CompTIA

Exam Questions CV0-003

CompTIA Cloud+ Certification Exam

About Exambible

Your Partner of IT Exam

Found in 1998

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

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

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

NEW QUESTION 1
- (Topic 1)
An organization is running a database application on a SATA disk, and a customer is experiencing slow performance most of the time.
Which of the following should be implemented to improve application performance?

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

Answer: D

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

NEW QUESTION 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 systems administrator disabled TLS 1.0 and 1.1, as well as RC4, 3DES, and AES-128 ciphers for TLS 1.2, on a web server. A client now reports being unable to access the web server, but the administrator verifies that the server is online, the web service is running, and other users can reach the server as well.
Which of the following should the administrator recommend the user do FIRST?

A. Disable antivirus/anti-malware software
B. Turn off the software firewall
C. Establish a VPN tunnel between the computer and the web server
D. Update the web browser to the latest version

Answer: D

Explanation:
Updating the web browser to the latest version is the first action that the user should do when experiencing a connection timeout error after the administrator configured a redirect from HTTP to HTTPS on the web server. Updating the web browser can ensure that it supports the latest security protocols and standards, such as TLS 1.2 or 1.3, which are required for HTTPS connections. If the web browser is outdated or incompatible with the security protocols or standards used by the web server, it may fail to establish a secure connection and result in a connection timeout error. References: CompTIA Cloud+ Certification Exam Objectives, page 15, section 2.8

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 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 6
- (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 7
- (Topic 1)
A company has deployed a new cloud solution and is required to meet security compliance.
Which of the following will MOST likely be executed in the cloud solution to meet security requirements?

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

Answer: C

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

NEW QUESTION 8
- (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 9
- (Topic 1)
An organization is hosting a cloud-based web server infrastructure that provides web- hosting solutions. Sudden continuous bursts of traffic have caused the web servers to saturate CPU and network utilizations.

Which of the following should be implemented to prevent such disruptive traffic from reaching the web servers?

A. Solutions to perform NAC and DLP
B. DDoS protection
C. QoS on the network
D. A solution to achieve microsegmentation

Answer: B

Explanation:
Distributed denial-of-service (DDoS) protection is a type of security solution that detects and mitigates DDoS attacks that aim to overwhelm or disrupt a system or service by sending large volumes of traffic from multiple sources. DDoS protection can prevent such disruptive traffic from reaching the web servers by filtering out malicious or unwanted traffic and allowing only legitimate traffic to pass through. DDoS protection can also help maintain the availability and functionality of web services and applications during a DDoS attack. References: CompTIA Cloud+ Certification Exam Objectives, page 14, section 2.7
Reference: https://blog.paessler.com/the-top-5-causes-of-sudden-network-spikes

NEW QUESTION 10
- (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 10
- (Topic 1)
A company has a cloud infrastructure service, and the cloud architect needs to set up a DR site.
Which of the following should be configured in between the cloud environment and the DR site?

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

Answer: D

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

NEW QUESTION 11
- (Topic 1)
A systems administrator recently upgraded the processors in a web application host. Upon the next login, the administrator sees a new alert regarding the license being out of compliance.
Which of the following licensing models is the application MOST likely using?

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

Answer: C

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

NEW QUESTION 14
- (Topic 1)
A systems administrator is provisioning VMs in a cloud environment and has been told to select an OS build with the furthest end-of-life date.
Which of the following OS builds would be BEST for the systems administrator to use?

A. Open-source
B. LTS
C. Canary
D. Beta
E. Stable

Answer: B

Explanation:
Long-term support (LTS) is a type of release cycle that provides extended support and maintenance for software products or operating systems. LTS releases typically have longer end-of-life dates than regular releases, as they receive security updates, bug fixes, and patches for several years after their initial release date. LTS releases can also offer higher stability, reliability, and compatibility than regular releases, as they undergo more testing and quality assurance processes before being released. LTS is the best OS build for a systems administrator to use when provisioning VMs in a cloud environment and being told to select an OS build with the furthest end-of-life date. References: CompTIA Cloud+ Certification Exam Objectives, page 11, section 1.6

NEW QUESTION 17
- (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 20
- (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 24
- (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 26
- (Topic 2)
A company is concerned about the security of its data repository that contains customer PII. A systems administrator is asked to deploy a security control that will prevent the exfiltration of such data. Which of the following should the systems administrator implement?

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

Answer: A

Explanation:
Reference: https://cloud.google.com/blog/products/identity-security/4-steps-to-stop-data- exfiltration-with-google-cloud
Implementing DLP (Data Loss Prevention) is the best solution to prevent the exfiltration of customer PII (Personally Identifiable Information) from a data repository. DLP is a security control that monitors, detects, and blocks sensitive data from leaving or being accessed by unauthorized parties. DLP can be applied at different levels, such as network, endpoint, storage, or cloud. DLP can help to protect customer PII from being leaked, stolen, or compromised.

NEW QUESTION 29
- (Topic 2)
A cloud solutions architect needs to determine the best strategy to deploy an application environment in production, given the following requirements:
No downtime
Instant switch to a new version using traffic control for all users
Which of the following deployment strategies would be the BEST solution?

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

Answer: B

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

NEW QUESTION 32
- (Topic 2)
A database analyst reports it takes two hours to perform a scheduled job after onboarding 10,000 new users to the system. The analyst made no changes to the scheduled job before or after onboarding the users. The database is hosted in an IaaS instance on a cloud provider. Which of the following should the cloud administrator evaluate to troubleshoot the performance of the job?

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

Answer: A

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

NEW QUESTION 34
- (Topic 2)
Some VMs that are hosted on a dedicated host server have each been allocated with 32GB of memory. Some of VMs are not utilizing more than 30% of the allocation. Which of the following should be enabled to optimize the memory utilization?

A. Auto-scaling of compute
B. Oversubscription
C. Dynamic memory allocations on guests
D. Affinity rules in the hypervisor

Answer: C

Explanation:
Enabling dynamic memory allocations on guests is the best option to optimize memory utilization for VMs that have been allocated with 32GB of memory but are not utilizing more than 30% of it. Dynamic memory allocation is a feature that allows a VM to adjust its memory usage according to its workload and demand, without requiring a reboot or manual intervention. Dynamic memory allocation can help to improve memory utilization and efficiency by allocating more memory to VMs that need it and releasing memory from VMs that do not need it.

NEW QUESTION 39
- (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 40
- (Topic 2)
A company has an in-house-developed application. The administrator wants to utilize cloud services for additional peak usage workloads. The application has a very unique stack of dependencies.
Which of the following cloud service subscription types would BEST meet these requirements?

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

Answer: D

Explanation:
IaaS (Infrastructure as a Service) 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 applications that have a unique stack of dependencies that may not be supported by other cloud service models.

NEW QUESTION 42
- (Topic 2)
A private IaaS administrator is receiving reports that all newly provisioned Linux VMs are running an earlier version of the OS than they should be. The administrator reviews the automation scripts to troubleshoot the issue and determines the scripts ran successfully. Which of the following is the MOST likely cause of the issue?

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

Answer: C

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

NEW QUESTION 47
- (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 48
- (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 50
- (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 53
- (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 55
- (Topic 2)
A systems administrator is troubleshooting performance issues with a VDI environment. The administrator determines the issue is GPU related and then increases the frame buffer on the virtual machines. Testing confirms the issue is solved, and everything is now working correctly. Which of the following should the administrator do NEXT?

A. Consult corporate policies to ensure the fix is allowed

B. Conduct internal and external research based on the symptoms
C. Document the solution and place it in a shared knowledge base
D. Establish a plan of action to resolve the issue

Answer: C

Explanation:
Documenting the solution and placing it in a shared knowledge base is what the administrator should do next after troubleshooting performance issues with a VDI (Virtual Desktop Infrastructure) environment, determining that the issue is GPU (Graphics Processing Unit) related, increasing the frame buffer on the virtual machines, and testing that confirms that the issue is solved and everything is now working correctly. Documenting the solution is a process of recording and describing what was done to fix or resolve an issue, such as actions, steps, methods, etc., as well as why and how it worked. Placing it in a shared knowledge base is a process of storing and organizing documented solutions in a central location or repository that can be accessed and used by others. Documenting the solution and placing it in a shared knowledge base can provide benefits such as:
? Learning: Documenting the solution and placing it in a shared knowledge base can help to learn from past experiences and improve skills and knowledge.
? Sharing: Documenting the solution and placing it in a shared knowledge base can help to share information and insights with others who may face similar issues or situations.
? Reusing: Documenting the solution and placing it in a shared knowledge base can help to reuse existing solutions for future issues or situations.

NEW QUESTION 59
- (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 64
- (Topic 2)
Which of the following service models would be used for a database in the cloud?

A. PaaS
B. laaS
C. CaaS
D. SaaS

Answer: A

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

NEW QUESTION 67
- (Topic 2)
A company needs a solution to find content in images. Which of the following technologies, when used in conjunction with cloud services, would facilitate the BEST solution?

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

Answer: C

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

NEW QUESTION 68

- (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 71
- (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 76
- (Topic 2)
A cloud provider wants to make sure consumers are utilizing its IaaS platform but prevent them from installing a hypervisor on the server. Which of the following will help the cloud provider secure the environment and limit consumers' activity?

A. Patch management
B. Hardening
C. Scaling
D. Log and event monitoring

Answer: B

Explanation:
Hardening is the best option to help the cloud provider secure the environment and limit consumers' activity on its IaaS platform. Hardening is a process of reducing the attack surface and vulnerabilities of a system or device by applying security configurations, patches, updates, policies, rules, etc. Hardening can prevent consumers from installing unauthorized or unsupported software on their cloud servers, such as hypervisors.

NEW QUESTION 78
- (Topic 2)
An administrator is securing a private cloud environment and wants to ensure only approved systems can connect to switches. Which of the following would be MOST useful to accomplish this task?

