CompTIA

Exam Questions CV0-003

CompTIA Cloud+ Certification Exam

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

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

Answer: B

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

NEW QUESTION 2
- (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 3
- (Topic 1)
A DevOps administrator is automating an existing software development workflow. The administrator wants to ensure that prior to any new code going into production, tests confirm the new code does not negatively impact existing automation activities.
Which of the following testing techniques would be BEST to use?

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

Answer: B

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

NEW QUESTION 4
- (Topic 1)
After analyzing a web server’s logs, a systems administrator sees that users are connecting to the company’s application through HTTP instead of HTTPS. The administrator then configures a redirect from HTTP to HTTPS on the web server, and the application responds with a connection time-out message.
Which of the following should the administrator verify NEXT?

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

Answer: B

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

NEW QUESTION 5
- (Topic 1)
A systems administrator needs to configure an email client to ensure data integrity of the email messages.
Which of the following provides the BEST mechanism to achieve this goal?

A. Cyclic redundancy check
B. SHA-1 hashes
C. SHA-256 hashes
D. Digital signature

Answer: D

Explanation:
A digital signature is a type of cryptographic technique that verifies the authenticity, integrity, and non-repudiation of an electronic message or document. A digital signature can help configure an email client to ensure data integrity of the email messages, as it can prove that the email message has not been altered or tampered with during transmission by using a mathematical algorithm to generate a unique code (signature) based on the content and identity of the sender. A digital signature can also help prevent spoofing, phishing, or impersonation attacks, as it can confirm that the email message originates from a legitimate source. References: CompTIA Cloud+ Certification Exam Objectives, page 14, section 2.7
Reference: https://www.fsl.cs.sunysb.edu/docs/integrity-storagess05/integrity.html

NEW QUESTION 6
- (Topic 1)
A company wants to implement business continuity, and the cloud solution architect needs to design the correct solution.
Which of the following will provide the data to measure business continuity? (Choose two.)

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

Answer: AF

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

NEW QUESTION 7
- (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 8
- (Topic 1)
A systems administrator is configuring RAID for a new server. This server will host files for users and replicate to an identical server. While redundancy is necessary, the most important need is to maximize storage.
Which of the following RAID types should the administrator choose?

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

Answer: C

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

NEW QUESTION 9
- (Topic 1)
A company wants to check its infrastructure and application for security issues regularly. Which of the following should the company implement?

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

Answer: C

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

NEW QUESTION 10
- (Topic 1)
A company has developed a cloud-ready application. Before deployment, an administrator needs to select a deployment technology that provides a high level of portability and is lightweight in terms of footprint and resource requirements.
Which of the following solutions will be BEST to help the administrator achieve the requirements?

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

Answer: A

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

NEW QUESTION 10
- (Topic 1)
A company is switching from one cloud provider to another and needs to complete the migration as quickly as possible.
Which of the following is the MOST important consideration to ensure a seamless migration?

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

Answer: C

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

NEW QUESTION 11
- (Topic 1)
A systems administrator is creating a playbook to run tasks against a server on a set schedule.
Which of the following authentication techniques should the systems administrator use within the playbook?

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

Answer: C

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

NEW QUESTION 14
- (Topic 1)
A systems administrator is troubleshooting performance issues with a Windows VDI environment. Users have reported that VDI performance has been slow since

the images were upgraded from Windows 7 to Windows 10.
This VDI environment is used to run simple tasks, such as Microsoft Office. The administrator investigates the virtual machines and finds the following settings:
? 4 vCPU
? 16GB RAM
? 10Gb networking
? 256MB frame buffer
Which of the following MOST likely needs to be upgraded?

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

Answer: C

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

NEW QUESTION 15
- (Topic 1)
A cloud administrator is designing a multiregion network within an IaaS provider. The business requirements for configuring the network are as follows:
? Use private networking in and between the multisites for data replication.
? Use low latency to avoid performance issues.
Which of the following solutions should the network administrator use within the IaaS provider to connect multiregions?

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

Answer: A

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

NEW QUESTION 16
- (Topic 1)
A company that utilizes an IaaS service provider has contracted with a vendor to perform a penetration test on its environment. The vendor is able to exploit the virtualization layer and obtain access to other instances within the cloud provider's environment that do not belong to the company.
Which of the following BEST describes this attack?

