, running, and managing applications without the cost, complexity, and inflexibility that often comes with building and maintaining that platform on-premises1.
To develop a new website using a PaaS, the development team needs to deploy new virtual machines (VMs) on the cloud platform. VMs are software emulations of physical computers that can run different operating systems and applications. By deploying new VMs, the development team can create a scalable and flexible environment for their website project, without having to invest in or manage physical hardware2.
To enable remote access to the workstations using their corporate email addresses, the development team needs to integrate identity services on the cloud platform. Identity services are services that provide authentication, authorization, and identity management for users and devices accessing cloud resources. By integrating identity services, the development team can use their corporate email addresses as single sign-on (SSO) credentials to access their workstations from any device and location, while ensuring security and compliance3.
The other options are not the best solutions for these requirements:
? Configuring email account replication is not necessary for remote access to the workstations. Email account replication is a process of synchronizing email accounts across different servers or locations. It can provide backup and redundancy for email services, but it does not provide authentication or identity management for remote access4.
? Implementing a Virtual Desktop Infrastructure (VDI) solution is not a PaaS solution.
VDI is a technology that allows users to access virtual desktops hosted on a centralized server. VDI can provide remote access to desktop environments, but it requires additional hardware, software, and management costs that are not included in a PaaS model5.
? Migrating local VHD workstations is not a PaaS solution. VHD stands for Virtual Hard Disk, which is a file format that represents a virtual hard disk drive. Migrating local VHD workstations means moving the virtual hard disk files from local storage to cloud storage. This can provide backup and portability for the workstations, but it does not provide a complete cloud platform for developing and running applications6.
? Creating a new directory service is not necessary for remote access to the workstations. A directory service is a service that stores and organizes information about users, devices, and resources on a network. Creating a new directory service means setting up a new database and schema for storing this information. This can provide identity management and access control for the network, but it does not provide authentication or SSO for remote access.

NEW QUESTION 135
- (Topic 4)
An organization provides integration services for finance companies that use web services. A new company that sends and receives more than 100,000 transactions per second has
been integrated using the web service. The other integrated companies are now reporting slowness with regard to the integration service. Which of the following is the cause of the issue?

A. Incorrect configuration in the authentication process
B. Incorrect configuration in the message queue length
C. Incorrect configuration in user access permissions
D. Incorrect configuration in the SAN storage pool

Answer: B

Explanation:
The correct answer is B. Incorrect configuration in the message queue length.
A message queue is a data structure that stores messages or requests that are sent and received by web services. A message queue allows asynchronous communication between web services, as it decouples the sender and the receiver, and enables them to process messages at different rates. A message queue also provides reliability, scalability, and load balancing for web services, as it ensures that messages are not lost, duplicated, or corrupted, and that they are distributed evenly among the available servers .
However, a message queue also has a limit on how many messages it can store at a time. This limit is determined by the configuration of the message queue length, which is the maximum number of messages that can be in the queue before it becomes full. If the message queue length is too short, the queue may fill up quickly and reject new messages, causing errors or delays in communication. If the message queue length is too long, the queue may consume too much memory or disk space, affecting the performance or availability of the web service .
Therefore, if an organization provides integration services for finance companies that use web services, and a new company that sends and receives more than 100,000 transactions per second has been integrated using the web service, the most likely cause of the issue is an incorrect configuration in the message queue length. The new company may have generated a large volume of messages that exceeded the capacity of the message queue, resulting in slowness for the other integrated companies. The organization should adjust the message queue length to accommodate the increased traffic and optimize the resource utilization of the web service.

NEW QUESTION 137
- (Topic 4)
A company is using a hybrid cloud environment. The private cloud is hosting the business applications, and the cloud services are being used to replicate for

availability purposes.
The cloud services are also being used to accommodate the additional resource requirements to provide continued services. Which of the following scalability models is the company utilizing?

A. Vertical scaling
B. Autoscaling
C. Cloud bursting
D. Horizontal scaling

Answer: C

Explanation:
Cloud bursting is a scalability model that allows a company to use a hybrid cloud environment to handle peak or unpredictable workloads. Cloud bursting involves using the private cloud to host the core or critical applications, and using the public cloud to provide additional or temporary resources when the demand exceeds the capacity of the private cloud .
Cloud bursting can help a company to:
Improve the availability and reliability of the applications by replicating them across multiple cloud platforms and locations .
Optimize the performance and efficiency of the applications by dynamically allocating and releasing resources based on the workload and traffic .
Reduce the cost and complexity of the IT infrastructure by leveraging the pay-as-you-go and on-demand models of the public cloud .