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

Answer: D

Explanation:

Reference: https://www.cisco.com/c/en/us/products/security/what-is-network-access- control-nac.html
NAC (Network Access Control) is what the administrator should implement to ensure only approved systems can connect to switches in a private cloud environment. NAC is a security technique that controls and restricts access to network resources based on predefined policies or rules. NAC can verify and authenticate users or devices before granting them access to switches or other network devices. NAC can also enforce compliance and security standards on users or devices before allowing them to connect to switches.

NEW QUESTION 83
- (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 86
- (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 87
- (Topic 2)
A cloud administrator set up a link between the private and public cloud through a VPN tunnel. As part of the migration, a large set of files will be copied. Which of the following network ports are required from a security perspective?

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

Answer: B

Explanation:
These are the network ports that are required from a security perspective to copy a large set of files between the private and public cloud through a VPN tunnel. A VPN (Virtual Private Network) tunnel is a secure and encrypted connection that allows data to be transferred between two networks or locations over the public internet. To copy files between the private and public cloud, the following ports are needed:
? Port 22: This is the port used by SSH (Secure Shell) protocol, which is a method of remotely accessing and managing cloud resources or systems using a command- line interface. SSH can also be used to securely transfer files using SCP (Secure Copy Protocol) or SFTP (SSH File Transfer Protocol).
? Port 443: This is the port used by HTTPS (Hypertext Transfer Protocol Secure), which is a protocol that encrypts and secures web traffic. HTTPS can also be used to transfer files using web browsers or tools such as curl or wget.
? Port 445: This is the port used by SMB (Server Message Block) protocol, which is a protocol that allows file sharing and access over a network. SMB can also be used to transfer files using tools such as robocopy or rsync.

NEW QUESTION 89
- (Topic 1)
A web server has been deployed in a public IaaS provider and has been assigned the public IP address of 72.135.10.100. Users are now reporting that when they browse to the website, they receive a message indicating the service is unavailable. The cloud administrator logs into the server, runs a netstat command, and notices the following relevant output:

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

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

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

Answer: D

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

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

NEW QUESTION 93
- (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

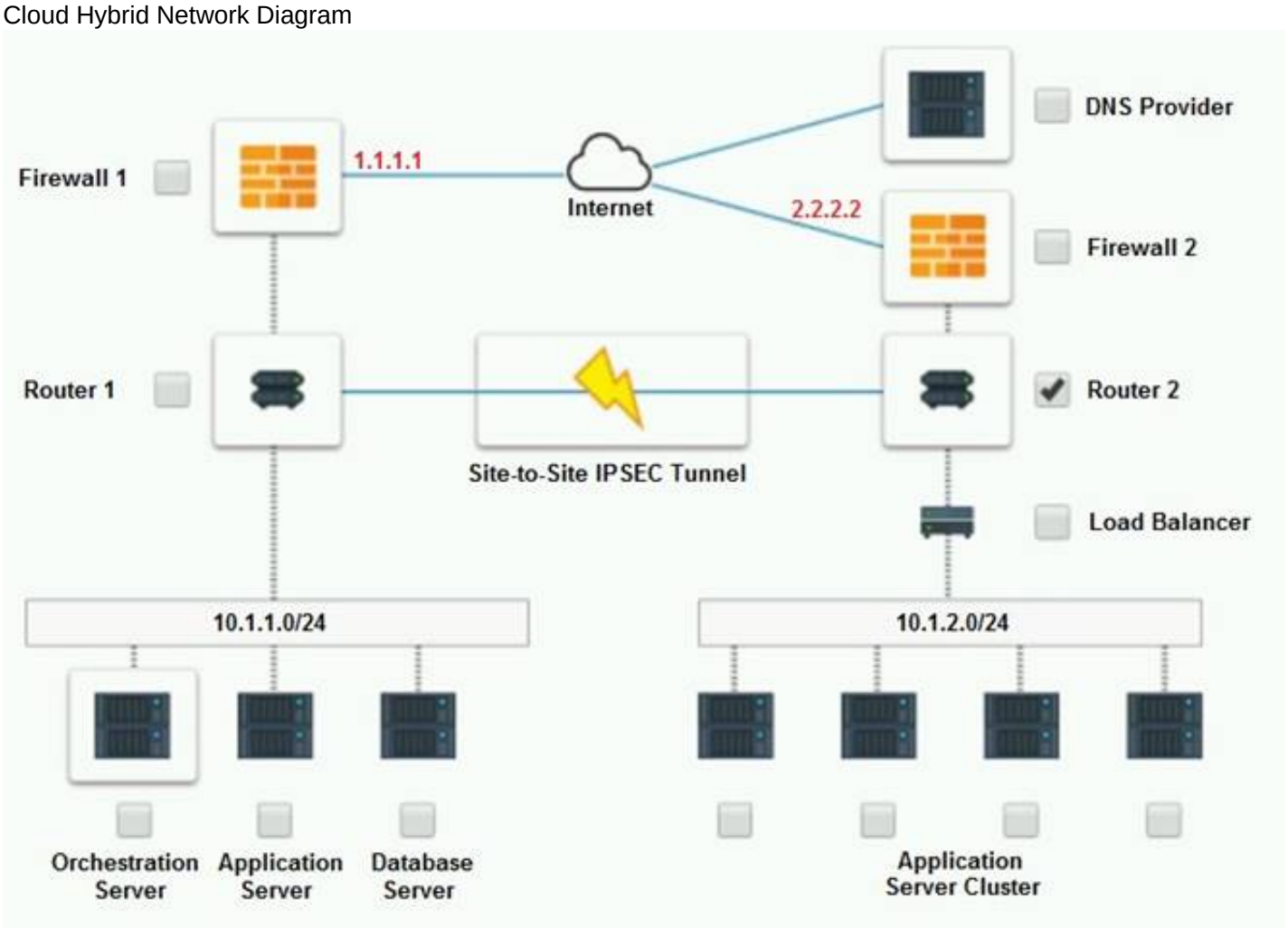
Answer: C

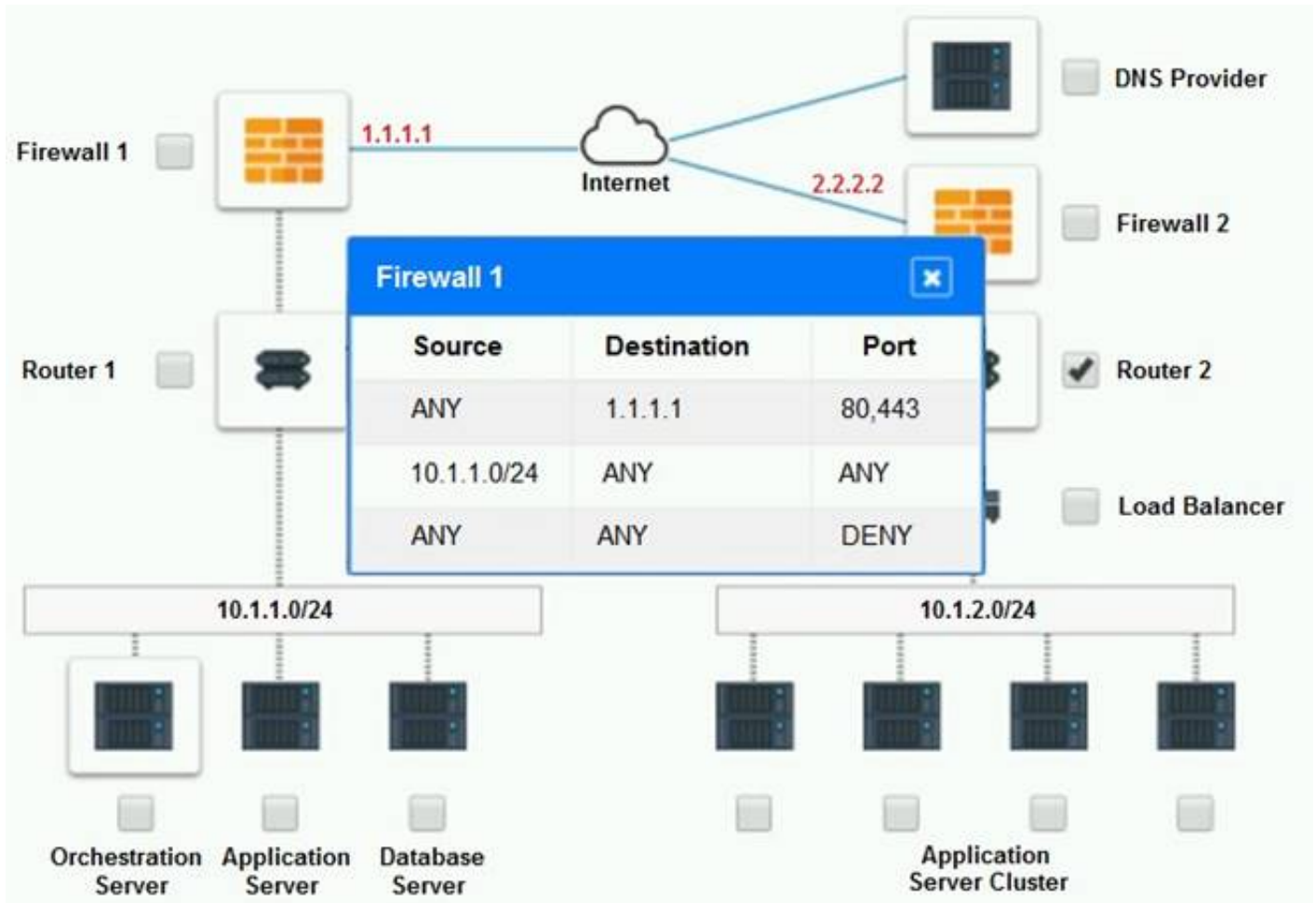
Explanation:
Identity federation is a type of authentication mechanism that allows users to access multiple systems or applications across different domains or organizations with a single login credential. Identity federation can help integrate the cloud resources of Company A and Company B after Company 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