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

Answer: A

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

NEW QUESTION 20
- (Topic 1)
An organization requires the following to be achieved between the finance and marketing departments:
? Allow HTTPS/HTTP.
? Disable FTP and SMB traffic.
Which of the following is the MOST suitable method to meet the requirements?

A. Implement an ADC solution to load balance the VLAN traffic
B. Configure an ACL between the VLANs
C. Implement 802.1X in these VLANs
D. Configure on-demand routing between the VLANs

Answer: B

Explanation:
An access control list (ACL) is a set of rules that defines which traffic is allowed or denied between different network segments or devices. An ACL can be used to filter traffic based on various criteria, such as source and destination addresses, ports, protocols, and applications. Configuring an ACL between the VLANs of the

finance and marketing departments is the most suitable method to meet the requirements of allowing HTTPS/HTTP and disabling FTP and SMB traffic. An ACL can specify which ports and protocols are permitted or blocked between the VLANs, such as allowing port 80 (HTTP) and port 443 (HTTPS), and denying port 21 (FTP) and port 445 (SMB). References: [CompTIA Cloud+ Certification Exam Objectives], page 15, section 2.8

NEW QUESTION 21
- (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 23
- (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 26
- (Topic 1)
A cloud administrator is setting up a DR site on a different zone of the same CSP. The application servers are replicated using the VM replication, and the database replication is set up using log shipping. Upon testing the DR site, the application servers are unable to access the database servers. The administrator has verified the systems are running and are accessible from the CSP portal.
Which of the following should the administrator do to fix this issue?

A. Change the database application IP
B. Create a database cluster between the primary site and the DR site
C. Update the connection string
D. Edit the DNS record at the DR site for the application servers

Answer: C

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

NEW QUESTION 30
- (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 35
- (Topic 2)
A cloud administrator is managing an organization's infrastructure in a public cloud. All servers are currently located in a single virtual network with a single firewall that all traffic must pass through. Per security requirements, production, QA, and development servers should not be able to communicate directly with each other.
Which of the following should an administrator perform to comply with the security requirement?

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

Answer: A

Explanation:
These are the actions that the administrator should perform to comply with the security requirement of isolating production, QA, and development servers from each other in a public cloud environment:
? Create separate virtual networks for production, QA, and development servers: A virtual network is a logical isolation of network resources or systems within a cloud environment. Creating separate virtual networks for different types of servers can help to segregate them from each other and prevent direct communication or interference.
? Move the servers to the appropriate virtual network: Moving the servers to the appropriate virtual network can help to assign them to their respective roles and functions, as well as ensure that they follow the network policies and rules of their virtual network.
? Apply a network security group to each virtual network that denies all traffic except for the firewall: A network security group is a set of rules or policies that control and filter inbound and outbound network traffic for a virtual network or system. Applying a network security group to each virtual network that denies all traffic except for the firewall can help to enforce security and compliance by blocking any unauthorized or unwanted traffic between different types of servers, while allowing only necessary traffic through the firewall.

NEW QUESTION 36
- (Topic 2)
A systems administrator is troubleshooting a performance issue with a virtual database server. The administrator has identified the issue as being disk related and believes the cause is a lack of IOPS on the existing spinning disk storage. Which of the following should the administrator do NEXT to resolve this issue?

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

Answer: B

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

NEW QUESTION 40
- (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 41
- (Topic 2)
A systems administrator is deploying a new cloud application and needs to provision cloud services with minimal effort. The administrator wants to reduce the tasks required for maintenance, such as OS patching, VM and volume provisioning, and autoscaling configurations. Which of the following would be the BEST option to deploy the new application?

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

Answer: D

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

NEW QUESTION 45
- (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 49
- (Topic 2)
A cloud administrator wants to have a central repository for all the logs in the company’s private cloud. Which of the following should be implemented to BEST meet this requirement?

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

Answer: D

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

NEW QUESTION 53
- (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.