NEW QUESTION 138
- (Topic 4)
An organization is conducting a performance test of a public application. The following actions have already been completed:
• The baseline performance has been established.
• A load test has passed.
• A benchmark report has been generated.
Which of the following needs to be done to conclude the performance test?

A. Verify the application works well under an unexpected volume of requests.
B. Assess the application against vulnerabilities and/or misconfiguration exploitation.
C. Test how well the application can resist a DDoS attack.
D. Conduct a test with the end users and collect feedback.

Answer: A

Explanation:
To conclude the performance test of a public application, the organization needs to verify the application works well under an unexpected volume of requests. This is also known as a stress test, which is a type of performance test that evaluates the behavior and stability of the application under extreme conditions1. A stress test can help identify potential bottlenecks, errors, or failures that may occur when the application is subjected to a sudden surge or spike in demand2. A stress test can also help determine the maximum capacity and scalability of the application3.
References: CompTIA Cloud+ CV0-003 Exam Objectives, Objective 2.2: Given a scenario, deploy and test a cloud solution ; Performance Testing | Cloud Computing | CompTIA1 ; Stress Testing - Software Testing Fundamentals2 ; What is Stress Testing? Definition, Types, Tools & Examples3

NEW QUESTION 143
- (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 146
- (Topic 4)
A systems administrator notices the host filesystem is running out of storage space. Which of the following will best reduce the storage space on the system?

A. Deduplication
B. Compression
C. Adaptive optimization
D. Thin provisioning

Answer: A

Explanation:

Deduplication is a technique that reduces the storage space by eliminating duplicate data blocks and replacing them with pointers to the original data. Deduplication can help free up the host filesystem by removing redundant data and increasing the storage efficiency. Deduplication can be performed at the source or the target, and it can be applied at the file or block level. References: [CompTIA Cloud+ CV0-003 Certification Study Guide], Chapter 4, Objective 4.3: Given a scenario, troubleshoot common storage issues.

NEW QUESTION 147
- (Topic 4)
A cloud engineer recently set up a container image repository. The engineer wants to ensure that downloaded images are not modified in transit. Which of the following is the best method to achieve this goal?

A. SHA-256
B. IPSec
C. AES-256
D. MD5
E. serpent-256

Answer: A

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

NEW QUESTION 148
- (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 150
- (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 155

- (Topic 4)
A systems administrator is writing a script for provisioning nodes in the environment. Which of the following would be best for the administrator to use to provision the authentication credentials to the script?

A. password='curl https://10.2.3.4/api/sytemops?op=provision
B. password=$env_password
C. password=$ (cat /opt/app/credentials)
D. password="MyS3cretP4sswordIsVeryLong"

Answer: B

Explanation:
The best way to provision the authentication credentials to the script is to use an environment variable that stores the password. This way, the password is not exposed in plain text in the script, and it can be changed or updated without modifying the script. An environment variable is a dynamic value that can be accessed by processes or programs in the operating system. By using the syntax password=$env_password, the script can assign the value of the environment variable named env_password to the password variable. This is more secure and flexible than using a curl command, a file, or a hard-coded password in the script.
References: [CompTIA Cloud+ CV0-003 Certification Study Guide], Chapter 8, Objective 8.1: Given a scenario, implement cloud automation and orchestration.

NEW QUESTION 157
- (Topic 4)
An integration application that communicates between different application and database servers is currently hosted on a physical machine. A P2V migration needs to be done to reduce the hardware footprint. Which of the following should be considered to maintain the same level of network throughput and latency in the virtual server?

A. Upgrading the physical server NICs to support IOGbps
B. Adding more vCPU
C. Enabling SR-IOV capability
D. Increasing the VM swap/paging size

Answer: C

Explanation:
SR-IOV stands for Single Root Input/Output Virtualization, which is a technology that allows a physical device, such as a network interface card (NIC), to be shared by multiple virtual machines (VMs) without sacrificing performance or latency. By enabling SR-IOV capability, the integration application can communicate directly with the physical NIC, bypassing the hypervisor and the virtual switch, and reducing the network overhead and latency .

NEW QUESTION 161
- (Topic 4)
A cloud administrator is choosing a backup schedule for a new application platform that creates many small files. The backup process impacts the performance of the application, and backup times should be minimized during weekdays. Which of the following backup types best meets the weekday requirements?