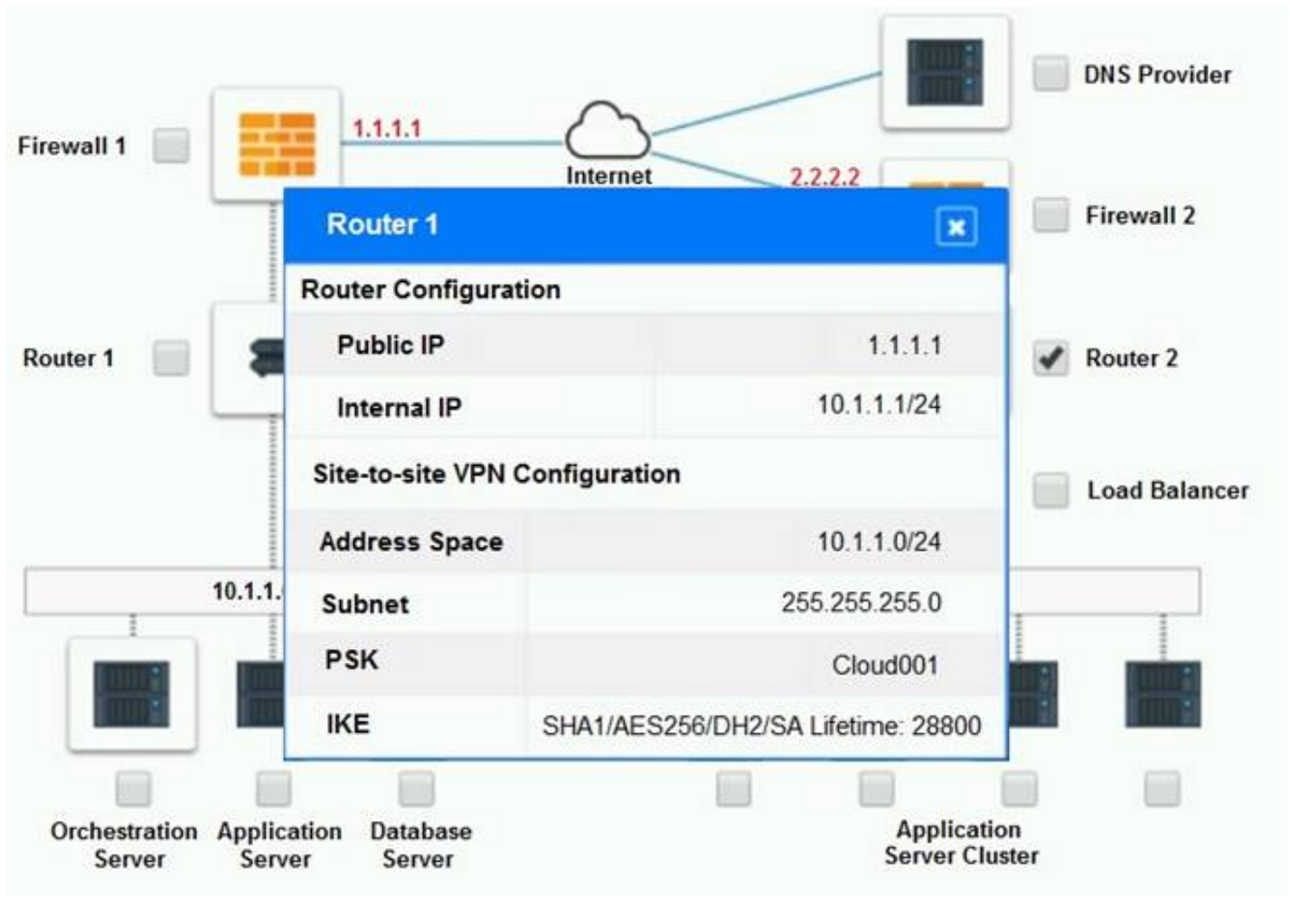
NEW QUESTION 98
SIMULATION - (Topic 1)
A company has decided to scale its e-commerce application from its corporate datacenter to a commercial cloud provider to meet an anticipated increase in demand during an upcoming holiday.
The majority of the application load takes place on the application server 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).

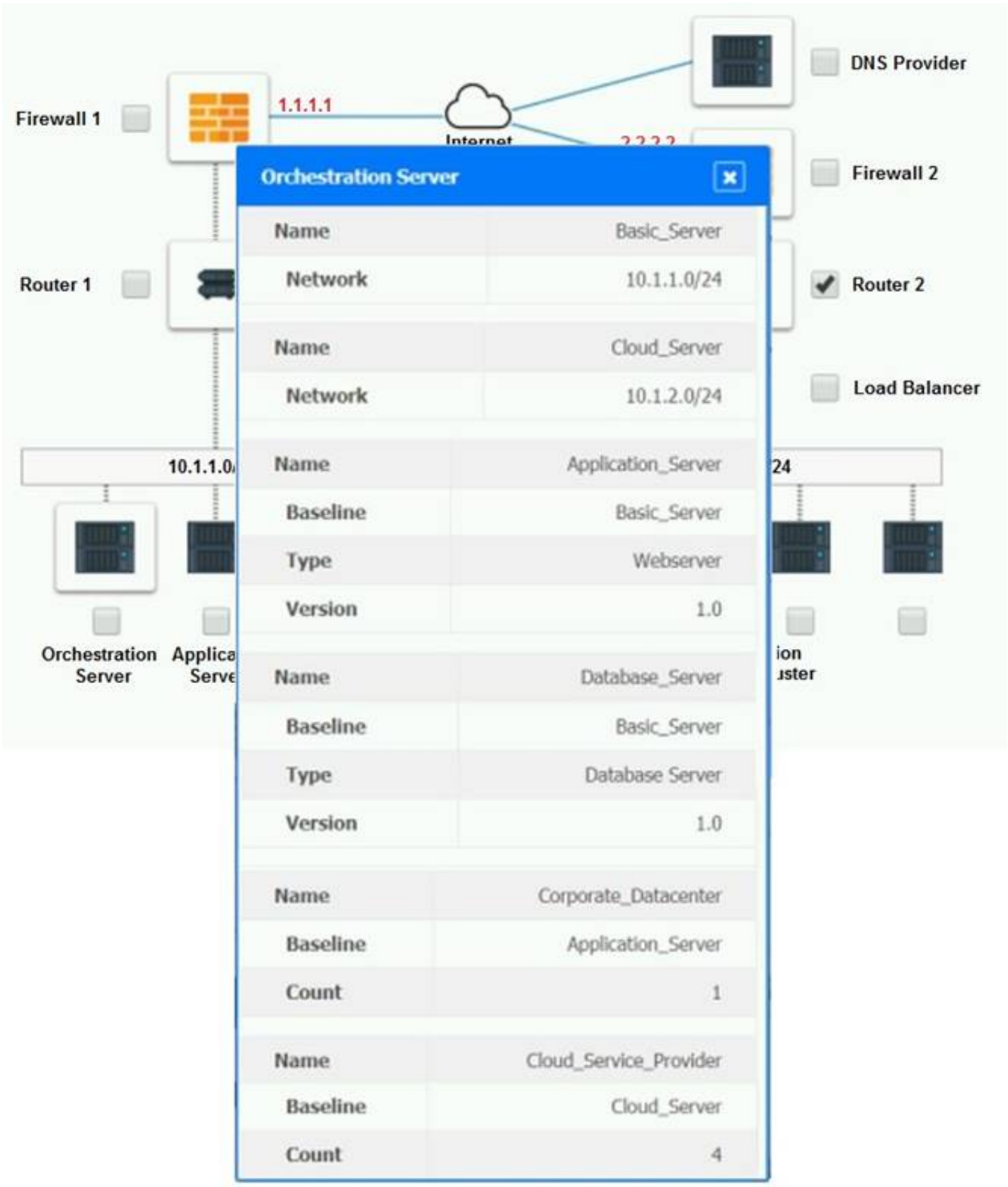
Part 2:
- Identify the correct options to provide adequate configuration for hybrid cloud architecture.