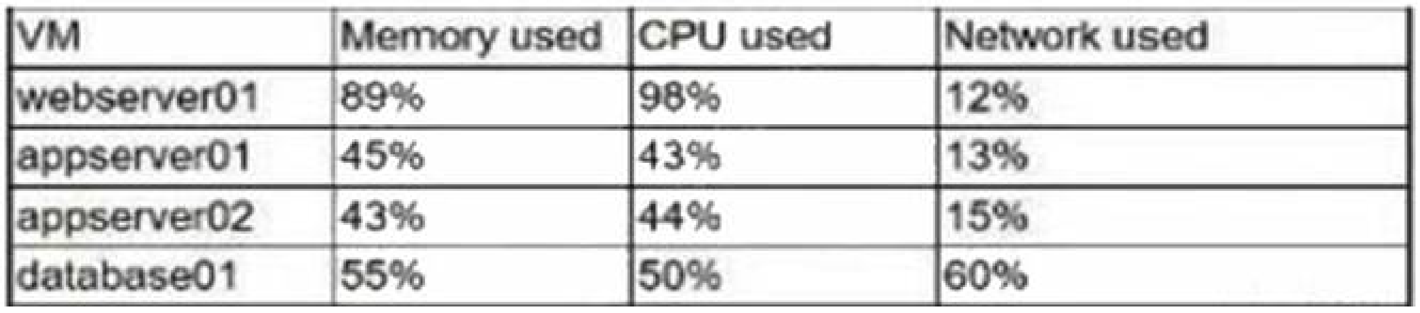
NEW QUESTION 54
- (Topic 2)
Which of the following definitions of serverless computing BEST explains how it is different from using VMs?

A. Serverless computing is a cloud-hosting service that utilizes infrastructure that is fully managed by the CSP.
B. Serverless computing uses predictable billing and offers lower costs than VM compute services.
C. Serverless computing is a scalable, highly available cloud service that uses SDN technologies.
D. Serverless computing allows developers to focus on writing code and organizations to focus on business.

Answer: D

Explanation:
This is the best definition of serverless computing that explains how it is different from using VMs (Virtual Machines). Serverless computing is a cloud service model that provides customers with a platform to run applications or functions without having to manage or provision any underlying infrastructure or resources, such as servers, storage, network, OS, etc. Serverless computing is different from using VMs in the following ways:
? Serverless computing allows developers to focus on writing code and organizations to focus on business, rather than spending time and effort on managing or scaling VMs or other infrastructure components.
? Serverless computing is event-driven and pay-per-use, which means that applications or functions are executed only when triggered by a specific event or request, and customers are charged only for the resources consumed during the execution time.
? Serverless computing is more scalable and flexible than using VMs, as it can automatically adjust the capacity and performance of applications or functions according to demand or workload, without requiring any manual intervention or configuration.

NEW QUESTION 57
- (Topic 2)
After announcing a big sales promotion, an e-commerce company starts to experience a slow response on its platform that is hosted in a public cloud. When checking the resources involved, the systems administrator sees the following consumption:



VM	Memory used	CPU used	Network used
webserver01	89%	98%	12%
appserver01	45%	43%	13%
appserver02	43%	44%	15%
database01	55%	50%	60%

Considering all VMs were built from the same templates, which of the following actions should the administrator perform FIRST to speed up the response of the e-commerce platform?

A. Spin up a new web server
B. Spin up a new application server
C. Add more memory to the web server
D. Spin up a new database server

Answer: D

Explanation:
Spinning up a new web server is what the administrator should perform first to speed up the response of the e-commerce platform that is hosted in a public cloud and starts to experience a slow response after announcing a big sales promotion. A web server is a system or service that hosts and delivers web content, such as web pages, images, videos, etc., to clients over a network or internet connection. A web server can affect the response of an e-commerce platform by determining how fast it can process and serve web requests or responses from clients. Spinning up a new web server can speed up the response of an e-commerce platform by providing benefits such as:
? Scalability: Spinning up a new web server can increase the scalability of the e-commerce platform by adding more capacity or resources to handle the increased demand or load caused by the sales promotion, without affecting the existing web servers.
? Performance: Spinning up a new web server can improve the performance of the e-commerce platform by reducing the latency or overhead of processing and serving web requests or responses from clients, which may cause delays or errors.

NEW QUESTION 61
- (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 66
- (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 70
- (Topic 2)
A cloud administrator has been using a custom VM deployment script. After three months of use, the script no longer joins the LDAP domain. The cloud administrator verifies the account has the correct permissions. Which of the following is the MOST likely cause of the failure?

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

Answer: D

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

NEW QUESTION 73
- (Topic 2)
Users of an enterprise application, which is configured to use SSO, are experiencing slow connection times. Which of the following should be done to troubleshoot the issue?