A. Database dump
B. Differential
C. Incremental
D. Full

Answer: C

Explanation:
Incremental backups only back up the files that have changed since the last backup, which minimizes the backup time and the performance impact on the application. Differential backups back up all the files that have changed since the last full backup, which can take longer and consume more storage space. Database dump and full backups are not suitable for weekday requirements, as they back up the entire database or filesystem, which can be time-consuming and resource-intensive.
References: CompTIA Cloud+ CV0-003 Exam Objectives, Objective 3.3: Given a scenario, implement backup, restore, disaster recovery and business continuity solutions

NEW QUESTION 164
- (Topic 4)
A cloud administrator is supporting an application that has several reliability issues. The administrator needs visibility into the performance characteristics of the application. Which of the following will MOST likely be used in a reporting dashboard?

A. Data from files containing error messages from the application
B. Results from the last performance and workload testing
C. Detail log data from syslog files of the application
D. Metrics and time-series data measuring key performance indicators

Answer: D

Explanation:
The best answer is D. Metrics and time-series data measuring key performance indicators.
Metrics and time-series data are numerical values that represent the state and behavior of a system over time. They can measure key performance indicators (KPIs) such as availability, latency, throughput, error rate, and resource utilization. Metrics and time-series data can help a cloud administrator to monitor, analyze, and troubleshoot the performance characteristics of an application .
Metrics and time-series data are most likely to be used in a reporting dashboard, because they can provide a clear and concise overview of the application's performance. A reporting dashboard is a graphical user interface that displays the most important information about a system or a process in a single view. A reporting dashboard can help a cloud administrator to:
Visualize the trends and patterns of the metrics and time-series data using charts, graphs, tables, or gauges .
Compare the actual performance of the application with the expected or desired performance based on the defined service level objectives (SLOs) or service level agreements (SLAs) .
Identify and diagnose any performance issues or anomalies that may affect the reliability of the application .

Communicate and report the performance status and results to the stakeholders or customers.
The other options are not as likely to be used in a reporting dashboard, because they are either too detailed, too outdated, or too irrelevant for measuring the performance characteristics of the application. For example:
Data from files containing error messages from the application (A) may help to identify and debug some specific errors or exceptions that occur in the application. However, they are not sufficient to measure the overall performance or reliability of the application. They are also too verbose and unstructured to be displayed in a reporting dashboard.
Results from the last performance and workload testing (B) may help to evaluate and optimize the performance of the application under different scenarios and conditions. However, they are not representative of the current or real-time performance of the application in production. They are also too static and outdated to be displayed in a reporting dashboard.
Detail log data from syslog files of the application © may help to record and track the events and activities that happen in the application. However, they are not designed to measure the key performance indicators or metrics of the application. They are also too complex and voluminous to be displayed in a reporting dashboard.

NEW QUESTION 169
- (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 173
- (Topic 4)
A systems administrator is troubleshooting a VDI deployment that is used to run high- frame-rate rendering. Users are reporting frequent application crashes. After running a benchmark, the administrator discovers the following:

GPU utilization	30%
Video RAM utilization	99%
GPU mode	Mixed

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

A. Configure the GPU to run in compute mode.
B. Allocate more RAM in the VM template.
C. Select a higher vGPU profile.
D. Configure the GPU to run in graphics mode.

Answer: C

Explanation:
The benchmark results show that the video RAM utilization is at 99%, which is likely causing the application crashes. Video RAM is used to store graphics data and textures that are processed by the GPU. Selecting a higher vGPU profile can help allocate more video RAM to the virtual machines, which can help resolve this issue. A vGPU profile is a predefined configuration that specifies the amount of video RAM, the number of display heads, and the maximum resolution that a virtual machine can use. By selecting a higher vGPU profile, the administrator can increase the performance and stability of the high- frame-rate rendering application. References: [CompTIA Cloud+ CV0-003 Study Guide], Chapter 4, Objective 4.2: Given a scenario, troubleshoot common virtualization issues.

NEW QUESTION 177
- (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 179
- (Topic 4)
A VDI administrator is enhancing the existing environment with a feature to allow users to connect devices to virtual workstations. Which of the following types of devices are most likely to be allowed in the upgrade? (Select two).