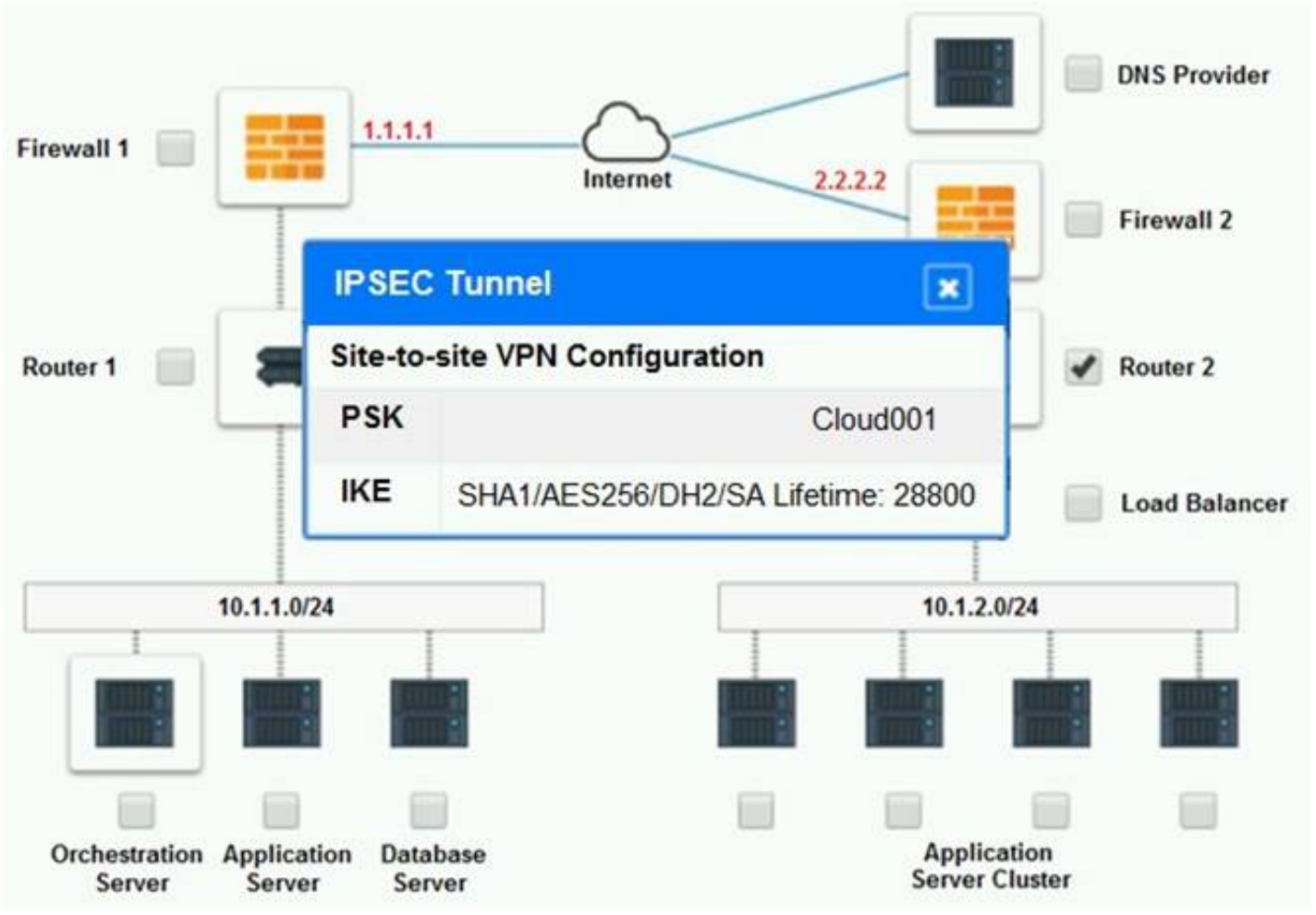
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.
Part 1:
Cloud Hybrid Network Diagram

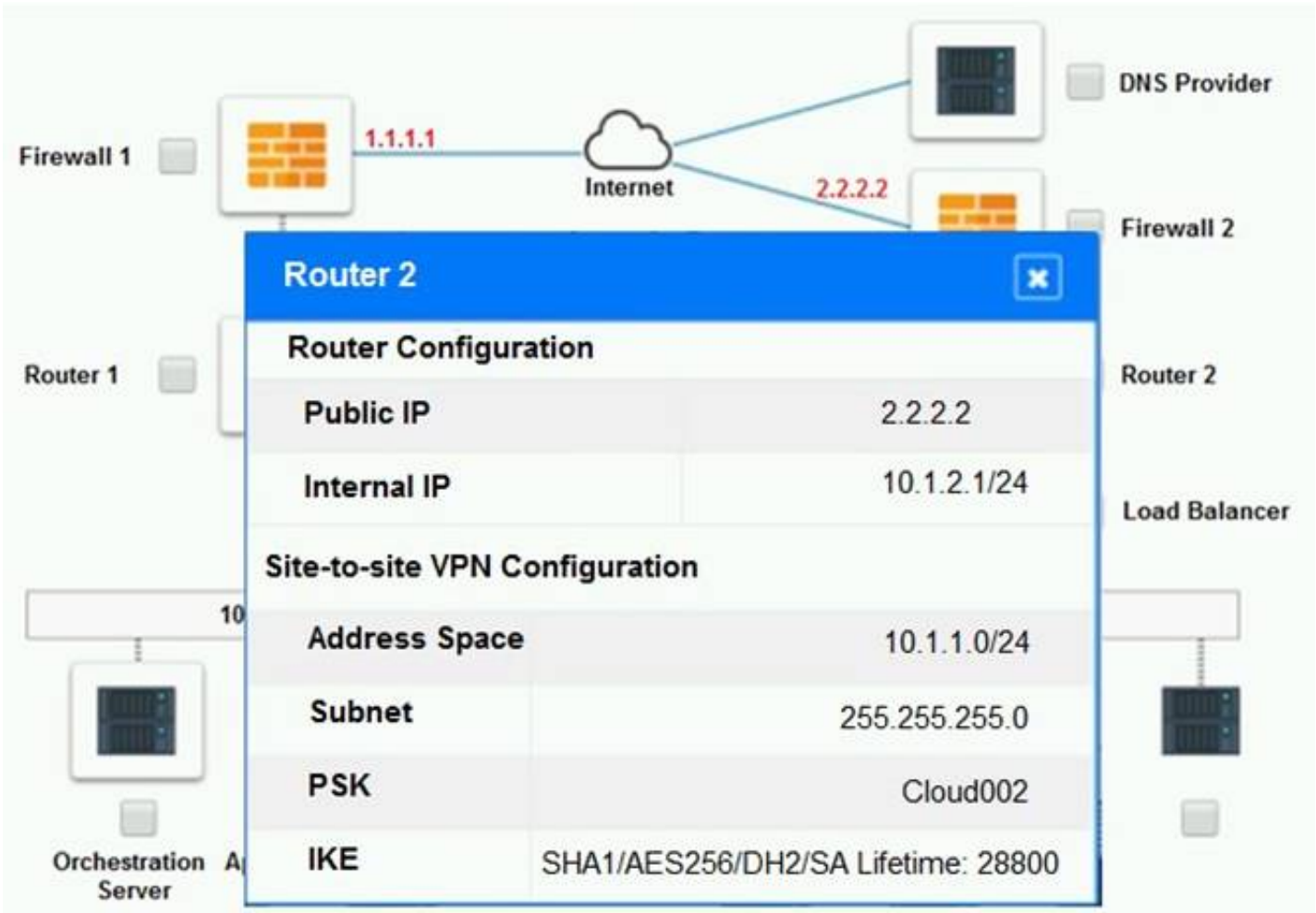


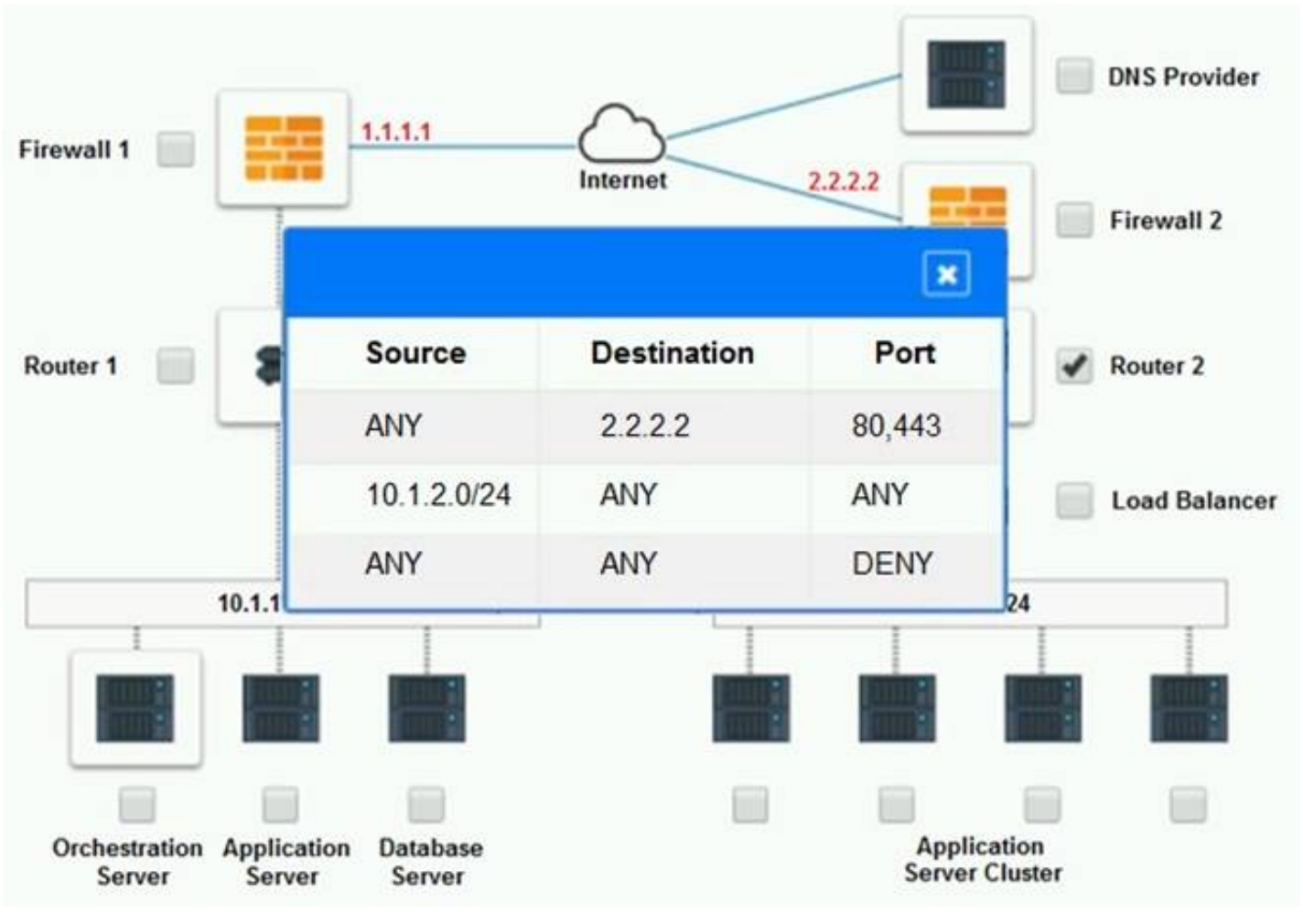

Firewall 1
1.1.1.1
Internet
2.2.2.2
DNS Provider
Firewall 2
Router 1
Router 2
Load Balancer
Firewall 1
Source
Destination
Port
ANY
1.1.1.1
80,443
10.1.1.0/24
ANY
ANY
ANY
ANY
DENY
10.1.1.0/24
10.1.2.0/24
Orchestration Server
Application Server
Database Server
Application Server Cluster

