CompTIA

Exam Questions CV0-003

CompTIA Cloud+ Certification Exam

NEW QUESTION 1
- (Topic 1)
A systems administrator has migrated an internal application to a public cloud. The new web server is running under a TLS connection and has the same TLS certificate as the internal application that is deployed. However, the IT department reports that only internal users who are using new versions of the OSs are able to load the application home page.
Which of the following is the MOST likely cause of the issue?

A. The local firewall from older OSs is not allowing outbound connections
B. The local firewall from older OSs is not allowing inbound connections
C. The cloud web server is using a self-signed certificate that is not supported by older browsers
D. The cloud web server is using strong ciphers that are not supported by older browsers

Answer: D

Explanation:
Ciphers are algorithms or methods that are used to encrypt and decrypt data for secure communication. Strong ciphers are ciphers that use high-level encryption techniques and keys to provide stronger security and protection for data. The cloud web server is using strong ciphers that are not supported by older browsers is the most likely cause of the issue of only internal users who are using new versions of the OSs being able to load the application home page after the administrator configured a redirect from HTTP to HTTPS on the web server. Older browsers may not support the strong ciphers used by the cloud web server for HTTPS connections, which can result in a failure to establish a secure connection and load the application home page. References: CompTIA Cloud+ Certification Exam Objectives, page 15, section 2.8

NEW QUESTION 2
- (Topic 1)
Which of the following strategies will mitigate the risk of a zero-day vulnerability MOST efficiently?

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

Answer: D

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

NEW QUESTION 3
- (Topic 1)
A DevOps administrator is automating an existing software development workflow. The administrator wants to ensure that prior to any new code going into production, tests confirm the new code does not negatively impact existing automation activities.
Which of the following testing techniques would be BEST to use?

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

Answer: B

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

NEW QUESTION 4
- (Topic 1)
An SQL injection vulnerability was reported on a web application, and the cloud platform
team needs to mitigate the vulnerability while it is corrected by the development team. Which of the following controls will BEST mitigate the risk of exploitation?

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

Answer: D

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

NEW QUESTION 5
- (Topic 1)
A SAN that holds VM files is running out of storage space.
Which of the following will BEST increase the amount of effective storage on the SAN?

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

Answer: D

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

NEW QUESTION 6
- (Topic 1)
A systems administrator is deploying a GPU-accelerated VDI solution. Upon requests from several users, the administrator installs an older version of the OS on their virtual workstations. The majority of the VMs run the latest LTS version of the OS.
Which of the following types of drivers will MOST likely ensure compatibility will all virtual workstations?

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

Answer: D

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

NEW QUESTION 7
- (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 8
- (Topic 1)
A company wants to implement business continuity, and the cloud solution architect needs to design the correct solution.
Which of the following will provide the data to measure business continuity? (Choose two.)

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

Answer: AF

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

NEW QUESTION 9
- (Topic 1)
An organization is implementing a new requirement to facilitate users with faster downloads of corporate application content. At the same time, the organization is also expanding cloud regions.
Which of the following would be suitable to optimize the network for this requirement?

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

Answer: C

Explanation:

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

NEW QUESTION 10
- (Topic 1)
A cloud administrator is switching hosting companies and using the same script that was previously used to deploy VMs in the new cloud. The script is returning errors that the command was not found.
Which of the following is the MOST likely cause of the script failure?

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

Answer: C

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

NEW QUESTION 10
- (Topic 1)
A cloud administrator has built a new private cloud environment and needs to monitor all computer, storage, and network components of the environment.
Which of the following protocols would be MOST useful for this task?

A. SMTP
B. SCP
C. SNMP
D. SFTP

Answer: C

Explanation:
Simple Network Management Protocol (SNMP) is a protocol that enables monitoring and managing network devices and components in an IP network. SNMP can help monitor all computer, storage, and network components of a private cloud environment, as it can collect and report information about their status, performance, configuration, and events. SNMP can also help troubleshoot and optimize the private cloud environment, as it can detect and alert any issues or anomalies related to the network devices and components. References: CompTIA Cloud+ Certification Exam Objectives, page 15, section 2.8

NEW QUESTION 14
- (Topic 1)
A company wants to check its infrastructure and application for security issues regularly. Which of the following should the company implement?

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

Answer: C

Explanation:
Vulnerability testing is a type of testing that identifies and evaluates the weaknesses or flaws in a system or application that could be exploited by attackers. Vulnerability testing can help check the infrastructure and application for security issues regularly, as it can reveal the potential risks and exposures that may compromise the confidentiality, integrity, or availability of the system or application. Vulnerability testing can also help remediate or mitigate the vulnerabilities by providing recommendations or solutions to fix or reduce them. References: CompTIA Cloud+ Certification Exam Objectives, page 19, section 4.1
Reference: https://pure.security/services/technical-assurance/external-penetration-testing/

NEW QUESTION 17
- (Topic 1)
A cloud administrator recently deployed an update to the network drivers of several servers. Following the update, one of the servers no longer responds to remote

login requests. The cloud administrator investigates the issue and gathers the following information:
? The cloud management console shows the VM is running and the CPU and memory utilization is at or near 0%.
? The cloud management console does not show an IP address for that server.
? A DNS lookup shows the hostname resolves to an IP address.
? The server is a member of the same security group as the others.
? The cloud administrator is able to log in remotely to the other servers without issue.
Which of the following is the MOST likely cause of the server being unavailable?

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

Answer: A

NEW QUESTION 20
- (Topic 1)
A company is switching from one cloud provider to another and needs to complete the migration as quickly as possible.
Which of the following is the MOST important consideration to ensure a seamless migration?

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

Answer: C

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

NEW QUESTION 22
- (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 24
- (Topic 1)
A systems administrator needs to configure a set of policies to protect the data to comply with mandatory regulations.
Which of the following should the administrator implement to ensure DLP efficiently prevents the exposure of sensitive data in a cloud environment?

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

Answer: C

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

NEW QUESTION 29
- (Topic 1)
A systems administrator is troubleshooting performance issues with a Windows VDI environment. Users have reported that VDI performance is very slow at the start of the workday, but the performance is fine during the rest of the day. Which of the following is the MOST likely cause of the issue? (Choose two.)

A. Disk I/O limits
B. Affinity rule
C. CPU oversubscription

D. RAM usage
E. Insufficient GPU resources
F. License issues

Answer: AC

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

NEW QUESTION 30
- (Topic 1)
In an existing IaaS instance, it is required to deploy a single application that has different versions.
Which of the following should be recommended to meet this requirement?

A. Deploy using containers
B. Install a Type 2 hypervisor
C. Enable SR-IOV on the host
D. Create snapshots

Answer: A

Explanation:
Containers are a type of deployment technology that packages an application and its dependencies into a lightweight and portable unit that can run on any platform or environment. Containers can help deploy a single application that has different
versions in an existing IaaS instance, as they can isolate and run multiple versions of the same application without any conflicts or interference. Containers can also enable faster and easier deployment, scaling, and management of cloud-based applications. References: CompTIA Cloud+ Certification Exam Objectives, page 11, section 1.6

NEW QUESTION 33
- (Topic 1)
A cloud administrator is reviewing a new application implementation document. The administrator needs to make sure all the known bugs and fixes are applied, and unwanted
ports and services are disabled.
Which of the following techniques would BEST help the administrator assess these business requirements?

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

Answer: D

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

NEW QUESTION 38
- (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 40
- (Topic 1)
A cloud administrator is setting up a DR site on a different zone of the same CSP. The application servers are replicated using the VM replication, and the database replication is set up using log shipping. Upon testing the DR site, the application servers are unable to access the database servers. The administrator has verified the systems are running and are accessible from the CSP portal.
Which of the following should the administrator do to fix this issue?

A. Change the database application IP
B. Create a database cluster between the primary site and the DR site
C. Update the connection string

D. Edit the DNS record at the DR site for the application servers

Answer: C

Explanation:
A connection string is a parameter that specifies how to connect to a database server or instance. A connection string typically includes information such as the server name, database name, user name, password, and other options. Updating the connection string is the best way to fix the issue of application servers being unable to access the database servers after setting up a DR site on a different zone of the same CSP and replicating the application and database servers using VM replication and log shipping. Updating the connection string can ensure that the application servers can connect to the correct database server or instance in the DR site, as the server name or IP address may have changed after the replication. References: CompTIA Cloud+ Certification Exam Objectives, page 10, section 1.5

NEW QUESTION 44
- (Topic 1)
A company recently subscribed to a SaaS collaboration service for its business users. The company also has an on-premises collaboration solution and would like users to have a seamless experience regardless of the collaboration solution being used.
Which of the following should the administrator implement?

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

Answer: D

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

NEW QUESTION 47
- (Topic 2)
A vendor is installing a new retail store management application for a customer. The application license ensures software costs are low when the application is not being used, but costs go up when use is higher.
Which of the following licensing models is MOST likely being used?

A. Socket-based
B. Core-based
C. Subscription
D. Volume-based

Answer: D

Explanation:
Volume-based licensing is a pricing model that charges the customers based on the amount of usage or consumption of a software product or service. The more the customers use the software, the higher the costs will be. This model is suitable for applications that have variable or seasonal demand patterns. Examples of volume-based licensing are AWS Lambda, Azure Functions, Google Cloud Run, etc.

NEW QUESTION 49
- (Topic 2)
Which of the following should be considered for capacity planning?

A. Requirements, licensing, and trend analysis
B. Laws and regulations
C. Regions, clusters, and containers
D. Hypervisors and scalability

Answer: A

Explanation:
These are the factors that should be considered for capacity planning in a cloud environment. Capacity planning is a process of estimating and allocating the necessary resources and performance to meet the current and future demands of cloud applications or services. Capacity planning can help to optimize costs, efficiency, and reliability of cloud resources or services. The factors that should be considered for capacity planning are:
? Requirements: These are the specifications or expectations of the cloud applications or services, such as functionality, availability, scalability, security, etc. Requirements can help to determine the type, amount, and quality of resources or services needed to meet the objectives and goals of the cloud applications or services.
? Licensing: This is the agreement or contract that grants customers the right to use or access certain cloud resources or services for a specific period or fee. Licensing can affect the cost, availability, and compliance of cloud resources or services. Licensing can help to determine the budget, duration, and scope of using or accessing cloud resources or services.
? Trend analysis: This is the technique of analyzing historical and current data to identify patterns, changes, or fluctuations in demand or usage of cloud resources or services. Trend analysis can help to predict and anticipate future demand or usage of cloud resources or services, as well as identify any opportunities or challenges that may arise.