A. Display monitors
B. USB devices
C. SATA devices
D. PCIe devices
E. PCI devices
F. Printers

Answer: BF

Explanation:
B. USB devices and F. Printers are most likely to be allowed in the upgrade. USB devices are common peripherals that users may want to connect to their virtual workstations, such as flash drives, keyboards, mice, webcams, etc. Printers are also useful devices that users may need to print documents from their virtual desktops. VDI software can support USB redirection and printer redirection to enable these devices to work with virtual workstations12.
Display monitors, SATA devices, PCIe devices, and PCI devices are less likely to be allowed in the upgrade, as they are either part of the physical hardware of the end device or the server, or they require direct access to the host system. VDI software typically does not support these types of devices, as they are not compatible with the virtualization layer or the remote display protocol34.
1: What is VDI? | Virtual Desktop Infrastructure | VMware 2: What Is Virtual Desktop Infrastructure (VDI)? | Microsoft Azure 3: What Is Virtual Desktop Infrastructure (VDI)? - Cisco 4: Best Virtual Desktop Infrastructure (VDI) Software in 2023 | G2

NEW QUESTION 182
- (Topic 4)
A cloud security engineer needs to design an IDS/IPS solution for a web application in a single virtual private network. The engineer is considering implementing IPS protection for traffic coming from the internet. Which of the following should the engineer consider to meet this requirement?

A. Configuring a web proxy server
B. Implementing load balancing using SSI- in front of web applications
C. Implementing IDS/IPS agents on each instance running in that virtual private network
D. Implementing dynamic routing

Answer: C

Explanation:
An Intrusion Detection System (IDS) is a software or hardware system that monitors network traffic for malicious activity and alerts the administrator of any potential threats.
An Intrusion Prevention System (IPS) is a software or hardware system that not only detects but also blocks or mitigates the malicious activity. Both IDS and IPS are essential for securing a web application in a cloud environment1.
A web proxy server is a server that acts as an intermediary between the client and the web server. It can provide caching, filtering, and authentication services, but it does not offer IDS/IPS functionality. Therefore, option A is incorrect.
Load balancing using SSI (Server Side Includes) is a technique that distributes the workload among multiple web servers by inserting dynamic content into web pages. It can improve the performance and availability of a web application, but it does not provide IDS/IPS protection. Therefore, option B is incorrect.
Implementing IDS/IPS agents on each instance running in that virtual private network is a valid solution for providing IPS protection for traffic coming from the internet. The agents can monitor and inspect the network traffic on each instance and block or report any suspicious activity to a central management console. This can prevent attacks from reaching the web application or spreading to other instances in the same network. Therefore, option C is correct.
Implementing dynamic routing is a technique that allows routers to select the best path for forwarding packets based on network conditions. It can enhance the reliability and efficiency of a network, but it does not offer IDS/IPS functionality. Therefore, option D is incorrect.

NEW QUESTION 187
- (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 192
- (Topic 4)
A cloud administrator is performing automated deployment of cloud infrastructure for clients. The administrator notices discrepancies from the baseline in the configuration of infrastructure that was deployed to a new client. Which of the following is most likely the cause?

A. The deployment user account changed
B. The deployment was done to a different resource group.
C. The deployment was done by a different cloud administrator.
D. The deployment template was modified.

Answer: D

Explanation:
A deployment template is a file that defines the resources and configurations that are required to deploy a cloud solution1. A deployment template can be used to automate the deployment of cloud infrastructure for clients, ensuring consistency and efficiency2. However, if the deployment template was modified, either intentionally or accidentally, it could cause discrepancies from the baseline in the configuration of infrastructure that was deployed to a new client. For example, the template could have different parameters, values, or dependencies that affect the outcome of the deployment3. Therefore, the most likely cause of the issue is that the deployment template was modified. References:
1: What is a template? - Azure Resource Manager | Microsoft Docs3
2: Automate cloud deployments with Azure Resource Manager templates - Learn | Microsoft Docs3
3: CompTIA Cloud+ CV0-003 Exam Objectives, Objective 2.2: Given a scenario, deploy and test a cloud solution

NEW QUESTION 196
- (Topic 3)
A technician deployed a VM with NL-SAS storage to host a critical application. Two weeks later, users have begun to report high application latency. Which of the following is the BEST action to correct the latency issue?

A. Increase the capacity of the data storage.
B. Migrate the data to SAS storage.
C. Increase the CPU of the VM.
D. Migrate the data to flash storage.