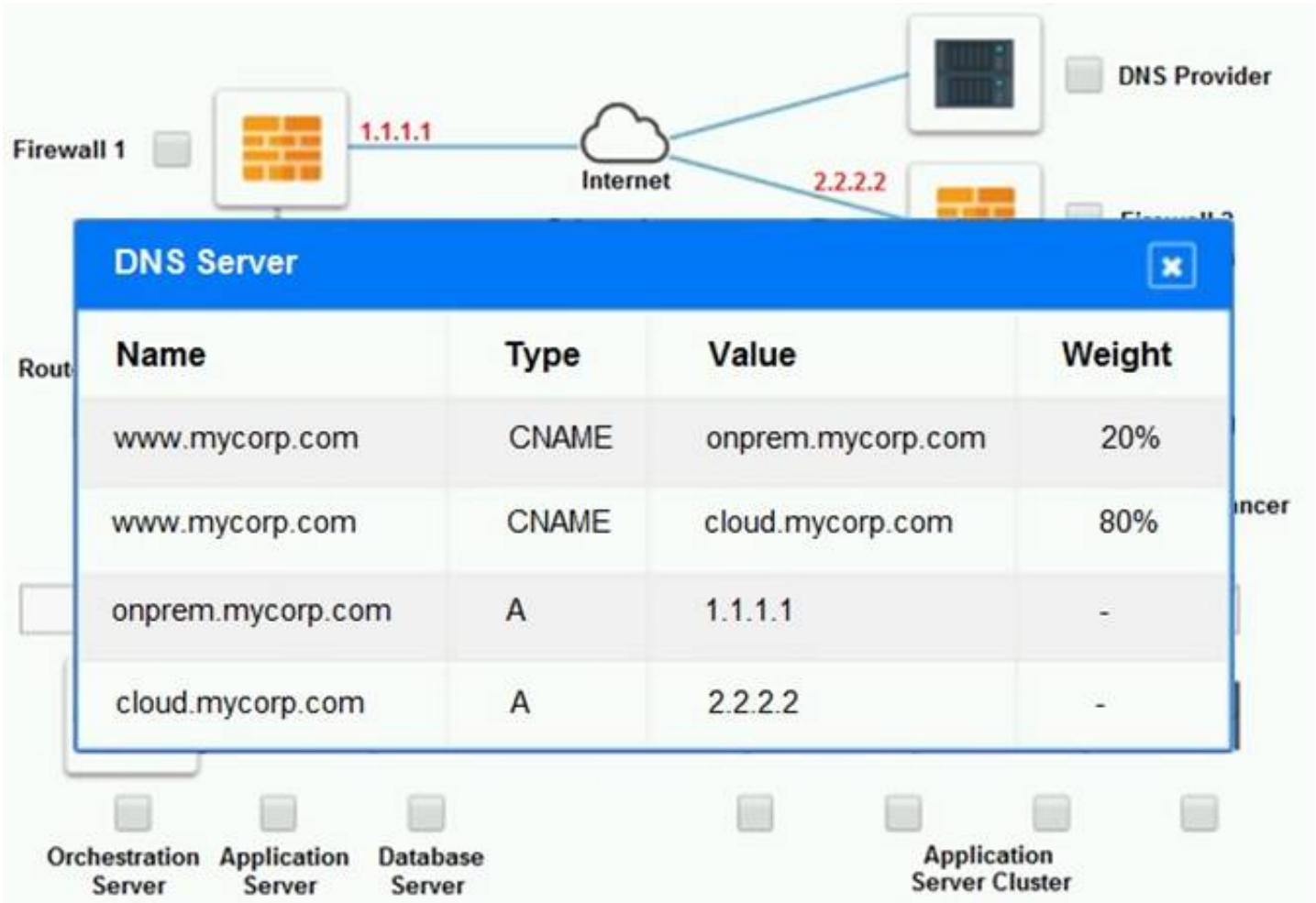

Firewall 1
1.1.1.1
Internet
2.2.2.2
DNS Provider
Firewall 2
Router 1
Router 2
Load Balancer
Router 1
Router Configuration
Public IP
1.1.1.1
Internal IP
10.1.1.1/24
Site-to-site VPN Configuration
Address Space
10.1.1.0/24
Subnet
255.255.255.0
PSK
Cloud001
IKE
SHA1/AES256/DH2/SA Lifetime: 28800
Orchestration Server
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
10.1.1.0
24
Orchestration Server
Applica Serve
ion
uster
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


DNS Provider
Firewall 1
1.1.1.1
Internet
2.2.2.2
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 1
Router 2
Load Balancer
Orchestration Server
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


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



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 100
- (Topic 1)
A cloud architect is designing the VPCs for a new hybrid cloud deployment. The business requires the following:
? High availability
? Horizontal auto-scaling
? 60 nodes peak capacity per region
? Five reserved network IP addresses per subnet
? /24 range
Which of the following would BEST meet the above requirements?

A. Create two /25 subnets in different regions
B. Create three /25 subnets in different regions
C. Create two /26 subnets in different regions
D. Create three /26 subnets in different regions
E. Create two /27 subnets in different regions
F. Create three /27 subnets in different regions

Answer: C

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

NEW QUESTION 101
- (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 104
- (Topic 1)
A systems administrator is reviewing two CPU models for a cloud deployment. Both CPUs have the same number of cores/threads and run at the same clock speed.
Which of the following will BEST identify the CPU with more computational power?

A. Simultaneous multithreading
B. Bus speed
C. L3 cache
D. Instructions per cycle

Answer: D

Explanation:
Instructions per cycle (IPC) is a metric that measures how many instructions a CPU can execute in one clock cycle. IPC can help identify the CPU with more computational power when comparing two CPU models that have the same number of cores/threads and run at the same clock speed, as it indicates the efficiency and performance of the CPU architecture and design. A higher IPC means that the CPU can process more instructions in less time, resulting in faster and better performance. References: CompTIA Cloud+ Certification Exam Objectives, page 9, section 1.4
Reference: https://en.wikipedia.org/wiki/Central_processing_unit

NEW QUESTION 106
- (Topic 1)
A SaaS provider wants to maintain maximum availability for its service. Which of the following should be implemented to attain the maximum SLA?

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

Answer: B

Explanation:
An active-active site is a type of disaster recovery (DR) site that runs simultaneously with the primary site and handles part of the normal workload or traffic. An

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

NEW QUESTION 109
- (Topic 1)
An organization's web server farm, which is hosted in the cloud with DNS load balancing, is experiencing a spike in network traffic. This has caused an outage of the organization's web server infrastructure.
Which of the following should be implemented to prevent this in the future as a mitigation method?

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

Answer: D

Explanation:
A virtual application delivery controller (vADC) is a type of network device or software that provides load balancing, security, and optimization for web applications or services. Deploying a vADC appliance can help prevent an outage of the organization's web server infrastructure due to a spike in network traffic, as it can distribute the traffic across multiple web servers and improve the performance and availability of web applications or services. Deploying a vADC appliance can also provide mitigation methods such as DDoS protection, SSL offloading, and caching to enhance the security and efficiency of web traffic delivery. References: CompTIA Cloud+ Certification Exam Objectives, page 15, section 2.8

NEW QUESTION 110
- (Topic 1)
A systems administrator for an e-commerce company will be migrating the company's main website to a cloud provider. The principal requirement is that the website must be highly available.
Which of the following will BEST address this requirement?

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

Answer: B

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

NEW QUESTION 112
- (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 113
- (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 116
- (Topic 4)
A cloud engineer is deploying a server in a cloud platform. The engineer reviews a security scan report. Which of the following recommended services should be disabled? (Select two).

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

Answer: AB

Explanation:
Telnet and FTP are recommended services to be disabled when deploying a server in a cloud platform, as they are insecure protocols that transmit data in plain text and expose credentials and sensitive information to potential attackers12. Remote log-in, DNS, DHCP, and LDAP are not necessarily recommended to be disabled, as they may provide useful functionality for the server and the cloud environment. However, they should be configured properly and secured with encryption, authentication, and authorization mechanisms34.
References: CompTIA Cloud+ CV0-003 Exam Objectives, Objective 4.2: Given a scenario, apply security configurations and compliance controls ; CompTIA Quick Start Guide to Tackling Cloud Security Concerns3

NEW QUESTION 118
- (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 120
- (Topic 4)
A company uses multiple SaaS-based cloud applications. All the applications require authentication upon access. An administrator has been asked to address this issue and enhance security. Which of the following technologies would be the BEST solution?

A. Single sign-on
B. Certificate authentication
C. Federation
D. Multifactor authentication

Answer: A

Explanation:
Single sign-on (SSO) is a technology that allows a user to access multiple applications or services with a single login and authentication process. SSO can enhance security by reducing the number of passwords that a user has to remember and enter, and by enabling centralized management and enforcement of security policies .
SSO can help address the issue of multiple SaaS-based cloud applications requiring authentication upon access. By implementing SSO, an administrator can:
Simplify the user experience and increase productivity by eliminating the need to enter multiple usernames and passwords for different applications .
Improve the security and compliance of the applications by using a trusted identity provider (IdP) that can verify the user’s identity and credentials, and grant or deny access based on predefined rules .
Reduce the risk of password breaches, phishing, or identity theft by minimizing the exposure of passwords to third-party applications or malicious actors .