NEW QUESTION 54
- (Topic 2)
A cloud architect is reviewing four deployment options for a new application that will be hosted by a public cloud provider. The application must meet an SLA that allows for no
more than five hours of downtime annually. The cloud architect is reviewing the SLAs for the services each option will use:

Option A		Option B	
VM servers	99.00%	Container hosting	99.90%
Attached block storage	99.99%	Shared network storage	99.90%
Total uptime	99.00%	Total uptime	99.90%

Option C		Option D	
Container deployment services	99.95%	Container application services	99.99%
Attached block storage	99.99%	Shared network storage	99.99%
Total uptime	99.95%	Total uptime	99.99%

Based on the information above, which of the following minimally complies with the SLA requirements?

A. Option A
B. Option B
C. Option C
D. Option D

Answer: B

Explanation:
Option B is what minimally complies with the SLA (Service Level Agreement) requirements of allowing for no more than five hours of downtime annually for a new application that will be hosted by a public cloud provider. An SLA is a contract or agreement that defines the level of service or performance that a customer expects from a provider, such as availability, reliability, scalability, security, etc. An SLA can help to measure and monitor the quality and satisfaction of service or performance, as well as identify any penalties or rewards for meeting or failing to meet the SLA. Option B minimally complies with the SLA requirements by using services that have availability percentages that are equal to or higher than 99.95%, which translates to no more than five hours of downtime annually. Option B uses services such as:
? Compute: This is a service that provides computing resources such as servers, processors, memory, etc., to run applications or functions. Option B uses compute service with availability percentage of 99.95%, which means that it guarantees to be available for 99.95% of the time in a year, and allows for no more than five hours of downtime in a year.
? Storage: This is a service that provides storage resources such as disks, volumes, files, etc., to store data or information. Option B uses storage service with availability percentage of 99.99%, which means that it guarantees to be available for 99.99% of the time in a year, and allows for no more than one hour of downtime in a year.
? Database: This is a service that provides database resources such as tables, records, queries, etc., to store and retrieve data or information. Option B uses database service with availability percentage of 99.95%, which means that it guarantees to be available for 99.95% of the time in a year, and allows for no more than five hours of downtime in a year.

NEW QUESTION 58
- (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 59
- (Topic 2)
A systems administrator adds servers to a round-robin, load-balanced pool, and then starts receiving reports of the website being intermittently unavailable. Which of the following is the MOST likely cause of the issue?

A. The network is being saturated.
B. The load balancer is being overwhelmed.
C. New web nodes are not operational.
D. The API version is incompatible.
E. There are time synchronization issues.

Answer: C

Explanation:
New web nodes are not operational is the most likely cause of the issue of website being intermittently unavailable after adding servers to a round-robin, load-balanced pool. A round-robin, load-balanced pool is a method of distributing network traffic evenly and sequentially among multiple servers or nodes that provide the same service or function. A round-robin, load-balanced pool can help to improve performance, availability, and scalability of network applications or services by ensuring that no server or node is overloaded or underutilized. New web nodes are not operational if they are not configured properly or functioning correctly to provide web service or function. New web nodes are not operational can cause website being intermittently unavailable by disrupting the round- robin, load-balanced pool and creating inconsistency or unreliability in web service or function.

NEW QUESTION 64

- (Topic 2)
A system administrator has provisioned a new web server. Which of the following, in combination, form the best practice to secure the server's OS? (Choose three.)

A. Install TLS certificates on the server.
B. Forward port 80 traffic to port 443.
C. Disable TLS 1.0/1.1 and SSL.
D. Disable password authentication.
E. Enable SSH key access only.
F. Provision the server in a separate VPC.
G. Disable the superuser/administrator account.
H. Restrict access on port 22 to the IP address of the administrator's workstation.

Answer: ADE

Explanation:
These are the best practices to secure the OS of a new web server that has been provisioned in a cloud environment:
? Install TLS certificates on the server: TLS (Transport Layer Security) certificates are digital 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. Installing TLS certificates on the web server can encrypt and secure web traffic between the server and the clients, as well as prevent spoofing or impersonation attacks.
? Disable password authentication: Password authentication is a method of verifying and authenticating users or devices based on passwords or other credentials. Password authentication can be insecure or vulnerable to attacks such as brute force, dictionary, phishing, etc., especially if passwords are weak, reused, or compromised. Disabling password authentication can enhance security by preventing unauthorized or malicious access to the web server using passwords.
? Enable SSH key access only: SSH key access is a method of verifying and authenticating users or devices based on digital keys issued by a trusted authority. SSH key access can provide more security and convenience than password authentication, as it does not require users or devices to remember or enter passwords every time they access the web server. Enabling SSH key access only can ensure that only authorized or trusted users or devices can access the web server using keys.

NEW QUESTION 67
- (Topic 2)
A cloud administrator has been using a custom VM deployment script. After three months of use, the script no longer joins the LDAP domain. The cloud administrator verifies the account has the correct permissions. Which of the following is the MOST likely cause of the failure?

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

Answer: D

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

NEW QUESTION 68
- (Topic 2)
Users are experiencing slow response times from an intranet website that is hosted on a cloud platform. There is a site-to-site VPN connection to the cloud provider over a link of 100Mbps.
Which of the following solutions will resolve the issue the FASTEST?

A. Change the connection to point-to-site VPN
B. Order a direct link to the provider
C. Enable quality of service
D. Upgrade the link to 200Mbps

Answer: B

Explanation:
Ordering a direct link to the provider is the fastest solution to resolve the issue of slow response times from an intranet website that is hosted on a cloud platform. A direct link is a dedicated, high-bandwidth, low-latency connection between the customer's network and the cloud provider's network. It bypasses the public internet and provides better performance, security, and reliability. Examples of direct links are AWS Direct Connect, Azure ExpressRoute, Google Cloud Interconnect, etc.

NEW QUESTION 71
- (Topic 2)
An update is being deployed to a web application, and a systems administrator notices the cloud SQL database has stopped running. The VM is responding to pings, and there were not any configuration changes scheduled for the VM. Which of the following should the administrator check NEXT?

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

Answer: A

Explanation:
Checking the logs on the VM is the next step that the administrator should take if the cloud SQL database has stopped running after an update deployment. Logs

are records of events and activities that occur on a system or application. Logs can provide useful information for troubleshooting and identifying the root cause of an issue. The administrator should look for any errors, warnings, or messages that indicate what happened to the SQL database service and why it stopped running.

NEW QUESTION 75
- (Topic 2)
A company is currently running a website on site. However, because of a business requirement to reduce current RTO from 12 hours to one hour, and the RPO from one day to eight hours, the company is considering operating in a hybrid environment. The website uses mostly static files and a small relational database. Which of the following should the cloud architect implement to achieve the objective at the LOWEST cost possible?

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

Answer: C

Explanation:
This is the best solution to achieve the objective of reducing current RTO (Recovery Time Objective) from 12 hours to one hour, and RPO (Recovery Point Objective) from one day to eight hours, at the lowest cost possible, for a website that uses mostly static files and a small relational database. RTO is a metric that measures how quickly a system or service can be restored after a disruption or disaster. RPO is a metric that measures how much data can be lost or how far back in time a recovery point can be without causing significant impact or damage. To reduce RTO and RPO, the administrator should implement a website replica in the cloud with auto-scaling using the smallest possible footprint. A website replica is a copy or backup of a website that can be used for recovery or failover purposes. Auto-scaling is a feature that allows cloud resources or systems to adjust their capacity and performance according to demand or workload. Using auto-scaling with the smallest possible footprint can minimize costs by using only the necessary resources and scaling up or down as needed. The administrator should also use DNS (Domain Name System) to shift the load from on premises to the cloud. DNS is a service that translates domain names into IP addresses and vice versa. Using DNS, the administrator can redirect traffic from the on-premises website to the cloud replica in case of a disruption or disaster, and vice versa when recovery is complete.

NEW QUESTION 77
- (Topic 2)
Which of the following cloud services is fully managed?

A. IaaS
B. GPU in the cloud
C. IoT
D. Serverless compute
E. SaaS

Answer: E

Explanation:
SaaS (Software as a Service) is a cloud service model that provides fully managed applications to the end users. The users do not have to worry about installing, updating, or maintaining the software, as the cloud provider handles all these tasks. Examples of SaaS are Gmail, Office 365, Salesforce, etc.

NEW QUESTION 78
- (Topic 2)
A technician just received the lessons learned from some recent data that was lost due to an on-premises file-server crash. The action point is to change the backup strategy to minimize manual intervention. Which of the following is the BEST approach for the technician to implement?

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

Answer: A

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

NEW QUESTION 82
- (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 83
- (Topic 2)
A cloud administrator would like to deploy a cloud solution to its provider using automation techniques. Which of the following must be used? (Choose two.)

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

Answer: CD

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

NEW QUESTION 87
- (Topic 2)
A technician needs to deploy two virtual machines in preparation for the configuration of a financial application next week. Which of the following cloud deployment models should the technician use?

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

Answer: B

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

NEW QUESTION 88
- (Topic 2)
A systems administrator is configuring network management but is concerned about confidentiality. Which of the following should the administrator configure to address this concern?

A. SNMPv3
B. Community strings
C. IPSec tunnels
D. ACLs

Answer: A

Explanation:
SNMPv3 is the protocol that the administrator should configure to address the concern about confidentiality for network management. SNMP (Simple Network Management Protocol) is a standard protocol that allows network devices and systems to exchange information and perform management tasks. SNMPv3 is the latest version of SNMP that provides security enhancements, such as authentication, encryption, and access control, to protect the confidentiality, integrity, and availability of network data.

NEW QUESTION 91
- (Topic 2)
An organization is using multiple SaaS-based business applications, and the systems administrator is unable to monitor and control the use of these subscriptions. The administrator needs to implement a solution that will help the organization apply security policies and monitor each individual SaaS subscription. Which of the following should be deployed to achieve these requirements?

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

Answer: B

Explanation:
CASB (Cloud Access Security Broker) is what should be deployed to monitor and control the use of multiple SaaS-based business applications in a cloud environment. SaaS (Software as a Service) is a cloud service model that provides customers with access to software applications hosted on remote servers over a network or internet connection. SaaS can provide customers with convenience, flexibility, and scalability, but it may also introduce security risks such as data breaches, leaks, losses, etc., especially if customers have multiple SaaS subscriptions from different providers. CASB is a tool or service that acts as an intermediary between customers and SaaS providers. CASB can help to monitor and control the use of multiple SaaS subscriptions by providing features such as:
? Visibility: CASB can provide visibility into what SaaS applications are being used, by whom, when, where, how, etc., as well as identify any unauthorized or suspicious activities.
? Compliance: CASB can provide compliance with various laws, regulations, standards, policies, etc., that apply to SaaS applications and data, such as GDPR, HIPAA, PCI DSS, etc., as well as enforce them using rules or actions.
? Security: CASB can provide security for SaaS applications and data by detecting and preventing any threats or attacks, such as malware, phishing, ransomware, etc., as well as protecting them using encryption, authentication, authorization, etc.