A. Perform a memory dump of the O
B. Analyze the memory dump.Upgrade the host CPU to a higher clock speed CPU.
C. Perform a packet capture during authenticatio
D. Validate the load-balancing configuration.Analyze the network throughput of the load balancer.
E. Analyze the storage system IOP
F. Increase the storage system capacit
G. Replace the storage system disks to SS
H. Evaluate the OS ACL
I. Upgrade the router firmware.Increase the memory of the router.

Answer: B

Explanation:
These are the steps that should be done to troubleshoot the issue of slow connection times for users of an enterprise application that is configured to use SSO (Single Sign-On). SSO is a feature that allows users to access multiple applications or services with one login credential, without having to authenticate separately for each application or service. SSO can improve user experience and security, but it may also introduce performance issues if not configured properly. To troubleshoot the issue, the administrator should perform a packet capture during authentication to analyze the network traffic and identify any delays or errors in the SSO process. The administrator should also validate the load-balancing configuration to ensure that the SSO requests are distributed evenly and efficiently among the available servers or instances. The administrator should also analyze the network throughput of the load balancer to check if there is any congestion or bottleneck that may affect the SSO performance.

NEW QUESTION 78
- (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 79
- (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 80
- (Topic 2)
A technician just received the lessons learned from some recent data that was lost due to an on-premises file-server crash. The action point is to change the backup strategy to minimize manual intervention. Which of the following is the BEST approach for the technician to implement?

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

Answer: A

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

NEW QUESTION 82
- (Topic 2)
A cloud administrator 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 86
- (Topic 2)
A systems administrator swapped a failed hard drive on a server with a RAID 5 array. During the RAID resynchronization, a second hard drive failed.
Which of the following actions will make the server fully operational?

A. Restart the RAID resynchronization process
B. Perform a P2V migration of the server
C. Swap the failed hard drive with a fresh one
D. Restore the server from backup

Answer: D

Explanation:
RAID 5 is a disk array configuration that uses parity to provide fault tolerance and data recovery. RAID 5 can tolerate the failure of one disk, but not two or more disks. If a second disk fails during the resynchronization process, the data on the RAID 5 array will be lost and unrecoverable. The only way to make the server fully operational is to restore the data from a backup source.

NEW QUESTION 90
- (Topic 2)
A systems administrator has received an email from the virtualized environment's alarms indicating the memory was reaching full utilization. When logging in, the administrator notices that one out of a five-host cluster has a utilization of 500GB out of 512GB of RAM. The baseline utilization has been 300GB for that host.
Which of the following should the administrator check NEXT?

A. Storage array
B. Running applications
C. VM integrity
D. Allocated guest resources

Answer: D

Explanation:
Allocated guest resources is what the administrator should check next after receiving an email from the virtualized environment’s alarms indicating the memory was reaching full utilization and noticing that one out of a five-host cluster has a utilization of 500GB out of 512GB of RAM. Allocated guest resources are the amount of resources or capacity that are assigned or reserved for each guest system or device within a host system or device. Allocated guest resources can affect performance and utilization of host system or device by determining how much resources or capacity are available or used by each guest system or device. Allocated guest resources should be checked next by comparing them with the actual usage or demand of each guest system or device, as well as identifying any overallocation or underallocation of resources that may cause inefficiency or wastage.

NEW QUESTION 91
- (Topic 2)
A technician needs to deploy two virtual machines in preparation for the configuration of a financial application next week. Which of the following cloud deployment models should the technician use?

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

Answer: B

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

NEW QUESTION 96
- (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 97
- (Topic 2)
A cloud administrator is responsible for managing a cloud-based content management solution. According to the security policy, any data that is hosted in the cloud must be protected against data exfiltration. Which of the following solutions should the administrator implement?

A. HIDS

B. FIM
C. DLP
D. WAF

Answer: C

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

NEW QUESTION 102
- (Topic 2)
A systems administrator is performing upgrades to all the hypervisors in the environment. Which of the following components of the hypervisors should be upgraded? (Choose two.)

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

Answer: CF

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

NEW QUESTION 107
- (Topic 2)
A VDI administrator has received reports from the drafting department that rendering is slower than normal. Which of the following should the administrator check FIRST to optimize the performance of the VDI infrastructure?

A. GPU
B. CPU
C. Storage
D. Memory

Answer: A

Explanation:
Checking the GPU (Graphics Processing Unit) is the first thing that the VDI administrator should do to optimize the performance of the VDI infrastructure for rendering tasks. GPU is a specialized hardware device that accelerates graphics processing and rendering. GPU can improve the user experience and performance of VDI applications that require intensive graphics processing, such as drafting, gaming, video editing, etc.