NEW QUESTION 122

- (Topic 4)
An organization deployed an application using a cloud provider's internal managed certificates. Developers are unable to retrieve data when calling the API from any machine.
The following error message is in the log:
12-04-2023-10:05:25, SSL Negotiation Error 12-04-2023-10:05:28,Invalid Certificate
12-04-2023-10:05:29, TLS Handshake Failed 12-04-2023-10:05:30,Connection Closed
Which of the following is the most likely cause of the error?

A. TLS version
B. Insecure cipher
C. Self-signed certificate
D. Root trust

Answer: D

Explanation:
The error message indicates that the SSL/TLS handshake failed due to an invalid certificate. This means that the client machine does not trust the certificate authority (CA) that issued the certificate for the cloud provider’s API. A self-signed certificate or an insecure cipher would not cause this error, as they would be detected during the certificate validation process. The TLS version is not relevant, as the error occurs before the protocol negotiation. The most likely cause of the error is that the client machine does not have the root CA certificate installed in its trust store, or that the cloud provider’s certificate chain is incomplete or broken. To fix the error, the client machine needs to install the root CA certificate or the cloud provider needs to fix its certificate chain. References: The Official CompTIA Cloud+ Self-Paced Study Guide (CV0-003) eBook, Chapter 6, Section 6.2, page 2321

NEW QUESTION 126
- (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 129
- (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 133
- (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 135
- (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 140
- (Topic 4)
A company has a web application running in an on-premises environment that needs to be migrated to the cloud. The company wants to implement a solution that maximizes scalability, availability, and security, while requiring no infrastructure administration. Which of the following services would be BEST to meet this goal?

A. A PaaS solution
B. A hybrid solution
C. An laaS solution

D. A SaaS solution

Answer: A

Explanation:
A PaaS solution, or platform as a service, is a cloud computing service that provides a complete, ready-to-use, cloud-hosted platform for developing, running, maintaining and managing applications1. A PaaS solution would meet the company's goal of maximizing scalability, availability, and security, while requiring no infrastructure administration, because:
Scalability: A PaaS solution can automatically scale up or down the resources needed to run the application based on the demand and traffic. The company does not need to worry about provisioning or managing servers, storage, network, or load balancers23.
Availability: A PaaS solution can ensure high availability and reliability of the application by replicating it across multiple regions and zones. The company does not need to worry about backup, recovery, or failover23.
Security: A PaaS solution can provide built-in security features such as encryption, authentication, authorization, and firewall. The company does not need to worry about installing or updating security patches or software23.
No infrastructure administration: A PaaS solution can abstract away the underlying infrastructure and hardware from the company. The company only needs to focus on developing and deploying the application code and data. The PaaS provider takes care of the rest23.
A hybrid solution (B) is a cloud computing service that combines on-premises and cloud resources. It may offer some benefits such as flexibility and cost optimization, but it would not meet the company's goal of requiring no infrastructure administration. The company would still need to manage and maintain the on-premises part of the solution4.
An IaaS solution ©, or infrastructure as a service, is a

NEW QUESTION 143
- (Topic 4)
A cloud solutions architect has an environment that must only be accessed during work hours. Which of the following processes should be automated to BEST reduce cost?

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

Answer: C

Explanation:
One of the main benefits of cloud computing is that you only pay for the resources that you use. However, this also means that you need to manage your cloud resources efficiently and avoid paying for idle or unused resources1.
Shutting down the environment after work hours is a process that can be automated to best reduce cost in a cloud environment that must only be accessed during work hours. This process involves stopping or terminating the cloud resources, such as virtual machines, databases, load balancers, etc., that are not needed outside of the work hours. This can significantly reduce the cloud bill by avoiding charges for compute, storage, network, and other services that are not in use2.
The other options are not the best processes to automate to reduce cost in this scenario:
? Option A: Scaling of the environment after work hours. Scaling is a process that involves adjusting the number or size of cloud resources to match the demand or workload. Scaling can be done manually or automatically using triggers or policies. Scaling can help optimize the performance and availability of a cloud environment, but it does not necessarily reduce the cost. Scaling down the environment after work hours may reduce some costs, but it may still incur charges for the remaining resources. Scaling up the environment before work hours may increase the cost and also introduce delays or errors in provisioning new resources3.
? Option B: Implementing access control after work hours. Access control is a process that involves defining and enforcing rules and policies for who can access what resources in a cloud environment. Access control can help improve the security and compliance of a cloud environment, but it does not directly affect the cost. Implementing access control after work hours may prevent unauthorized access to the environment, but it does not stop or terminate the resources that are still running and consuming cloud services4.
? Option D: Blocking external access to the environment after work hours. Blocking external access is a process that involves restricting or denying network traffic from outside sources to a cloud environment. Blocking external access can help protect the environment from potential attacks or breaches, but it does not impact the cost. Blocking external access after work hours may prevent unwanted requests or connections to the environment, but it does not shut down or release the resources that are still active and generating cloud charges.

NEW QUESTION 146
- (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 149
- (Topic 4)
A cloud architect is reviewing the design for a new cloud-based ERP solution. The solution consists of eight servers with a single network interface. The allocated IP range is 172.16.0.0/28. One of the requirements of the solution is that it must be able to handle the potential addition of 16 new servers to the environment. Because of the complexity of the firewall and related ACL requirements, these new servers will need to be in the same network range. Which of the following changes
would allow for the potential server addition?

A. Change the IP address range to use a 10.0.0.0 address.
B. Change the server template to add network interfaces.
C. Change the subnet mask to use a 255.255.255.128 range.
D. Change the server scaling configuration to increase the maximum limit.

Answer: C

Explanation:
Changing the subnet mask to use a 255.255.255.128 range would allow for the potential server addition. The current subnet mask of 255.255.255.240 (/28) only allows for 14 usable host addresses in the 172.16.0.0 network, which is not enough to accommodate the existing eight servers and the possible 16 new servers. Changing the subnet mask to 255.255.255.128 (/25) would increase the number of usable host addresses to 126 in the same network, which is sufficient to handle the server expansion. Changing the IP address range to use a 10.0.0.0 address, changing the server template to add network interfaces, or changing the server scaling configuration to increase the maximum limit would not solve the issue of the limited host addresses in the same network range. References: CompTIA Cloud+ CV0-003 Certification Study Guide, Chapter 3, Objective 3.1: Given a scenario, implement cloud networking solutions.

NEW QUESTION 151
- (Topic 4)
During a security incident on an laaS platform, which of the following actions will a systems administrator most likely take as part of the containment procedure?

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

Answer: B

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

NEW QUESTION 154
- (Topic 4)
A systems administrator is planning to deploy a database cluster in a virtualization environment. The administrator needs to ensure the database nodes do not exist on the same physical host. Which of the following would best meet this requirement?

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

Answer: B

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

NEW QUESTION 159
- (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 164
- (Topic 4)
A systems administrator is troubleshooting issues with audio lag during phone conferences. When looking at the core switch, the administrator notices its buffers are consistently full, and packets are being dropped due to the large number being sent and received. There is no room in the budget for new hardware, but it is critical that the audio lag be fixed immediately. Which of the following will most likely resolve the issue?

A. Enable compression of audio traffic.
B. Configure QoS rules for VoIP traffic.
C. Verify that the gateway uplink is not saturated.
D. Add an exception to IPS for voice traffic.

Answer: B

Explanation:
Quality of Service (QoS) rules can be configured to prioritize certain types of traffic, such as voice over IP (VoIP) traffic. This can help reduce audio lag during phone conferences by ensuring that VoIP packets are delivered faster and with less delay than other types of traffic. QoS rules can be applied at different levels of the network, such as the core switch, the router, or the firewall. By configuring QoS rules for VoIP traffic, the administrator can avoid packet drops and buffer overflows that can affect the quality of the audio. References: [CompTIA Cloud+ CV0-003 Study Guide], Chapter 3, Objective 3.2: Given a scenario, troubleshoot network connectivity issues.

NEW QUESTION 166
- (Topic 4)
An organization is conducting a performance test of a public application. The following actions have already been completed:
• The baseline performance has been established.
• A load test has passed.
• A benchmark report has been generated.
Which of the following needs to be done to conclude the performance test?

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

Answer: A

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

NEW QUESTION 167
- (Topic 4)
A company plans to publish a new application and must conform with security standards. Which of the following types of testing are most important for the systems administrator to run to assure the security and compliance of the application before publishing? (Select two).

A. Regression testing
B. Vulnerability testing
C. Usability testing
D. Functional testing
E. Penetration testing
F. Load testing

Answer: BE

Explanation:
Vulnerability testing and penetration testing are two types of security testing that can help to identify and mitigate potential risks in an application before publishing. Vulnerability testing is the process of scanning the application for known weaknesses or flaws that could be exploited by attackers. Penetration testing is the process of simulating real-world attacks on the application to test its defenses and find vulnerabilities that may not be detected by automated scans. Both types of testing can help to assure the security and compliance of the application by revealing and resolving any issues that could compromise the confidentiality, integrity, or availability of the application or its
data. References: CompTIA Cloud+ CV0-003 Study Guide, Chapter 5: Maintaining a Cloud Environment, page 221.

NEW QUESTION 172

- (Topic 4)
A systems administrator has verified that a physical switchport that is connected to a virtualization host is using all available bandwidth. Which of the following would best address this issue?

A. Port mirroring
B. Link aggregation
C. Spanning tree
D. Microsegmentation

Answer: B

Explanation:
Link aggregation is a technique that combines multiple physical links into a logical link that provides higher bandwidth and redundancy. Link aggregation can help address the issue of a physical switchport that is connected to a virtualization host using all available bandwidth by increasing the capacity and availability of the connection. Link aggregation can also balance the traffic load across the links and improve the fault tolerance of the network. Link aggregation can be implemented using protocols such as LACP (Link Aggregation Control Protocol) or static configuration. References: CompTIA Cloud+ CV0-003 Certification Study Guide, Chapter 3, Objective 3.2: Given a scenario, troubleshoot network connectivity
issues.