NEW QUESTION 92
- (Topic 2)
A cloud administrator needs to reduce the cost of cloud services by using the company's off-peak period. Which of the following would be the BEST way to achieve this with minimal effort?

A. Create a separate subscription.
B. Create tags.
C. Create an auto-shutdown group.
D. Create an auto-scaling group.

Answer: C

Explanation:
Creating an auto-shutdown group is the best way to reduce the cost of cloud services by using the company's off-peak period with minimal effort. An auto-shutdown group is a feature that allows customers to automatically turn off or shut down certain cloud resources or services during a specified time period or schedule. An auto-shutdown group can help to reduce the cost of cloud services by minimizing the consumption of resources or services during off-peak periods, when they are not needed or used. An auto-shutdown group can also help to reduce the effort of managing cloud resources or services by automating the shutdown process, without requiring any manual intervention or configuration.

NEW QUESTION 95
- (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 97
- (Topic 2)
A systems administrator is performing upgrades to all the hypervisors in the environment. Which of the following components of the hypervisors should be upgraded? (Choose two.)

A. The fabric interconnects
B. The virtual appliances
C. The firmware
D. The virtual machines
E. The baselines
F. The operating system

Answer: CF

Explanation:
These are the components of the hypervisors that should be upgraded by the administrator who is performing upgrades to all the hypervisors in the environment. A hypervisor is a software or hardware that allows multiple VMs (Virtual Machines) to run on a single physical host or server. A hypervisor consists of various components, such as:
? The firmware: This is the software that controls the basic functions and operations of the hardware or device. The firmware can affect the performance, compatibility, and security of the hypervisor and the VMs. The firmware should be upgraded to ensure that it supports the latest features and functions of the hardware or device, as well as fix any bugs or vulnerabilities.
? The operating system: This is the software that manages the resources and activities of the hypervisor and the VMs. The operating system can affect the functionality, reliability, and efficiency of the hypervisor and the VMs. The operating system should be upgraded to ensure that it supports the latest applications and services of the hypervisor and the VMs, as well as improve stability and performance.

NEW QUESTION 102
- (Topic 2)

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

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

Answer: D

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

NEW QUESTION 106
- (Topic 2)
A systems administrator is working in a globally distributed cloud environment. After a file server VM was moved to another region, all users began reporting slowness when saving files. Which of the following is the FIRST thing the administrator should check while troubleshooting?

A. Network latency
B. Network connectivity
C. Network switch
D. Network peering

Answer: A

Explanation:
Network latency is the first thing that the administrator should check while troubleshooting slowness when saving files after a file server VM was moved to another region in a globally distributed cloud environment. Network latency is a measure of how long it takes for data to travel from one point to another over a network or connection. Network latency can affect performance and user experience of cloud applications or services by determining how fast data can be transferred or processed between clients and servers or vice versa. Network latency can vary depending on various factors, such as distance, bandwidth, congestion, interference, etc. Network latency can increase when a file server VM is moved to another region in a globally distributed cloud environment, as it may increase the distance and decrease the bandwidth between clients and servers, which may result in delays or errors in data transfer or processing.

NEW QUESTION 107
- (Topic 2)
A cloud administrator is assigned to establish a connection between the on-premises data center and the new CSP infrastructure. The connection between the two locations must be secure at all times and provide service for all users inside the organization. Low latency is also required to improve performance during data transfer operations. Which of the following would BEST meet these requirements?

A. A VPC peering configuration
B. An IPSec tunnel
C. An MPLS connection
D. A point-to-site VPN

Answer: B

Explanation:
An IPSec tunnel is what would best meet the requirements of establishing a connection between the on-premises data center and the new CSP infrastructure that is secure at all times and provides service for all users inside the organization with low latency. IPSec (Internet Protocol Security) is a protocol that encrypts and secures network traffic over IP networks. IPSec tunnel is a mode of IPSec that creates a virtual private network (VPN) tunnel between two endpoints, such as routers, firewalls, gateways, etc., and encrypts and secures all traffic that passes through it. An IPSec tunnel can meet the requirements by providing:
? Security: An IPSec tunnel can protect network traffic from interception, modification, spoofing, etc., by using encryption, authentication, integrity, etc., mechanisms.
? Service: An IPSec tunnel can provide service for all users inside the organization by allowing them to access and use network resources or services on both ends of the tunnel, regardless of their physical location.
? Low latency: An IPSec tunnel can provide low latency by reducing the number of hops or devices that network traffic has to pass through between the endpoints of the tunnel.

NEW QUESTION 111
- (Topic 2)
A cloud administrator is upgrading a cloud environment and needs to update the automation script to use a new feature from the cloud provider. After executing the script, the deployment fails. Which of the following is the MOST likely cause?

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

Answer: A

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

NEW QUESTION 113
- (Topic 2)
A resource pool in a cloud tenant has 90 GB of memory and 120 cores. The cloud administrator needs to maintain a 30% buffer for resources for optimal performance of the hypervisor. Which of the following would all ow for the maximum number of two-core machines with equal memory?

A. 30 VMs, 3GB of memory
B. 40 VMs, 1,5GB of memory
C. 45 VMs, 2 GB of memory
D. 60 VMs, 1 GB of memory

Answer: C

Explanation:
To calculate the maximum number of two-core machines with equal memory, we need to consider the resource pool capacity and the buffer requirement. The resource pool has 90 GB of memory and 120 cores, but the cloud administrator needs to maintain a 30% buffer for optimal performance. This means that only 70% of the resources can be used for VM allocation. Therefore, the available memory is 90 GB x 0.7 = 63 GB, and the available cores are 120 x 0.7 = 84 cores. To allocate two-core machines with equal memory, we need to divide the available memory by the available cores and multiply by two. This gives us the memory size per VM: (63 GB / 84 cores) x 2 = 1.5 GB. However, this is not a valid answer option, so we need to find the closest option that does not exceed the available resources. The best option is C, which allocates 45 VMs with 2 GB of memory each. This uses up 45 x 2 = 90 GB of memory and 45 x 2 = 90 cores, which are within the available limits.

NEW QUESTION 115
- (Topic 2)
A disaster situation has occurred, and the entire team needs to be informed about the situation. Which of the following documents will help the administrator find the details of the relevant team members for escalation?

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

Answer: D

Explanation:
A call tree is what will help the administrator find the details of the relevant team members for escalation after a disaster situation has occurred and the entire team needs to be informed about the situation. A call tree is a document or diagram that shows the hierarchy or sequence of communication or notification among team members in case of an emergency or incident, such as a disaster situation. A call tree can help to find the details of the relevant team members for escalation by providing information such as:
? Name: This indicates who is involved in the communication or notification process, such as team members, managers, stakeholders, etc.
? Role: This indicates what is their function or responsibility in the communication or notification process, such as initiator, receiver, sender, etc.
? Contact: This indicates how they can be reached or contacted in the communication or notification process, such as phone number, email address, etc.

NEW QUESTION 118
- (Topic 2)
A systems administrator wants to ensure two VMs remain together on the same host. Which of the following must be set up to enable this functionality?

A. Affinity
B. Zones
C. Regions
D. A cluster

Answer: A

Explanation:
Affinity is what must be set up to ensure two VMs remain together on the same host. Affinity is a feature that allows customers to specify preferences or requirements for placing VMs on certain hosts or clusters within a cloud environment. Affinity can help to improve performance, availability, compatibility, or security of VMs by ensuring they are located on optimal hosts or clusters. Affinity can also help to keep two VMs together on the same host by creating an affinity rule that binds them together.

NEW QUESTION 119
- (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 122
- (Topic 2)
A Chief Information Security Officer (CISO) is evaluating the company’s security management program. The CISO needs to locate all the assets with identified deviations and mitigation measures. Which of the following would help the CISO with these requirements?

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

Answer: D

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

NEW QUESTION 123
- (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 124
- (Topic 2)
A development team recently completed testing changes to a company's web-based CMS in the sandbox environment. The cloud administrator deployed these CMS application changes to the staging environment as part of the next phase in the release life cycle. The deployment was successful, but after deploying the CMS application, the web page displays an error message stating the application is unavailable. After reviewing the application logs, the administrator sees an error message that the CMS is unable to connect to the database. Which of the following is the BEST action for the cloud administrator to perform to resolve the issue?

A. Modify the deployment script to delete and recreate the database whenever the CMS application is deployed.
B. Modify the ACL to allow the staging environment to access the database in the sandbox environment.
C. Modify the CMS application deployment to use the previous version and redeploy the application.
D. Modify the configuration settings of the CMS application to connect to the database in the current environment.

Answer: D

Explanation:
Modifying the configuration settings of the CMS (Content Management System) application to connect to the database in the current environment is what the cloud administrator should do to resolve the issue of web page displaying an error message stating the application is unavailable after deploying CMS application changes to the staging environment. A CMS is a software or platform that allows users to create, manage, and publish web content. A CMS may use a database to store and retrieve web content and information. A staging environment is a testing or pre-production environment that simulates the production environment and allows users to verify and validate changes or updates before deploying them to production. Modifying the configuration settings of the CMS application can help to resolve the issue by ensuring that the CMS application can access and communicate with the database in the current environment, rather than using the previous or default settings that may point to a different or non-existent database.

NEW QUESTION 127
- (Topic 2)
A company had a system compromise, and the engineering team resolved the issue after 12 hours. Which of the following information will MOST likely be requested by the Chief Information Officer (CIO) to understand the issue and its resolution?

A. A root cause analysis
B. Application documentation
C. Acquired evidence
D. Application logs

Answer: A

Explanation:
A root cause analysis is what will most likely be requested by the Chief Information Officer (CIO) to understand the issue and its resolution after a system compromise that was resolved by the engineering team after 12 hours. A root cause analysis is a technique of investigating and identifying the underlying or fundamental cause or reason for an incident or issue that affects or may affect the normal operation or performance of a system or service. A root cause analysis can help to understand the issue and its resolution by providing information such as:
? What happened: This describes what occurred during the incident or issue, such as symptoms, effects, impacts, etc.
? Why it happened: This explains why the incident or issue occurred, such as triggers, factors, conditions, etc.
? How it was resolved: This details how the incident or issue was fixed or mitigated, such as actions, steps, methods, etc.
? How it can be prevented: This suggests how the incident or issue can be avoided or reduced in the future, such as recommendations, improvements, changes, etc.