Answer: D

Explanation:
The correct answer is D. Migrate the data to flash storage. Flash storage is a type of solid- state storage that uses flash memory to store data. Flash storage has much faster performance and lower latency than NL-SAS storage, which is a type of hard disk drive that uses nearline serial attached SCSI interface. According to the web search results, NL-SAS devices have much higher response times than flash devices123. Therefore, migrating the data to flash storage can reduce the application latency and improve the user experience. Increasing the capacity of the data storage, migrating the data to SAS storage, or increasing the CPU of the VM are not likely to solve the latency issue, as they do not address the root cause of the problem, which is the slow performance of NL-SAS storage. For more information on flash storage and its benefits, you can refer to the Dell EMC Unity: FAST Technology Overview2 or the Dell Technologies website4.

NEW QUESTION 200
- (Topic 3)
A systems administrator is setting up a backup solution to follow the 3-2-1 policy. Currently, the solution is set to back up from the servers to an on-site storage server. Which of the following should the administrator configure to comply with the 3-2-1 policy?

A. Weekly lull backups, with daily incremental backups
B. A second on-site storage server for backups
C. Storage snapshots
D. An off-site storage server for backups

Answer: D

Explanation:
The 3-2-1 backup policy states that there should be three copies of data, stored on two different media, with one copy being off-site. The current backup solution only has one copy of data on one media (the on-site storage server). To comply with the 3- 2-1 policy, the systems administrator should configure an off-site storage server for backups, which will provide another copy of data on a different media and location. Reference: CompTIA Cloud+ Certification Exam Objectives, Domain 3.0 Maintenance, Objective 3.2 Given a scenario, implement backup, restore, disaster recovery and business continuity measures.

NEW QUESTION 203
- (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 206
- (Topic 3)
An organization recently deployed a private cloud on a cluster of systems that delivers compute, network, and storage resources in a single hardware, managed by an intelligent software. Which of the following BEST describes this type of deployment?

A. High-performance computing
B. Hyperconverged infrastructure
C. Stand-alone computing
D. Dynamic allocations

Answer: B

Explanation:
Hyperconverged infrastructure (HCI) is a type of deployment that combines compute, network, and storage resources in a single hardware appliance that is managed by an intelligent software layer. HCI simplifies the configuration and management of cloud resources, reduces hardware costs and complexity, and improves scalability and performance. Reference: CompTIA Cloud+ Certification Exam Objectives, Domain 1.0 Configuration and Deployment, Objective 1.2 Given a scenario involving requirements for deploying an application in the cloud, select an appropriate solution design.

NEW QUESTION 211
- (Topic 3)
A cloud administrator is troubleshooting a highly available web application running within three containers behind a Layer 7 load balancer with a WAF inspecting all traffic. The application frequently asks the users to log in again even when the session timeout has not been reached. Which of the following should the cloud administrator configure to solve this issue?

A. Firewall outbound rules
B. Firewall inbound rules
C. Load balancer certificates
D. Load balancer stickiness
E. WAF transaction throttling

Answer: D

Explanation:
Reference: https://docs.aws.amazon.com/elasticloadbalancing/latest/application/application-load- balancers.html#sticky-sessions
Load balancer stickiness is what the cloud administrator should configure to solve the issue of the application frequently asking the users to log in again even when the session timeout has not been reached for a highly available web application running within three containers behind a Layer 7 load balancer with a WAF inspecting all traffic. Load balancer stickiness is a feature that allows customers to maintain user sessions or connections with the same server or node that provides a service or function, such as a web application, database, etc., even when there are multiple servers or nodes behind a load balancer. Load balancer stickiness can solve the issue by providing benefits such as:
Consistency: Load balancer stickiness can provide consistency by ensuring that users receive the same service or function from the same server or node throughout their session or connection, without any changes or variations.
Performance: Load balancer stickiness can provide performance by reducing the latency or overhead of switching between different servers or nodes during a session or connection, which may cause delays or errors.
Security: Load balancer stickiness can provide security by preserving and protecting user authentication or authorization information on the same server or node during a session or connection, without exposing or transferring it to other servers or nodes.

NEW QUESTION 216
- (Topic 3)
A systems administrator deployed a new application release to the green stack of a blue- green infrastructure model and made the green stack primary. Immediately afterward, users began reporting application issues. The systems administrator must take action to bring the service online as quickly as possible. Which of the following is the FASTEST way to restore the service?