NEW QUESTION 175
- (Topic 4)
After an infrastructure-as-code cloud migration to an laaS environment, the cloud engineer discovers that configurations on DB servers have drifted from the corporate standard baselines. Which of the following should the cloud engineer do to best ensure configurations are restored to the baselines?

A. Utilize a template to automate and update the DB configuration.
B. Create an image of the DB, delete the previous DB server, and restore from the image.
C. Manually log in to the DB servers and update the configurations.
D. Rename and change the IP of the old DB server and rebuild a new DB server.

Answer: A

Explanation:
A template is a file that defines the desired state and configuration of a cloud resource, such as a server, a network, or a database. Infrastructure as code (IaC) is the practice of using templates to automate and manage cloud resources, rather than manually configuring them. IaC can help prevent configuration drift, which is the deviation of the actual state of a resource from the desired state defined by the template. In this scenario, the cloud engineer discovers that configurations on DB servers have drifted from the corporate standard baselines after an IaC cloud migration to an IaaS environment. The best way to ensure configurations are restored to the baselines is to utilize a template to automate and update the DB configuration. This way, the cloud engineer can apply the same template to all the DB servers, and ensure they are consistent and compliant with the corporate standards. Creating an image of the DB, deleting the previous DB server, and restoring from the image is not a good solution, as it may cause data loss, downtime, and additional costs. Manually logging in to the DB servers and updating the configurations is not a good solution, as it is time-consuming, error-prone, and not scalable. Renaming and
changing the IP of the old DB server and rebuilding a new DB server is not a good solution, as it may cause compatibility issues, network disruptions, and security risks. References: CompTIA Cloud+ CV0-003 Certification Study Guide, Chapter 23, Infrastructure as Code and Configuration Management, page 3691.

NEW QUESTION 176
- (Topic 4)
A non-critical file on a database server was deleted and needs to be recovered. A cloud administrator must use the least disruptive restoration process to retrieve the file, as the database server cannot be stopped during the business day. Which of the following restoration methods would best accomplish this goal?

A. Alternate location
B. Restore from image
C. Revert to snapshot
D. In-place restoration

Answer: D

Explanation:
In-place restoration is the process of restoring data to the same location where it was originally stored, without affecting the rest of the system. This method is suitable for recovering non-critical files that were accidentally deleted, as it does not require stopping the server or creating a new instance. In contrast, alternate location, restore from image, and revert to snapshot are more disruptive methods that involve creating a new copy of the data or the entire system, which may affect the performance or availability of the
server. References: CompTIA Cloud+ CV0-003 Certification Study Guide, Chapter 20, Backup and Restore Operations, page 3211.

NEW QUESTION 180
- (Topic 4)
A cloud administrator is reviewing the current private cloud and public laaS environment, and is building an optimization plan. Portability is of great concern for the administrator so resources can be easily moved from one environment to another.
Which of the following should the administrator implement?

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

Answer: C

Explanation:
Containers are packages of software that contain all of the necessary elements to run in any environment. Containers virtualize the operating system and run anywhere, from a private data center to the public cloud or even on a developer’s personal laptop. Containers provide an isolated environment for running applications, sharing the host OS kernel but isolating processes, file systems, and network resources. Containers package applications and their dependencies together, ensuring they run consistently across different environments, from development to production. Containers are lightweight, resource-efficient, fast, and

immutable, making them ideal for portability and scalability. By using containers, a cloud administrator can easily move resources from one environment to another without changing the code or configuration of the applications. References: CompTIA Cloud+ CV0-003 Study Guide, Chapter 2: Deploying a Cloud Environment, page 75-76; What are containers?; Portability in the Cloud: Cloud Native and Containers.

NEW QUESTION 185
- (Topic 4)
A company is preparing a hypervisor environment to implement a database cluster. One of the requirements is to share the disks between the nodes of the cluster to access the same LUN. Which of the following protocols Should the company use? (Select TWO)

A. CIFS
B. FTP
C. Iscsi
D. Raid 10
E. Nfs
F. fc

Answer: CF

Explanation:
The correct answer is C and F. iSCSI and FC.
iSCSI and FC are protocols that the company can use to share the disks between the nodes of the cluster to access the same LUN. A LUN, or logical unit number, is a unique identifier for a block of storage space that can be accessed by a host system or a cluster of systems. iSCSI and FC are both block-level protocols that allow transferring data between the storage device and the host system or cluster over a network.
iSCSI stands for Internet Small Computer System Interface, which is a protocol that uses TCP/IP to send SCSI commands over an Ethernet network. iSCSI can provide a low-cost and flexible solution for sharing disks between the nodes of the cluster, as it does not require any special hardware or cables, and can use existing network infrastructure. iSCSI can also support encryption and authentication for security purposes .
FC stands for Fibre Channel, which is a protocol that uses optical fiber cables to send SCSI commands over a dedicated network. FC can provide a high-performance and reliable solution for sharing disks between the nodes of the cluster, as it offers high bandwidth, low latency, and error correction. FC can also support zoning and masking for security purposes .
CIFS, or Common Internet File System, is a file-level protocol that allows sharing files and folders over a network. CIFS does not support sharing disks or accessing LUNs at the block level.
FTP, or File Transfer Protocol, is a protocol that allows transferring files between two systems over a network. FTP does not support sharing disks or accessing LUNs at the block level.
NFS, or Network File System, is a file-level protocol that allows sharing files and folders over a network. NFS does not support sharing disks or accessing LUNs at the block level. RAID 10, or Redundant Array of Independent Disks 10, is a storage configuration that combines mirroring and striping to provide high performance and fault tolerance. RAID 10 is not a protocol that allows sharing disks or accessing LUNs over a network.

NEW QUESTION 190
- (Topic 4)
A cloud administrator is troubleshooting an issue regarding users at one location who are reporting that their API access tokens have become invalid. The users are issued tokens based on their credentials in a federated cluster. Which of the following should the administrator check to determine the cause of this issue?

A. SAML
B. DNS
C. SSL
D. NTP

Answer: A

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

NEW QUESTION 194
- (Topic 4)
A cloud engineer is responsible for a legacy web application that runs on an on-premises VM environment. The VM environment is approaching end of life. The engineer needs to migrate the web application to the cloud as quickly as possible because the VM environment has the following limitations:
• The VM environment has a single IOGB disk.
• The VM environment still uses 10Mbps, which leaves a 100Mbps WAN connection underutilized.
• No installation media is available.
Which of the following is the best way to migrate the web application to the cloud?

A. Use the VM import connector to import the VM into the cloud.
B. Use import/export to import the VM as a snapshot and attach it to a cloud instance.
C. Use REST APIs to import an image of the VM into the cloud.
D. Use object storage to create a backup of the VM and restore data into the cloud instance.

Answer: A

Explanation:
A VM import connector is a tool that allows you to import virtual machines from your on-premises environment into the cloud using a graphical user interface. This

is the fastest and easiest way to migrate a legacy web application without requiring installation media or changing the configuration of the VM. The VM import connector can also handle the disk size and network bandwidth limitations of the on-premises VM environment. References: EC2 VM Import Connector | AWS News Blog, Import a VMware Virtual Machine to Oracle Cloud Infrastructure, 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.

NEW QUESTION 199
- (Topic 4)
A systems administrator is configuring a DNS server. Which of the following steps should a technician take to ensure confidentiality between the DNS server and an upstream DNS provider?

A. Enable DNSSEC.
B. Implement single sign-on.
C. Configure DOH.
D. Set up DNS over SSL.

Answer: C

Explanation:
DNS (Domain Name System) is a service that translates human-friendly domain names into IP addresses that can be used to communicate over the Internet1. However, DNS queries and responses are usually sent in plain text, which means that anyone who can intercept the network traffic can see the domain names that the users are requesting. This poses a threat to the confidentiality and privacy of the users and their online activities2.
To ensure confidentiality between the DNS server and an upstream DNS provider, a technician should configure DOH (DNS over HTTPS). DOH is a protocol that encrypts DNS queries and responses using HTTPS (Hypertext Transfer Protocol Secure), which is a secure version of HTTP that uses SSL/TLS (Secure Sockets Layer/Transport Layer Security) to protect the data in transit3. By using DOH, the technician can prevent eavesdropping, tampering, or spoofing of DNS traffic by malicious actors3.
The other options are not the best steps to ensure confidentiality between the DNS server and an upstream DNS provider:
? Option A: Enable DNSSEC (DNS Security Extensions). DNSSEC is a set of
extensions that add digital signatures to DNS records, which can be used to verify the authenticity and integrity of the DNS data. DNSSEC can prevent DNS cache poisoning attacks, where an attacker inserts false DNS records into a DNS server's cache, redirecting users to malicious websites. However, DNSSEC does not encrypt or hide the DNS queries and responses, so it does not provide confidentiality for DNS traffic2.
? Option B: Implement single sign-on (SSO). SSO is a mechanism that allows users
to access multiple services or applications with one set of credentials, such as a username and password. SSO can simplify the authentication process and reduce the risk of password compromise or phishing attacks. However, SSO does not affect the communication between the DNS server and an upstream DNS provider, so it does not provide confidentiality for DNS traffic.
? Option D: Set up DNS over SSL (DNS over Secure Sockets Layer). This option is
not a valid protocol for securing DNS traffic. SSL is a deprecated protocol that has been replaced by TLS (Transport Layer Security), which is more secure and robust. The correct protocol for encrypting DNS traffic using SSL/TLS is DOH (DNS over HTTPS), as explained above.

NEW QUESTION 201
FILL IN THE BLANK - (Topic 4)
?MISSING?

A.