NEW QUESTION 131
- (Topic 2)

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

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

Answer: A

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

NEW QUESTION 135
- (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 138
- (Topic 2)
A systems administrator is about to deploy a new VM to a cloud environment. Which of the following will the administrator MOST likely use to select an address for the VM?

A. CDN
B. DNS
C. NTP
D. IPAM

Answer: D

Explanation:
IPAM (IP Address Management) is what the administrator will most likely use to select an address for the new VM that is about to be deployed to a cloud environment. IPAM is a tool or service that allows customers to plan, track, and manage the IP addresses and DNS names of their cloud resources or systems. IPAM can help to select an address for the new VM by providing information such as available IP addresses, IP address ranges, subnets, domains, etc., as well as ensuring that the address is unique and valid.

NEW QUESTION 139
- (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 140
- (Topic 2)
A cloud engineer is responsible for managing a public cloud environment. There is currently one virtual network that is used to host the servers in the cloud environment. The environment is rapidly growing, and the network does not have any more available IP addresses. Which of the following should the engineer do to accommodate additional servers in this environment?

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

Answer: A

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

NEW QUESTION 143
- (Topic 1)
Company A has acquired Company B and is in the process of integrating their cloud resources. Company B needs access to Company A's cloud resources while retaining its IAM solution.
Which of the following should be implemented?

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

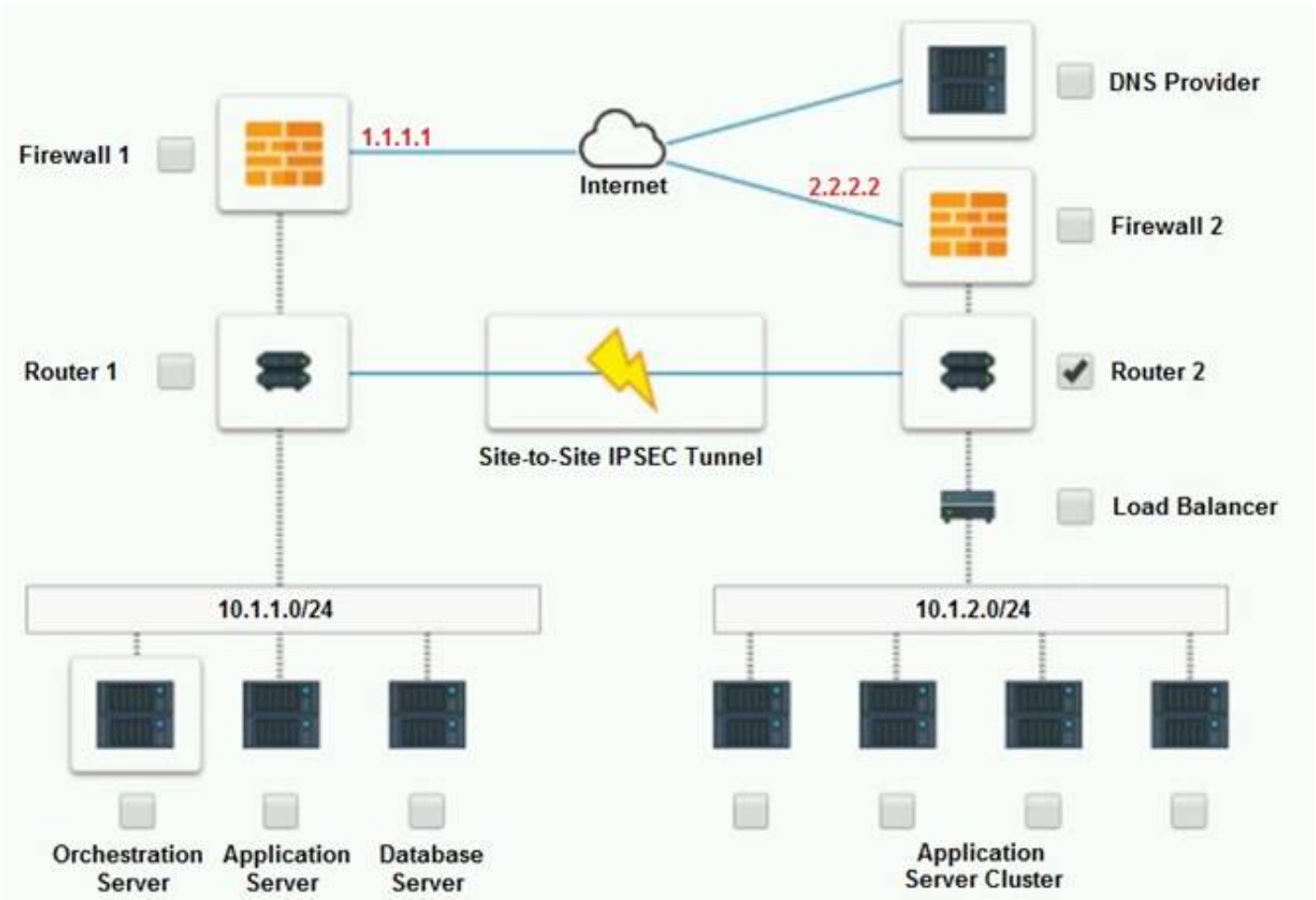
Answer: C

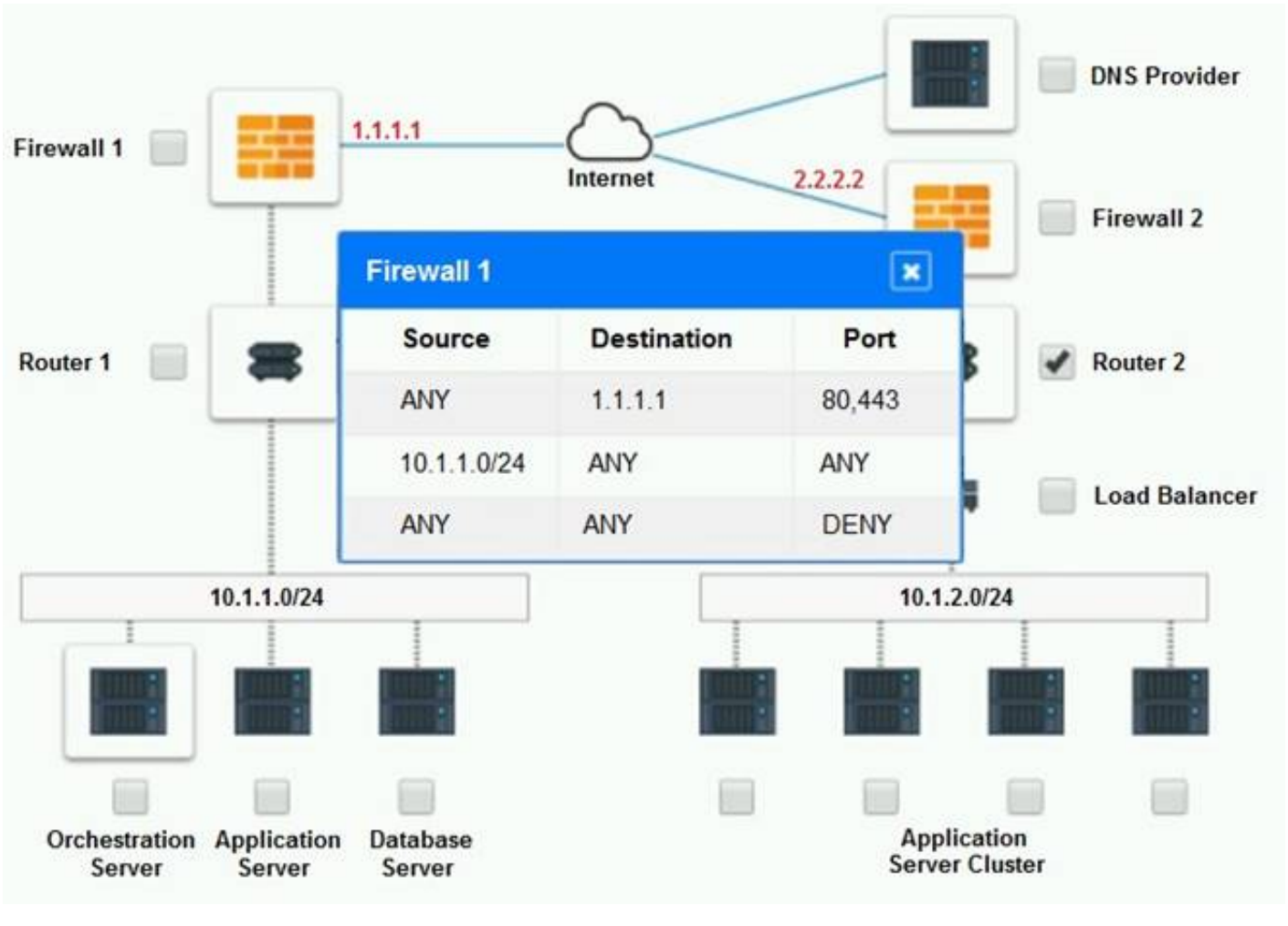
Explanation:
Identity federation is a type of authentication mechanism that allows users to access multiple systems or applications across different domains or organizations with a single login credential. Identity federation can help integrate the cloud resources of Company A and Company B after Company A has acquired Company B, as it can enable seamless and secure access to both companies' cloud resources using the same IAM solution. Identity federation can also improve user convenience, productivity, and security, as it can simplify the login process, reduce login errors, and enhance password management. References: CompTIA Cloud+ Certification Exam Objectives, page 14, section 2.7
Reference: https://medium.com/@dinika.15/identity-federation-a-brief-introduction- f2f823f8795a