A. Reboot all the servers in the green stack
B. Failback to the blue stack
C. Restore from backups
D. Troubleshoot and resolve the application issues

Answer: B

Explanation:
The fastest way to restore the service after deploying a new application release to the green stack of a blue-green infrastructure model and making the green stack primary is to failback to the blue stack. Failing back means switching back to the previous version of the application that is running on the blue stack, which is still available and functional. This will minimize the downtime and impact on the users, while allowing the systems administrator to troubleshoot and fix the issues on the green stack. Reference: [CompTIA Cloud+ Certification Exam Objectives], Domain 4.0 Troubleshooting, Objective 4.4 Given a scenario, troubleshoot deployment issues.

NEW QUESTION 219
- (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 224
- (Topic 3)
A systems administrator is working on the backup schedule for a critical business application that is running in a private cloud. Which of the following would help the administrator schedule the frequency of the backup job?

A. RPO
B. MTTR
C. SLA
D. RTO

Answer: A

Explanation:
RPO (Recovery Point Objective) is what would help the administrator schedule the frequency of the backup job for a critical business application that is running in a private cloud. RPO is a metric that measures how much data can be lost or how far back in time a recovery point can be without causing significant impact or damage. RPO can help to schedule the frequency of the backup job by determining how often backups should be performed to minimize data loss in case of a disruption or disaster.

NEW QUESTION 227
- (Topic 3)
A cloud administrator implemented SSO and received a business requirement to increase security when users access the cloud environment. Which of the following should be implemented NEXT to improve the company's security posture?

A. SSH
B. MFA
C. Certificates
D. Federation

Answer: B

Explanation:
MFA (Multi-Factor Authentication) is a security technique that requires the user to present two or more pieces of evidence to prove their identity when they try to access a system or an application. For example, a password and a physical token, or a fingerprint and a one-time code. MFA can improve the company’s security posture by preventing unauthorized access even if the password or single-factor authentication is compromised, as the attacker would also need to have the other factors to log
in. According to the web search results, MFA can prevent 99.9% of account attacks1.
SSO (Single Sign-On) is a system that allows the user to use one set of login credentials to access multiple systems and applications that previously may have each required their own logins. SSO can improve productivity and user convenience, but it does not replace MFA. In fact, SSO works in conjunction with MFA, as it can enforce MFA for all the systems and applications that are integrated with SSO2. Therefore, implementing SSO does not mean that MFA is not needed.

NEW QUESTION 230
- (Topic 3)
While investigating network traffic, a cloud administrator discovers the monthly billing has increased substantially. Upon further review, it appears the servers have been compromised, and sensitive files have been exfiltrated. Which of the following can be implemented to maintain data confidentiality?

A. Hardening
B. IAM
C. Encryption
D. IPSec

Answer: C

Explanation:
The best method to maintain data confidentiality after discovering that the servers have been compromised and sensitive files have been exfiltrated is encryption. Encryption is a process that transforms data into an unreadable format using an algorithm and a key. Encryption can protect data at rest, in transit, or in use from unauthorized access, tampering, or leakage. The systems administrator should encrypt the sensitive files and their backups using strong encryption algorithms and keys, and also encrypt the network traffic using protocols such as SSL or IPSec. 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 232
- (Topic 3)
An organization has a public-facing API that is hosted on a cloud provider. The API performs slowly at times. Which of the following technologies should the cloud administrator apply to provide speed acceleration and a secure connection?

A. WAF
B. EDR
C. IDS
D. HIPS
E. SSL

Answer: E

Explanation:

The best technology to provide speed acceleration and a secure connection for a public-facing API that is hosted on a cloud provider is SSL (Secure Sockets Layer). SSL is a protocol that encrypts and authenticates the data between a client and a server over an HTTP connection. It also compresses the data to reduce its size and improve its transmission speed. SSL can enhance the security and performance of an API by preventing unauthorized access, tampering, or interception of the data. Reference: [CompTIA Cloud+ Certification Exam Objectives], Domain 2.0 Security, Objective 2.2 Given a scenario, implement appropriate network security controls for a cloud environment.

NEW QUESTION 233
- (Topic 3)
A security audit related to confidentiality controls found the following transactions occurring in the system:
GET
http://gateway.securetransaction.com/privileged/api/v1/changeResource?id=123&user=277 Which of the following solutions will solve the audit finding?