Answer: D

Explanation:
This means that data is divided into blocks and written across multiple disks, and two additional disks are used to store parity information that can be used to reconstruct data in case of disk failure. RAID 6 can withstand the failure of up to two disks without losing any data or performance. RAID 6 also maximizes the storage capacity of its drives, as it only uses two disks for parity out of the total number of disks in the array. For example, if the array has 10 disks, RAID 6 will use 8 disks for data and 2 disks for parity, resulting in a storage capacity of 8/10 or 80% of the total disk space. RAID 6 is suitable for private cloud environments that require high availability, fault tolerance, and large storage
capacity. References: CompTIA Cloud+ CV0-003 Study Guide, Chapter 3: Storage Technologies, Section 3.2: RAID Levels, Page 125

NEW QUESTION 202
- (Topic 4)
A company has a large environment with multiple VPCs across three regions in a public cloud. The company is concerned about connectivity within the regions. Which of the following should the cloud administrator implement?

A. Peering
B. A firewall
C. Network access control
D. A load balancer

Answer: A

Explanation:
Peering is a networking technique that allows direct and private connection between two or more cloud networks without using the public Internet. Peering can help the cloud administrator improve the connectivity within the regions by reducing the latency, increasing the bandwidth, and enhancing the security of the data transfer. Peering can be implemented between VPCs within the same region or across different regions, depending on the CSP's offerings and the customer's requirements. Peering can also help reduce the network costs by avoiding the use of the Internet gateways or VPNs. References: CompTIA Cloud+ CV0-003 Certification Study Guide, Chapter 3, Objective 3.1: Given a scenario, implement cloud networking solutions.

NEW QUESTION 207
- (Topic 4)
An organization's executives would like to allow access to devices that meet the corporate security compliance levels. Which of the following criteria are most important for the organization to consider? (Select two).

A. Serial number

B. Firmware
C. Antivirus version and definition
D. OS patch level
E. CPU architecture
F. Manufacturer

Answer: CD

Explanation:
Antivirus version and definition and OS patch level are important criteria for the organization to consider when allowing access to devices that meet the corporate security compliance levels. These criteria can help ensure that the devices are protected from malware and vulnerabilities that could compromise the security of the organization's data and systems. Serial number, firmware, CPU architecture, and manufacturer are not directly related to security compliance levels, although they may be relevant for other purposes such as inventory management or compatibility.
References: CompTIA Cloud+ CV0-003 Exam Objectives, Objective 4.2: Given a scenario, apply security configurations and compliance controls1 ; CompTIA Quick Start Guide to Tackling Cloud Security Concerns2

NEW QUESTION 210
- (Topic 4)
A cloud administrator is looking at the company's cloud services bill for the previous month. The administrator notices on the billing dashboard that certain resources are not being billed to any particular department. Which of the following actions will help correct this billing issue?

A. Check the utilization of the resources.
B. Modify the chargeback details of the consumer.
C. Add the resources to the consumer monitoring group.
D. Modify the tags for all the unmapped resources.

Answer: D

Explanation:
Tags are metadata or labels that can be attached to cloud resources, such as VMs, storage, or networks. Tags can help organize, identify, and manage cloud resources, as well as track their usage and costs. Tags can also be used to implement chargeback or showback policies, which are methods of allocating the cloud services bill to different departments or consumers based on their consumption of resources .
A cloud administrator can modify the tags for all the unmapped resources to correct the billing issue. By adding or updating the tags with the relevant department or consumer name, the administrator can ensure that the resources are billed to the correct entity. The administrator can also use the tags to filter, sort, or group the resources on the billing dashboard, and generate reports or alerts based on the tags .
Checking the utilization of the resources may help identify the purpose or owner of the resources, but it will not help correct the billing issue. The administrator still needs to modify the tags for the resources to assign them to the appropriate department or consumer.
Modifying the chargeback details of the consumer may help adjust the billing rate or method for a specific consumer, but it will not help correct the billing issue. The administrator still needs to modify the tags for the resources to associate them with the consumer.
Adding the resources to the consumer monitoring group may help monitor the performance or availability of the resources for a specific consumer, but it will not help correct the billing issue. The administrator still needs to modify the tags for the resources to link them with the consumer.

NEW QUESTION 215
- (Topic 4)
A systems administrator is performing an OS upgrade on a production VM. Which of the following actions should the administrator take before the upgrade to ensure the FASTEST recovery of the system in case the upgrade fails in an unrecoverable way?

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

Answer: C

Explanation:
A snapshot is an image of your system/volume at a specific point in time. It captures the entire file system as it was when the snapshot was taken. When a snapshot is used to restore the system, the system will revert to exactly how it was at the time of the snapshot1. Snapshots are designed for short-term storage and fast recovery. They do not need a lot of storage space or time to create copies234.
Taking a snapshot of the system before the OS upgrade would ensure the fastest recovery of the system in case the upgrade fails in an unrecoverable way. The administrator could simply restore the system from the snapshot and avoid any data loss or corruption. This would be much faster and easier than performing a full backup or testing the upgrade in a preproduction environment.

NEW QUESTION 220
- (Topic 4)
A cloud engineer recently used a deployment script template to implement changes on a cloud-hosted web application. The web application communicates with a managed database on the back end. The engineer later notices the web application is no longer receiving data from the managed database. Which of the following is the most likely cause of the issue?

A. Misconfiguration in the user permissions
B. Misconfiguration in the routing traffic
C. Misconfiguration in the network ACL
D. Misconfiguration in the firewall

Answer: D

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

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

NEW QUESTION 223
- (Topic 4)
A cloud engineer recently used a deployment script template to implement changes on a cloud-hosted web application. The web application communicates with a managed database on the back end. The engineer later notices the web application is no longer receiving data from the managed database. Which of the following is the most likely cause of the issue?

A. Misconfiguration in the user permissions
B. Misconfiguration in the routing traffic
C. Misconfiguration in the network ACL
D. Misconfiguration in the firewall

Answer: D

Explanation:
A misconfiguration in the firewall is the most likely cause of the issue. A firewall is a security device or service that controls the incoming and outgoing network traffic based on predefined rules. A firewall can help protect the cloud-hosted web application and the managed database from unauthorized or malicious access. However, if the firewall rules are not configured properly, they can also block the legitimate communication between the web application and the database. For example, if the firewall rules deny the port or protocol that the web application uses to connect to the database, the web application will not be able to receive data from the database. To fix this issue, the cloud engineer should review and update the firewall rules to allow the necessary traffic between the web application and the database. References: CompTIA Cloud+ CV0-003 Certification Study Guide, Chapter 9, Objective 9.2: Given a scenario, troubleshoot common security issues.

NEW QUESTION 225
- (Topic 3)
A product-based company wants to transition to a method that provides the capability to enhance the product seamlessly and keep the development iterations to a shorter time frame. Which of the following would BEST meet these requirements?

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

Answer: C

Explanation:
CI/CD tools are software tools that enable continuous integration and continuous delivery or deployment, which are methods to frequently deliver software products to customers by introducing automation into the stages of software development. CI/CD tools can help a product-based company to transition to a method that provides the capability to enhance the product seamlessly and keep the development iterations to a shorter time frame, as they can offer the following benefits:
? Faster and more reliable delivery of software products, as CI/CD tools can automate the processes of building, testing, and deploying code changes, reducing manual errors and delays.
? Higher quality and performance of software products, as CI/CD tools can facilitate ongoing feedback, monitoring, and improvement of the code, ensuring that it meets the customer expectations and requirements.
? Greater collaboration and communication among the development teams, as CI/CD tools can integrate with various tools and platforms, such as version control systems, code repositories, testing frameworks, and cloud services, enabling a seamless workflow and visibility across the software lifecycle.
Some examples of popular CI/CD tools are Jenkins1, CircleCI2, GitLab CI/CD3, and AWS CodeBuild4.

NEW QUESTION 227
- (Topic 3)
A cloud administrator needs to control the connections between a group of web servers and database servers as part of the financial application security review. Which of the following would be the BEST way to achieve this objective?

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

Answer: D

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

NEW QUESTION 231
- (Topic 3)
A company has two primary offices, one in the United States and one in Europe. The company uses a public IaaS service that has a global data center presence to host its marketing materials. The marketing team, which is primarily based in Europe, has reported latency issues when retrieving these materials. Which of the following is the BEST option to reduce the latency issues?

A. Add an application load balancer to the applications to spread workloads.
B. Integrate a CDN solution to distribute web content globally.
C. Upgrade the bandwidth of the dedicated connection to the IaaS provider.
D. Migrate the applications to a region hosted in Europe.

Answer: B

Explanation:
The best option to reduce the latency issues for the marketing team that is primarily based in Europe when retrieving the marketing materials that are hosted on a public IaaS service is to integrate a CDN (content delivery network) solution to distribute web content globally. A CDN is a network of geographically distributed servers that cache and deliver web content to users based on their proximity and network conditions. A CDN can improve the performance and availability of web content by reducing the distance and hops between the users and the servers, as well as offloading the traffic from the origin server. Reference: [CompTIA Cloud+ Certification Exam Objectives], Domain 3.0 Maintenance, Objective 3.4 Given a scenario, implement automation and orchestration to optimize cloud operations

NEW QUESTION 234
- (Topic 3)
A company wants to move to a multicloud environment and utilize the technology that provides the most portability. Which of the following technology solutions would BEST meet the company's needs?

A. Bootstrap
B. Virtual machines
C. Clusters
D. Containers

Answer: D

Explanation:
The technology that provides the most portability for a multicloud environment is containers. Containers are units of software that package an application and its dependencies into a standardized and isolated environment that can run on any platform or cloud service. Containers are lightweight, scalable, and portable, as they do not depend on the underlying infrastructure or operating system. Containers can also be managed by orchestration tools that automate the deployment, scaling, and networking of containerized applications across multiple clouds. Reference: [CompTIA Cloud+ Certification Exam Objectives], Domain 1.0 Configuration and Deployment, Objective 1.3 Given a scenario involving integration between multiple cloud environments, select an appropriate solution design.

NEW QUESTION 238
.....

Relate Links

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

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

Contact us

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

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