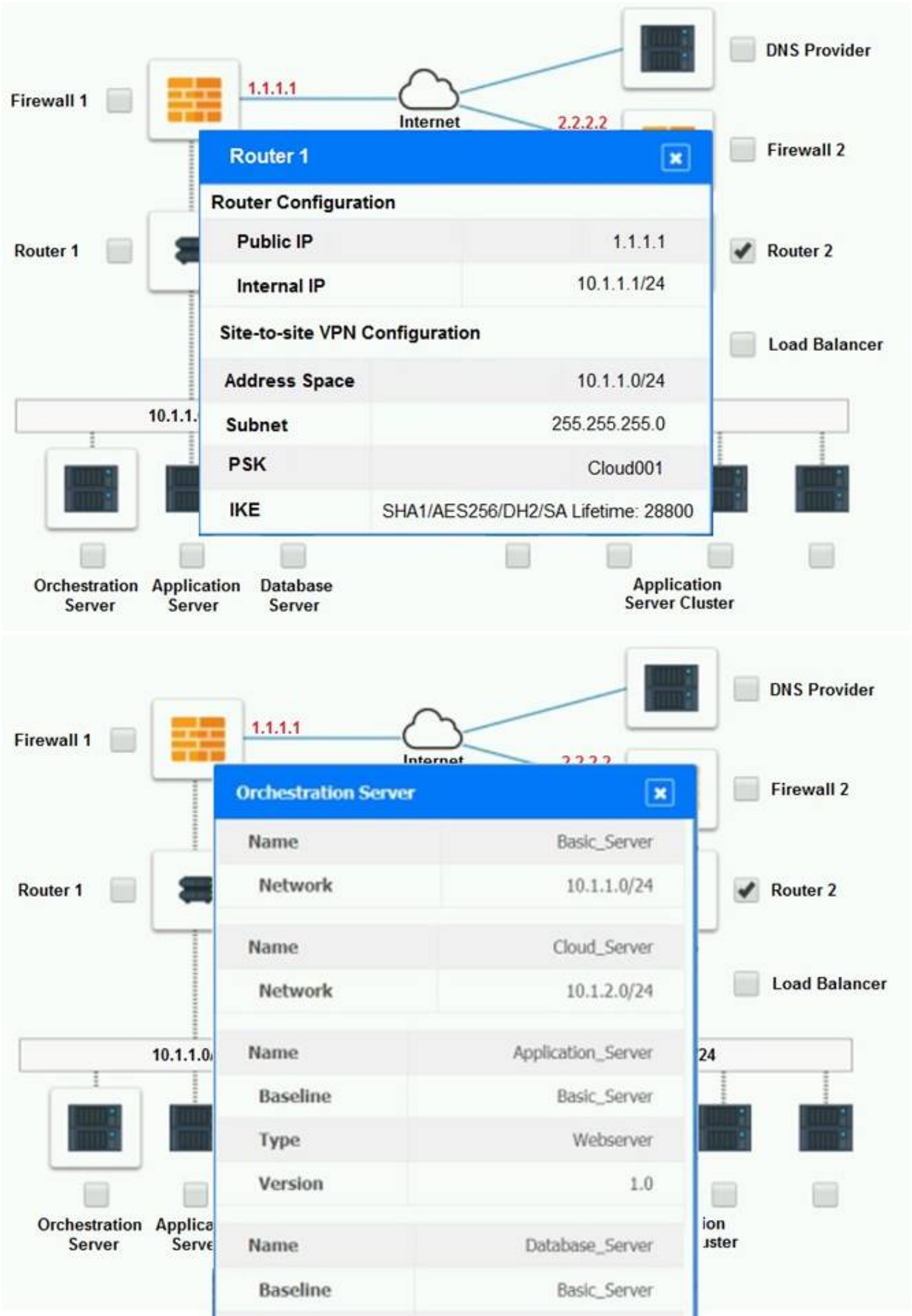
NEW QUESTION 144
SIMULATION - (Topic 1)
A company has decided to scale its e-commerce application from its corporate datacenter to a commercial cloud provider to meet an anticipated increase in demand during an upcoming holiday.
The majority of the application load takes place on the application server under normal conditions. For this reason, the company decides to deploy additional application servers into a commercial cloud provider using the on-premises orchestration engine that installs and configures common software and network configurations.
The remote computing environment is connected to the on-premises datacenter via a site- to-site IPSec tunnel. The external DNS provider has been configured to use weighted round-robin routing to load balance connections from the Internet.
During testing, the company discovers that only 20% of connections completed successfully.
INSTRUCTIONS
Review the network architecture and supporting documents and fulfill these requirements: Part 1:
- Analyze the configuration of the following components: DNS, Firewall 1, Firewall 2, Router 1, Router 2, VPN and Orchestrator Server.
- Identify the problematic device(s).

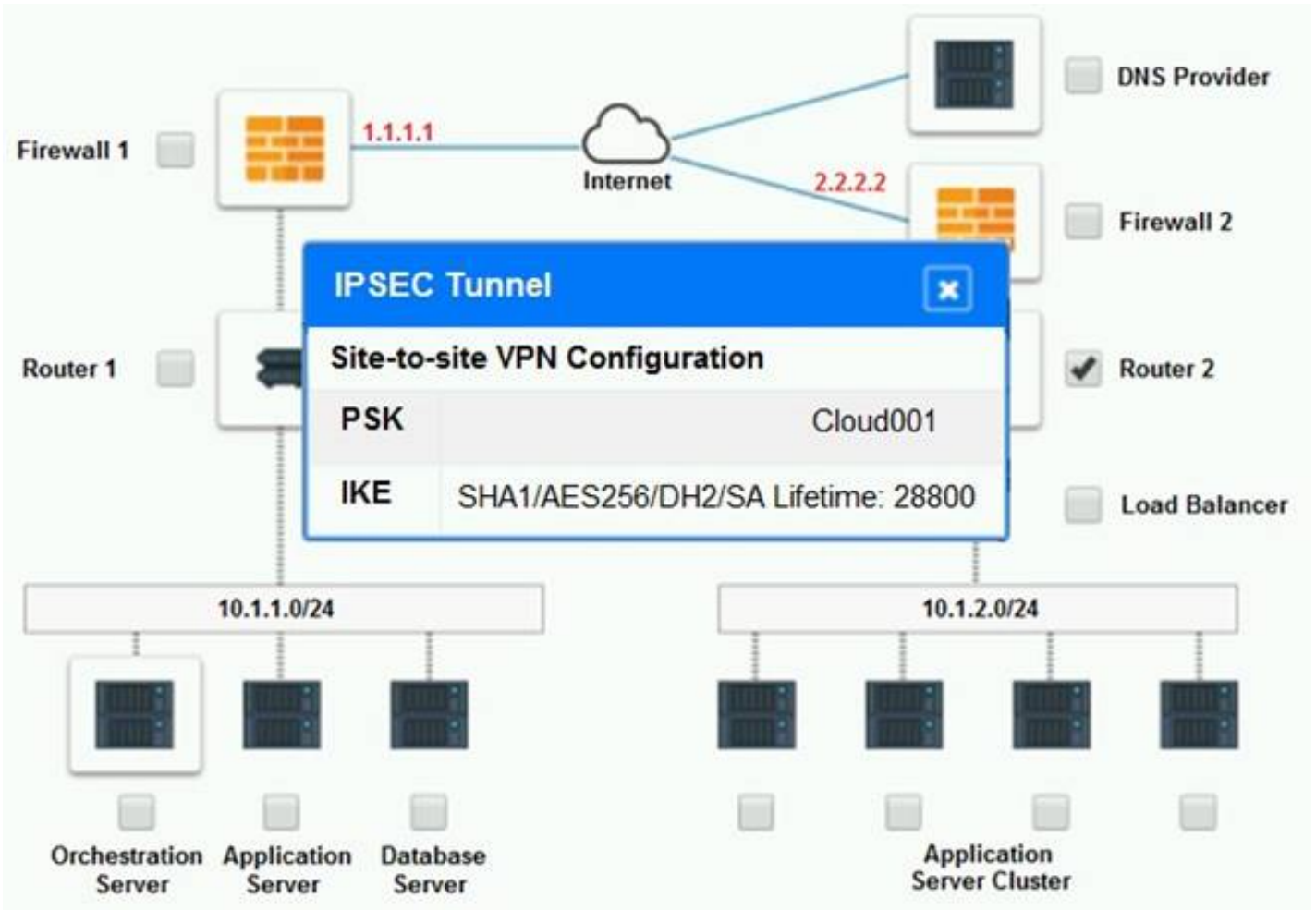
Part 2:
- Identify the correct options to provide adequate configuration for hybrid cloud architecture.

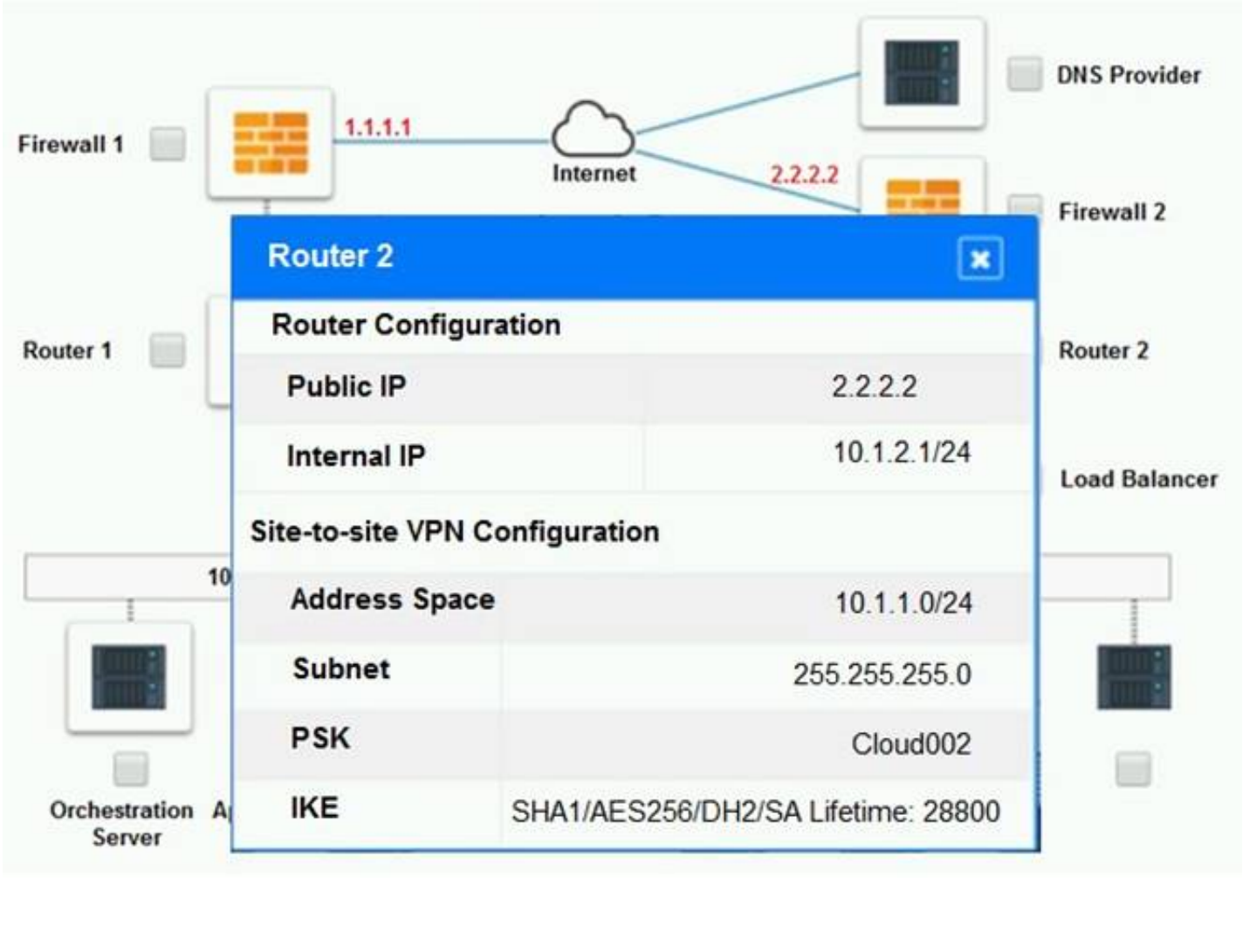
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.
Part 1:
Cloud Hybrid Network Diagram