A. Using a TLS-protected API endpoint
B. Implementing a software firewall
C. Deploying a HIDS on each system
D. Implementing a Layer 4 load balancer

Answer: A

Explanation:
Reference: https://cheatsheetseries.owasp.org/cheatsheets/Transport_Layer_Protection_Cheat_Sheet
.html
The audit finding is related to confidentiality, which means the data should be protected from unauthorized access. The current API endpoint is using HTTP, which is not secure and can expose the data in transit. Using a TLS-protected API endpoint would encrypt the data and prevent anyone from reading it. Reference: CompTIA Cloud+ Certification Exam Objectives, Domain 2.0 Security, Objective 2.1 Given a scenario, apply security configurations and compliance controls to meet cloud security requirements.

NEW QUESTION 234
- (Topic 3)
An administrator manages a file server that has a lot of users accessing and creating many files. As a result, the storage consumption is growing quickly. Which of the following would BEST control storage usage?

A. Compression
B. File permissions
C. User quotas
D. Access policies

Answer: C

Explanation:
User quotas are a feature that allows the administrator to limit the amount of storage space that a user or a group of users can consume on a file server. User quotas can help to control storage usage by preventing users from storing excessive or unnecessary files, as well as by enforcing fair and consistent storage policies across the organization. User quotas can also help to monitor and report on the storage consumption and trends of the users, and alert the administrator or the users when they are approaching or exceeding their quota limits.

NEW QUESTION 238
- (Topic 3)
A cloud administrator is configuring several security appliances hosted in the private IaaS environment to forward the logs to a central log aggregation solution using syslog. Which of the following firewall rules should the administrator add to allow the web servers to connect to the central log collector?

A. Allow UDP 161 outbound from the web servers to the log collector .
B. Allow TCP 514 outbound from the web servers to the log collector.
C. Allow UDP 161 inbound from the log collector to the web servers .
D. Allow TCP 514 inbound from the log collector to the web servers .

Answer: B

Explanation:
As mentioned in the question, the security appliances are using syslog to forward the logs to a central log aggregation solution. According to the web search results, syslog is a protocol that runs over UDP port 514 by default, or TCP port 6514 for secure and reliable transport1. However, some implementations of syslog can also use TCP port 514 for non-secure transport2. Therefore, to allow the web servers to connect to the central log collector using syslog over TCP, the firewall rule should allow TCP 514 outbound from the web servers to the log collector.

NEW QUESTION 240
- (Topic 3)
A systems administrator is helping to develop a disaster recovery solution. The solution
must ensure all production capabilities are available within two hours. Which of the following will BEST meet this requirement?

A. A hot site
B. A warm site
C. A backup site
D. A cold site

Answer: A

Explanation:
Reference: https://searchdisasterrecovery.techtarget.com/definition/hot-site
A hot site is what would best meet the requirement of ensuring all production capabilities are available within two hours for a disaster recovery solution. A disaster recovery solution is a plan or process of restoring normal operation and performance of a system or service after a disruption or disaster. A disaster recovery

solution can use different types of sites or locations to store and recover data or resources, such as:
A hot site: This is a site or location that has a fully operational and ready-to-use replica or copy of the original system or service, including data, resources, applications, etc. A hot site can provide benefits such as:
Availability: A hot site can provide availability by ensuring that the system or service can be switched or transferred to the hot site immediately or within minutes after a disruption or disaster, without any downtime or interruption.
Capability: A hot site can provide capability by ensuring that the system or service can function and perform at the same level or quality as the original system or service, without any loss or degradation.
A warm site: This is a site or location that has a partially operational and ready-to-use replica or copy of the original system or service, including some data, resources, applications, etc. A warm site can provide benefits such as:
Affordability: A warm site can provide affordability by reducing the cost of maintaining and updating the replica or copy of the original system or service, compared to a hot site.
Flexibility: A warm site can provide flexibility by allowing customers to customize and configure the replica or copy of the original system or service according to their needs and preferences, compared to a hot site.
A cold site: This is a site or location that has no operational and ready-to-use replica or copy of the original system or service, but only has the necessary infrastructure or facilities to support it, such as power, network, space, etc. A cold site can provide benefits such as:
Scalability: A cold site can provide scalability by enabling customers to expand and grow their replica or copy of the original system or service as needed, without any limitations or constraints.
Security: A cold site can provide security by minimizing the exposure or risk of the replica or copy of the original system or service to any threats or attacks, compared to a hot site or a warm site

NEW QUESTION 241
- (Topic 3)
A systems administrator wants to restrict access to a set of sensitive files to a specific group of users. Which of the following will achieve the objective?