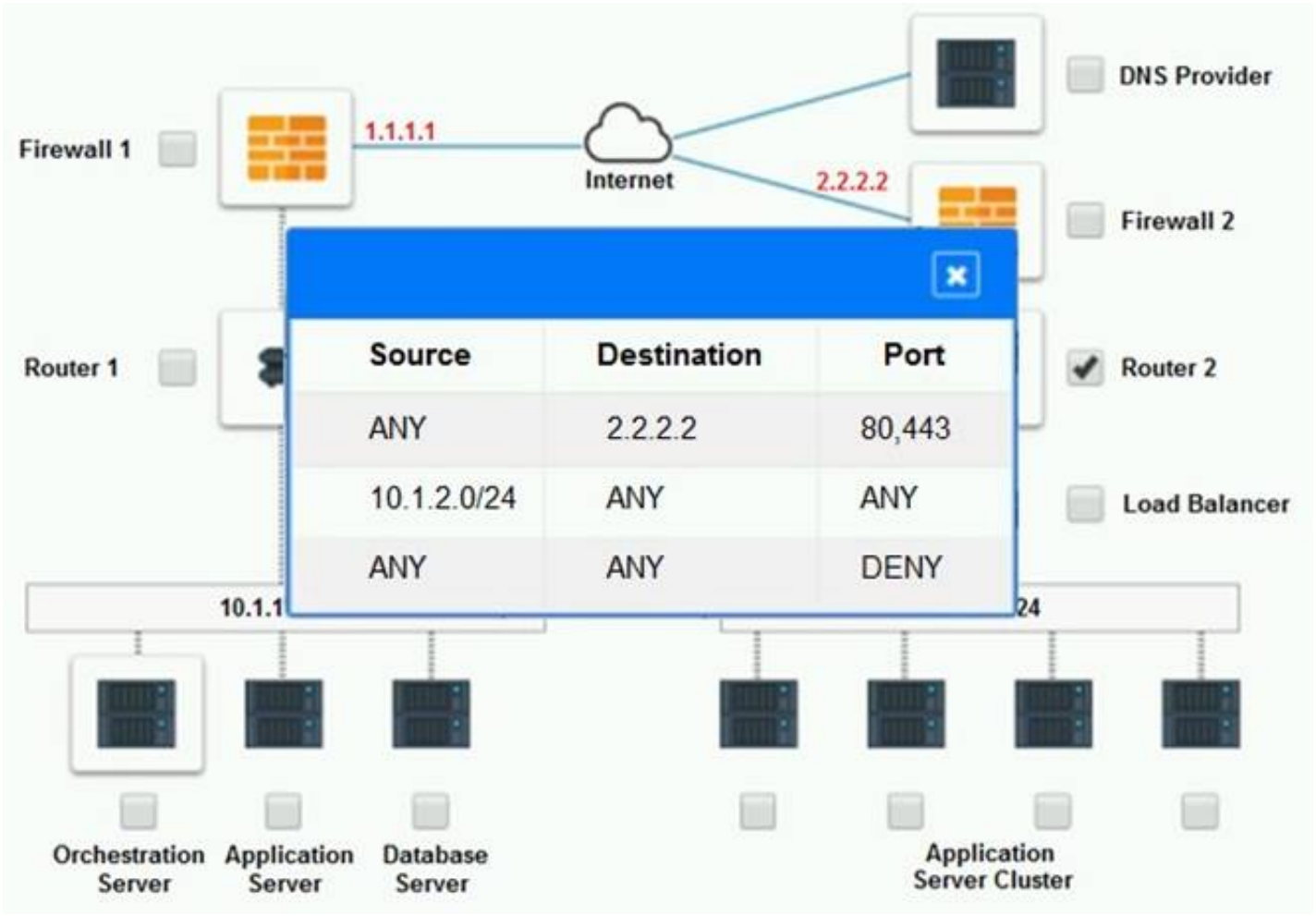

Firewall 1
1.1.1.1
Internet
2.2.2.2
DNS Provider
Firewall 2
Router 1
Router 2
Site-to-Site IPSEC Tunnel
Load Balancer
10.1.1.0/24
10.1.2.0/24
Orchestration Server
Application Server
Database Server
Application Server Cluster

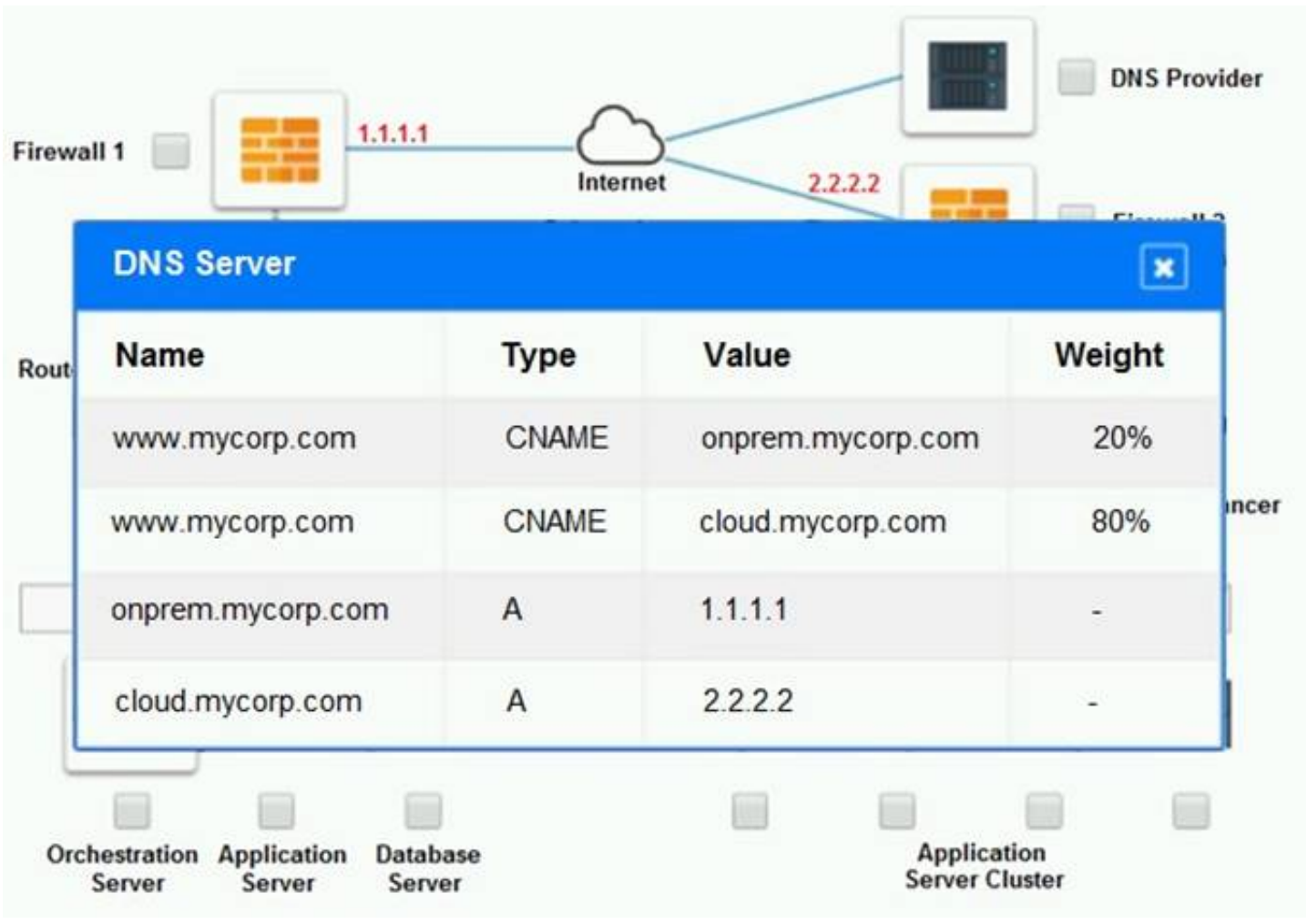

Firewall 1
1.1.1.1
Internet
2.2.2.2
DNS Provider
Firewall 2
Router 1
Router 2
Load Balancer
Firewall 1
Source
Destination
Port
ANY
1.1.1.1
80,443
10.1.1.0/24
ANY
ANY
ANY
ANY
DENY
10.1.1.0/24
10.1.2.0/24
Orchestration Server
Application Server
Database Server
Application Server Cluster


DNS Provider
Firewall 1
1.1.1.1
Internet
2.2.2.2
Firewall 2
Router 1
Router 2
Load Balancer
10.1.1.
Orchestration Server
Application Server
Database Server
Application Server Cluster
Router 1
Router Configuration
Public IP 1.1.1.1
Internal IP 10.1.1.1/24
Site-to-site VPN Configuration
Address Space 10.1.1.0/24
Subnet 255.255.255.0
PSK Cloud001
IKE SHA1/AES256/DH2/SA Lifetime: 28800
Orchestration Server
Name Basic_Server
Network 10.1.1.0/24
Name Cloud_Server
Network 10.1.2.0/24
Name Application_Server
Baseline Basic_Server
Type Webserver
Version 1.0
Name Database_Server
Baseline Basic_Server
Type Database Server
Version 1.0
Name Corporate_Datacenter
Baseline Application_Server
Count 1
Name Cloud_Service_Provider
Baseline Cloud_Server
Count 4


Firewall 1
1.1.1.1
Internet
2.2.2.2
DNS Provider
Firewall 2
IPSEC Tunnel
Site-to-site VPN Configuration
PSK
Cloud001
IKE
SHA1/AES256/DH2/SA Lifetime: 28800
Router 1
Router 2
Load Balancer
10.1.1.0/24
10.1.2.0/24
Orchestration Server
Application Server
Database Server
Application Server Cluster


Firewall 1
1.1.1.1
Internet
2.2.2.2
DNS Provider
Firewall 2
Router 2
Router Configuration
Public IP
2.2.2.2
Internal IP
10.1.2.1/24
Site-to-site VPN Configuration
Address Space
10.1.1.0/24
Subnet
255.255.255.0
PSK
Cloud002
IKE
SHA1/AES256/DH2/SA Lifetime: 28800
Router 1
Router 2
Load Balancer
Orchestration Server





Part 2:
Only select a maximum of TWO options from the multiple choice question

- ☐ Deploy a Replica of the Database Server in the Cloud Provider.
- ☐ Update the PSK (Pre-shared key) in Router 2.
- ☐ Update the A record on the DNS from 2.2.2.2 to 1.1.1.1.
- ☐ Promote deny All to allow All in Firewall 1 and Firewall 2.
- ☐ Change the Address Space on Router 2.
- ☐ Change internal IP Address of Router 1.
- ☐ Reverse the Weight property in the two CNAME records on the DNS.
- ☐ Add the Application Server at on-premises to the Load Balancer.