A. Add audit rules on the server
B. Configure data loss prevention in the environment
C. Change tine permissions and ownership of the files
D. Implement a HIPS solution on the host

Answer: C

Explanation:
The best way to restrict access to a set of sensitive files to a specific group of users is to change the file permissions and ownership of the files. File permissions and ownership are attributes that determine who can read, write, execute, or modify the files. By changing the file permissions and ownership, the systems administrator can grant or deny access to the files based on the user identity or group membership.
Reference: CompTIA Cloud+ Certification Exam Objectives, Domain 2.0 Security, Objective 2.3 Given a scenario, implement appropriate access control measures for a cloud environment.

NEW QUESTION 242
- (Topic 3)
A DevOps administrator is building a new application slack in a private cloud. This application will store sensitive information and be accessible from the internet. Which of the following would be MOST useful in maintaining confidentiality?

A. NAC
B. IDS
C. DLP
D. EDR

Answer: C

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

NEW QUESTION 244
- (Topic 3)
A financial industry services firm was the victim of an internal data breach, and the perpetrator was a member of the company's development team. During the investigation, one of the security administrators accidentally deleted the perpetrator's user data. Even though the data is recoverable, which of the following has been violated?

A. Chain of custody
B. Evidence acquisition
C. Containment
D. Root cause analysis

Answer: A

Explanation:
The chain of custody is a process that documents and preserves the integrity and authenticity of evidence from the time it is collected until it is presented in court. The chain of custody includes information such as who collected, handled, stored, or transferred the evidence, when and where it was done, and how it was done. By accidentally deleting the perpetrator’s user data, the security administrator has violated the chain of custody, as the evidence has been altered or destroyed and can no longer be used in court. 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 245
- (Topic 3)

During a security incident, an laaS compute instance is detected to send traffic to a host related to cryptocurrency mining. The security analyst handling the incident determines the scope of the incident is limited to that particular instance. Which of the following should the security analyst do NEXT?

A. Isolate the instance from the network into quarantine.
B. Perform a memory acquisition in the affected instance.
C. Create a snapshot of the volumes attached to the instance.
D. Replace the instance with another from the baseline.

Answer: A

Explanation:
The first step in incident response is to contain the incident activities and attackers, which means preventing them from spreading to other systems or causing more damage. In this case, the security analyst should isolate the instance from the network into quarantine, which means cutting off its communication with other hosts and services. This will stop the cryptocurrency mining activity and prevent the attacker from accessing the instance remotely. Isolating the instance also preserves the evidence for further analysis and investigation.

NEW QUESTION 250
- (Topic 2)
An organization is currently deploying a private cloud model. All devices should receive the time from the local environment with the least administrative effort. Which of the following ports needs to be opened to fulfill this requirement?

A. 53
B. 67
C. 123
D. 161

Answer: C

Explanation:
Reference: https://www.sciencedirect.com/topics/computer-science/network-time-protocol#:~:text=NTP%20is%20a%20built%2Don,for%20example%2C%20a%20desktop).
Port 123 is what needs to be opened to ensure all devices receive the time from the local environment with the least administrative effort in a private cloud model. Port 123 is the port used by NTP (Network Time Protocol), which is a protocol that synchronizes the clocks of network devices and systems. NTP can help to ensure accurate and consistent time across different devices and systems in a cloud environment, which can facilitate coordination, communication, logging, auditing, etc.

NEW QUESTION 252
- (Topic 2)
To save on licensing costs, the on-premises, IaaS-hosted databases need to be migrated to a public DBaaS solution. Which of the following would be the BEST technique?

A. Live migration
B. Physical-to-virtual
C. Storage-level mirroring
D. Database replication

Answer: D

Explanation:
Database replication is the best technique to migrate databases from an on- premises IaaS-hosted environment to a public DBaaS solution. Database replication is a process of copying data from one database server to another database server in real-time or near real-time. Database replication can ensure data consistency and availability across different locations and platforms. Database replication can facilitate migration by synchronizing data between on-premises databases and cloud databases.

NEW QUESTION 256
.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons and Answers in PDF Format

CV0-003 Practice Exam Features:

* CV0-003 Questions and Answers Updated Frequently

* CV0-003 Practice Questions Verified by Expert Senior Certified Staff

* CV0-003 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* CV0-003 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year