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Part 1: Router 2
The problematic device is Router 2, which has an incorrect configuration for the IPSec tunnel. The IPSec tunnel is a secure connection between the on-premises datacenter and the cloud provider, which allows the traffic to flow between the two networks. The IPSec tunnel requires both endpoints to have matching parameters, such as the IP addresses, the pre-shared key (PSK), the encryption and authentication algorithms, and the security associations (SAs) .
According to the network diagram and the configuration files, Router 2 has a different PSK and a different address space than Router 1. Router 2 has a PSK of "1234567890", while Router 1 has a PSK of "0987654321". Router 2 has an address space of 10.0.0.0/8, while Router 1 has an address space of 192.168.0.0/16. These mismatches prevent the IPSec tunnel from establishing and encrypting the traffic between the two networks.
The other devices do not have any obvious errors in their configuration. The DNS provider has two CNAME records that point to the application servers in the cloud provider, with different weights to balance the load. The firewall rules allow the traffic from and to the application servers on port 80 and port 443, as well as the traffic from and to the VPN server on port 500 and port 4500. The orchestration server has a script that installs and configures the application servers in the cloud provider, using the DHCP server to assign IP addresses.
Part 2:
The correct options to provide adequate configuration for hybrid cloud architecture are:
? Update the PSK in Router 2.
? Change the address space on Router 2.
These options will fix the IPSec tunnel configuration and allow the traffic to flow between the on-premises datacenter and the cloud provider. The PSK should match the one on Router 1, which is "0987654321". The address space should also match the one on Router 1, which is 192.168.0.0/16.
* B. Update the PSK (Pre-shared key in Router2)
* E. Change the Address Space on Router2

NEW QUESTION 148
- (Topic 1)
An organization purchased new servers with GPUs for render farms. The servers have limited CPU resources.
Which of the following GPU configurations will be the MOST optimal for virtualizing this environment?

A. Dedicated
B. Shared
C. Passthrough
D. vGPU

Answer: C

Explanation:
Passthrough is a type of GPU configuration that allows a VM to directly access a physical GPU on the host system without any virtualization layer or sharing mechanism. Passthrough can provide optimal performance and compatibility for GPU- intensive applications, such as rendering or gaming, as it eliminates any overhead or contention caused by virtualization or sharing. Passthrough is also suitable for servers with limited CPU resources, as it reduces the CPU load and offloads the graphics processing to the GPU. Passthrough is the most optimal GPU configuration for virtualizing a new server with GPUs for render farms.
References: CompTIA Cloud+ Certification Exam Objectives, page 11, section 1.6

NEW QUESTION 152
- (Topic 1)
A developer is no longer able to access a public cloud API deployment, which was working ten minutes prior.
Which of the following is MOST likely the cause?

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

Answer: A

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

NEW QUESTION 153
- (Topic 1)
An IaaS application has a two-hour RTO and a four-hour RPO. The application takes one hour to back up its data or restore from a local backup file. A systems administrator is tasked with configuring the backup policy.
Which of the following should the administrator configure to achieve the application requirements with the LEAST cost?

A. Back up to long-term storage every night
B. Back up to object storage every three hours
C. Back up to long-term storage every four hours
D. Back up to object storage every hour

Answer: B

Explanation:
Object storage is a type of storage service that stores data as objects with unique identifiers and metadata in a flat namespace or structure. Backing up to object storage every three hours can help achieve the application requirements with the least cost for an IaaS application that has a two-hour RTO and a four-hour RPO,

as it can provide scalable, durable, and cost-effective storage for backup data while meeting the recovery time and point objectives. Backing up to object storage every three hours can ensure that the backup data is no more than four hours old and can be restored within two hours in case of a disaster or failure. References: CompTIA Cloud+ Certification Exam Objectives, page 9, section 1.4

NEW QUESTION 157
- (Topic 1)
A systems administrator is building a new virtualization cluster. The cluster consists of five virtual hosts, which each have flash and spinning disks. This storage is shared among all the virtual hosts, where a virtual machine running on one host may store data on another host.
This is an example of:

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

Answer: C

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

NEW QUESTION 160
- (Topic 1)
An OS administrator is reporting slow storage throughput on a few VMs in a private IaaS cloud. Performance graphs on the host show no increase in CPU or memory. However, performance graphs on the storage show a decrease of throughput in both IOPS and MBps but not much increase in latency. There is no increase in workload, and latency is stable on the NFS storage arrays that are used by those VMs.
Which of the following should be verified NEXT?

A. Application
B. SAN
C. VM GPU settings
D. Network

Answer: D

Explanation:
The network is the set of devices, connections, protocols, and configurations that enable communication and data transfer between different systems and applications. The network can affect the performance of storage throughput by influencing factors such as bandwidth, latency, jitter, packet loss, and congestion. Poor network performance can result in low storage throughput in both IOPS and MBps, as it can limit the amount and speed of data that can be sent or received by the storage devices. Verifying the network should be the next step for troubleshooting the issue of slow storage throughput on a few VMs in a private IaaS cloud, as it can help identify and resolve any network-related problems that may be causing the issue. References: CompTIA Cloud+ Certification Exam Objectives, page 17, section 3.4

NEW QUESTION 165
- (Topic 1)
A marketing team is using a SaaS-based service to send emails to large groups of potential customers. The internally managed CRM system is configured to generate a list of target customers automatically on a weekly basis, and then use that list to send emails to each customer as part of a marketing campaign. Last week, the first email campaign sent emails successfully to 3,000 potential customers. This week, the email campaign attempted to send out 50,000 emails, but only 10,000 were sent.
Which of the following is the MOST likely reason for not sending all the emails?

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

Answer: A

Explanation:
An API request limit is a restriction on the number of requests that can be made to a web service or application programming interface (API) within a certain time period. API request limits are often used by SaaS-based services to control the usage and traffic of their customers and prevent overloading or abuse of their resources. An API request limit can cause a failure to send all the emails if the marketing team exceeds the number of requests allowed by the SaaS-based service in a week. The service may reject or block any requests that go beyond the limit, resulting in fewer emails being sent than expected. References: CompTIA Cloud+ Certification Exam Objectives, page 13, section 2.5
Reference: https://developers.google.com/analytics/devguides/config/mgmt/v3/limits- quotas

NEW QUESTION 167
- (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 172
- (Topic 1)
The human resources department was charged for a cloud service that belongs to another department. All other cloud costs seem to be correct.
Which of the following is the MOST likely cause for this error?

A. Misconfigured templates
B. Misconfigured chargeback
C. Incorrect security groups
D. Misconfigured tags

Answer: D

Explanation:
Tags are metadata or labels that can be assigned to cloud resources or services to identify and organize them based on various criteria, such as name, purpose, owner, or cost center. Tags can help track the costs for each business unit or department that uses cloud services, as they can enable granular and accurate billing and reporting based on the tags. Misconfigured tags can cause the issue of inaccurate cost tracking for different businesses, as they can result in incorrect or missing billing information or reports. The issue can be resolved by configuring the tags properly to reflect the correct business unit or department for each cloud resource or service. References: CompTIA Cloud+ Certification Exam Objectives, page 13, section 2.5

NEW QUESTION 176
- (Topic 1)
After accidentally uploading a password for an IAM user in plain text, which of the following should a cloud administrator do FIRST? (Choose two.)

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

Answer: BD

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

NEW QUESTION 180
- (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 183
- (Topic 4)
Which of the following are advantages of a public cloud? (Select TWO).

A. Full control of hardware
B. Reduced monthly costs
C. Decreased network latency
D. Pay as you use
E. Availability of self-service
F. More secure data

Answer: BD

Explanation:
The correct answers are B and D.
* B. Reduced monthly costs: One of the main advantages of public cloud is that it lowers the costs of IT infrastructure and maintenance for the customers. They do not need to purchase, install, or manage any hardware or software, and they only pay for the resources they use. This can result in significant savings compared to owning and operating a private cloud or an on-premise data center1234
* D. Pay as you use: Another benefit of public cloud is that it offers a flexible and scalable pricing model based on the actual usage of the customers. They can adjust their resource consumption according to their changing needs and demands, and only pay for what they use. This eliminates the need for upfront capital investment or long-term contracts, and allows customers to optimize their spending and performance1234

NEW QUESTION 187
- (Topic 4)
A systems administrator is trying to connect to a remote KVM host. The command line appears as follows:

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

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

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

Answer: B

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

NEW QUESTION 190
- (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 193
- (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 196
- (Topic 4)
A cloud administrator created a developer desktop image and added it to the VDI farm in a private cloud environment. One of the developers opened a VDI session and noticed that compiling the code was taking up to one hour to complete. However, when the developer compiles the code on a local machine, the job completes in less than five minutes. Which of the following sizing techniques would be best to use to improve the performance of the compile job?

A. Add more servers to the VDI environment.
B. Increase the CPU and the memory on the VDI template.
C. Configure the VDI environment to increase sessions automatically.
D. Migrate code compile jobs to a public cloud provider.

Answer: B

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

NEW QUESTION 201
- (Topic 4)
Which of the following enables CSPs to offer unlimited capacity to customers?

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

Answer: C

Explanation:
The correct answer is C. Economies of scale.
Economies of scale are the cost advantages that CSPs can achieve by increasing the size and scale of their operations. By spreading the fixed costs of infrastructure, software, and personnel over a larger customer base and data volume, CSPs can reduce the average cost per unit of service and offer unlimited capacity to customers at competitive prices1. Adequate budget is not a sufficient condition for offering unlimited capacity, as CSPs still need to optimize their resource utilization and efficiency to meet the growing demand for data storage and processing.
Global data center distribution is a strategy that CSPs use to improve their service availability, reliability, and performance by locating their servers closer to their customers and reducing network latency. However, this does not necessarily imply unlimited capacity, as CSPs still need to manage the trade-offs between data center size, cost, and power consumption.
Agile project management is a methodology that CSPs use to deliver their services faster, better, and cheaper by adopting iterative, incremental, and collaborative approaches. However, this does not directly affect their capacity, as CSPs still need to scale their infrastructure and software to handle the increasing data load.

NEW QUESTION 204
- (Topic 4)
A systems administrator audits a cloud application and discovers one of the key regulatory requirements has not been addressed. The requirement states that if a physical breach occurs and hard drives are stolen, the contents of the drives should not be readable. Which of the following should be used to address the requirement?

A. Obfuscation
B. Encryption
C. EDR
D. HIPS

Answer: B

Explanation:
Encryption is the process of transforming data into an unreadable format using a secret key or algorithm. Encryption can be used to protect data at rest or in transit from unauthorized access or theft. If a physical breach occurs and hard drives are stolen, encryption can prevent the contents of the drives from being readable by anyone who does not have the decryption key or algorithm.
References: [CompTIA Cloud+ Study Guide], page 236.

NEW QUESTION 205
- (Topic 4)
A cloud engineer is migrating a customer's web servers from a hypervisor platform to a CSP environment. The engineer needs to decouple the infrastructure and components during the migration to reduce the single points of failure. Which of the following storage options should the cloud engineer migrate the content to in

order to improve availability?

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

Answer: C

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

NEW QUESTION 210
- (Topic 4)
A company is using laaS 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 212
- (Topic 4)
A cloud security analyst needs to ensure the web servers in the public subnet allow only secure communications and must remediate any possible issue. The stateful configuration for the public web servers is as follows:

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

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

A. Remove rules I, 2. and 5.
B. Remove rules I, 3, and 4.
C. Remove rules 2.3. and 4.
D. Remove rules 3.4. and 5.

Answer: B

Explanation:
The correct answer is B. Remove rules 1, 3, and 4.
The objective is to ensure the web servers in the public subnet allow only secure communications. This means that only HTTPS traffic should be allowed on port 443, which is the standard port for secure web connections. HTTPS traffic uses the TCP protocol and encrypts the data between the client and the server.
Rule 1 allows all TCP traffic on any port from any source. This is too permissive and exposes the web servers to potential attacks or unauthorized access. Rule 1 should be removed to restrict the TCP traffic to only port 443.
Rule 3 allows all UDP traffic on any port from any source. UDP is a connectionless protocol that does not guarantee reliable or secure delivery of data. UDP is typically used for streaming media, voice over IP (VoIP), or online gaming, but not for web servers. Rule 3 should be removed to prevent unnecessary or malicious UDP traffic.
Rule 4 allows all ICMP traffic from any source. ICMP is a protocol that is used for diagnostic or control purposes, such as ping or traceroute. ICMP traffic can be used by attackers to scan or probe the network for vulnerabilities or information. Rule 4 should be removed to block ICMP traffic and reduce the attack surface.

Rule 2 allows TCP traffic on port 443 from any source. This is the desired rule that allows secure web communications using HTTPS. Rule 2 should be kept.
Rule 5 denies all other traffic that does not match any of the previous rules. This is the default rule that provides a catch-all protection for the web servers. Rule 5 should be kept. Therefore, the analyst should remove rules 1, 3, and 4 to accomplish the objective.

NEW QUESTION 214
- (Topic 4)
A cloud administrator is having difficulty correlating logs for multiple servers. Upon inspection, the administrator finds that the time-zone settings are mismatched throughout the deployment. Which of the following solutions can help maintain time synchronization between all the resources?

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

Answer: C

Explanation:
The correct answer is C. NTP.
NTP stands for Network Time Protocol, which is a standard protocol for synchronizing the clocks of computers over a network. NTP uses a hierarchical, client-server architecture, where a client requests the current time from a server, and the server responds with a timestamp. The client then adjusts its own clock to match the server's time, taking into account the network delay and clock drift. NTP can achieve sub-millisecond accuracy over local area networks and a few milliseconds over the internet12.
NTP can help maintain time synchronization between all the resources in a distributed cloud environment, as it allows each resource to get the accurate time from a reliable source. This can help with correlating logs, auditing, security, and other time-sensitive operations. NTP can also handle different time zones, as it uses Coordinated Universal Time (UTC) as the reference time, and each resource can convert UTC to its local time zone12.
DNS stands for Domain Name System, which is a protocol for resolving domain names into IP addresses. DNS does not provide any functionality for time synchronization3.
IPAM stands for IP Address Management, which is a method for planning, tracking, and managing the IP address space used in a network. IPAM does not provide any functionality for time synchronization.
SNMP stands for Simple Network Management Protocol, which is a protocol for collecting and organizing information about managed devices on a network. SNMP can be used to monitor the performance, availability, configuration, and security of network devices, but it does not provide any functionality for time synchronization.

NEW QUESTION 215
- (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 217
- (Topic 4)
A systems administrator deployed a new web application in a public cloud and would like to test it, but the company's network firewall is only allowing outside connections to the cloud provider network using TCP port 22. While waiting for the network administrator to open the required ports, which of the following actions should the systems administrator take to test the new application? (Select two).

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

Answer: BF

Explanation:
To test the new web application in the public cloud, the systems administrator should create a replica database, synchronize the data, and switch to the new

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

NEW QUESTION 221
- (Topic 4)
A systems administrator is responsible for upgrading operating systems on VMs that are hosted in a cloud environment. The systems administrator wants to ensure the VMs receive updates for as long as possible. Which of the following should the systems administrator choose?

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

Answer: C

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

NEW QUESTION 224
- (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 226
- (Topic 4)
When designing a three-node. load-balanced application, a systems administrator must ensure each node runs on a different physical server for HA purposes. Which of the following does the systems administrator need to configure?

A. Round-robin methods
B. Live migration
C. Anti-affinity rule
D. Priority queues

Answer: C

Explanation:
The correct answer is C. Anti-affinity rule.
An anti-affinity rule is a configuration option that prevents two or more virtual machines (VMs) from running on the same physical host. This can improve the availability and fault tolerance of the VMs, as it reduces the risk of losing multiple VMs due to a single host failure. An anti-affinity rule can also improve the

performance and load balancing of the VMs, as it distributes the workload across different hosts and avoids resource contention . A round-robin method is a load balancing algorithm that distributes incoming requests to a pool of servers in a circular order. A round-robin method does not consider the availability, capacity, or location of the servers, and may assign requests to servers that are overloaded, offline, or far away. A round-robin method does not ensure that each node runs on a different physical server.
A live migration is a process that allows moving a running VM from one physical host to another without interrupting its operation. A live migration can improve the availability and performance of the VMs, as it enables dynamic load balancing, maintenance, and disaster recovery. However, a live migration does not prevent two or more VMs from running on the same physical host in the first place.
A priority queue is a data structure that stores elements based on their priority values. A priority queue allows inserting and removing elements in order of their priority, such that the element with the highest priority is always at the front of the queue. A priority queue can be used to implement scheduling algorithms for processes or tasks, but it does not affect where they run on physical servers.

NEW QUESTION 230
- (Topic 4)
An organization is implementing a new requirement to facilitate faster downloads for users of corporate application content. At the same time, the organization is also expanding cloud regions. Which of the following would be suitable to optimize the network for this requirement?

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

Answer: A

Explanation:
CDN, or content delivery network, is a system of distributed servers that deliver web content to users based on their geographic location, the origin of the web page, and the content delivery server1. A CDN can improve the performance, availability, and scalability of cloud applications by caching static and dynamic content at the edge of the network, reducing the latency and bandwidth consumption between the users and the cloud servers2. A CDN can also provide security features such as encryption, authentication, and DDoS protection3.
Autoscaling, SR-IOV, and containerization are other techniques that can optimize the network for cloud applications, but they are not directly related to the requirement of faster downloads for users. Autoscaling is the process of automatically adjusting the number and size of compute resources based on the demand and workload of the application. SR-IOV, or single root I/O virtualization, is a technology that allows a physical network device to be partitioned into multiple virtual devices that can be assigned to different virtual machines or containers, bypassing the hypervisor and improving the network performance and efficiency. Containerization is the process of packaging an application and its dependencies into a lightweight and portable unit that can run on any platform, providing isolation, consistency, and portability.
References:
? CompTIA Cloud+ CV0-003 Study Guide, Chapter 4: Network Optimization, Section 4.1: Content Delivery Networks, Page 17523
? CompTIA Cloud+ CV0-003 Study Guide, Chapter 4: Network Optimization, Section 4.2: Autoscaling, Page 180
? CompTIA Cloud+ CV0-003 Study Guide, Chapter 4: Network Optimization, Section 4.3: SR-IOV, Page 184
? CompTIA Cloud+ CV0-003 Study Guide, Chapter 4: Network Optimization, Section 4.4: Containerization, Page 187
? What is a CDN?

NEW QUESTION 233
- (Topic 4)
A systems administrator has a redundant backup system in place. Which of the following should the systems administrator perform to maintain efficient operation and comply with the global standard in the corporate backup policies?

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

Answer: C

NEW QUESTION 235
- (Topic 4)
A VDI administrator is deploying 512 desktops for remote workers. Which of the following would meet the minimum number of IP addresses needed for the desktops?

A. /22
B. /23
C. /24
D. /25

Answer: B

Explanation:
A /23 subnet mask has 9 bits for the host portion, which allows up to 512 IP addresses for the desktops. A /22 subnet mask has 10 bits for the host portion, which allows up to 1024 IP addresses, but this is more than the minimum required. A /24 subnet mask has 8 bits for the host portion, which allows up to 256 IP addresses, but this is not enough for the desktops. A /25 subnet mask has 7 bits for the host portion, which allows up to 128 IP addresses, but this is also not enough for the desktops. References: CompTIA Cloud+ Certification Exam Objectives, Domain 1.0: Cloud Concepts, Objective 1.2: Given a scenario, analyze and compare the characteristics of various cloud service models (SaaS, IaaS, PaaS). Subnet Mask Cheat Sheet - aelius.com

NEW QUESTION 237
- (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 239
.....

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