NEW QUESTION 108
- (Topic 2)
A DevOps administrator is designing a new machine-learning platform. The application needs to be portable between public and private clouds and should be kept as small as possible. Which of the following approaches would BEST meet these requirements?

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

Answer: D

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

NEW QUESTION 112
- (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 114
- (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 119
- (Topic 2)
A systems administrator is trying to establish an RDP session from a desktop to a server in the cloud. However, the connection appears to be refused even through the VM is responding to ICMP echo requests. Which of the following should the administrator check FIRST?

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

Answer: A

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

NEW QUESTION 121
- (Topic 2)
A systems administrator wants to verify the word "qwerty" has not been used as a password on any of the administrative web consoles in a network. Which of the following will achieve this goal?

A. A service availability scan
B. An agent-based vulnerability scan
C. A default and common credentialed scan
D. A network port scan

Answer: C

Explanation:
A default and common credentialed scan is what the administrator should use to verify the word “qwerty” has not been used as a password on any of the administrative web consoles in a network. A credentialed scan is a type of vulnerability scan that uses valid credentials or accounts to access and scan target systems or devices. A credentialed scan can provide more accurate and detailed results than a non- credentialed scan, as it can perform more actions and tests on target systems or devices. A default and common credentialed scan is a type of credentialed scan that uses default or common credentials or accounts, such as admin/admin, root/root, etc., to access and scan target systems or devices. A default and common credentialed scan can help to identify weak or insecure passwords on administrative web consoles, such as “qwerty”, and recommend stronger passwords.

NEW QUESTION 123
- (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 124
- (Topic 2)
A resource pool in a cloud tenant has 90 GB of memory and 120 cores. The cloud administrator needs to maintain a 30% buffer for resources for optimal performance of the hypervisor. Which of the following would all ow for the maximum number of two-core machines with equal memory?

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

Answer: C

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

NEW QUESTION 129
- (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 134
- (Topic 2)
A company wants to move its environment from on premises to the cloud without vendor lock-in. Which of the following would BEST meet this requirement?

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

Answer: C

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

NEW QUESTION 138
- (Topic 2)
A software development manager is looking for a solution that will allow a team of developers to work in isolated environments that can be spun up and torn down quickly.
Which of the following is the MOST appropriate solution?

A. Containers
B. File subscriptions
C. Ballooning

D. Software-defined storage

Answer: A

Explanation:
Containers are isolated environments that can run applications and their dependencies without interfering with other processes or systems. Containers are lightweight, portable, and scalable, which makes them ideal for development and testing purposes. Containers can be spun up and torn down quickly using tools such as Docker, Kubernetes, etc.

NEW QUESTION 143
- (Topic 2)
A Chief Information Security Officer (CISO) is evaluating the company's security management program. The CISO needs to locate all the assets with identified deviations and mitigation measures. Which of the following would help the CISO with these requirements?

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

Answer: D

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

NEW QUESTION 148
- (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 153
- (Topic 2)
A system administrator supports an application in the cloud, which includes a restful API that receives an encrypted message that is passed to a calculator system. The administrator needs to ensure the proper function of the API using a new automation tool. Which of the following techniques would be BEST for the administrator to use to accomplish this requirement?

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

Answer: C

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

NEW QUESTION 157
- (Topic 2)
A systems administrator is deploying a VM and would like to minimize storage utilization by ensuring the VM uses only the storage if needs. Which of the following will BEST achieve this goal?

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

Answer: D

Explanation:
Reference: https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.vm_admin.doc/GUID-4C0F4D73-82F2-4B81-8AA7- 1DD752A8A5AC.html
Thin provisioning is the technique that will minimize storage utilization by ensuring the VM uses only the storage it needs. Thin provisioning is a storage allocation

method that assigns disk space to a VM on demand, rather than in advance. Thin provisioning can improve storage utilization and efficiency by avoiding overprovisioning and wasting disk space. Thin provisioning can also allow for more flexibility and scalability of storage resources.

NEW QUESTION 161
- (Topic 2)
A company had a system compromise, and the engineering team resolved the issue after 12 hours. Which of the following information will MOST likely be requested by the Chief Information Officer (CIO) to understand the issue and its resolution?

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

Answer: A

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

NEW QUESTION 166
- (Topic 2)
A company needs to migrate the storage system and batch jobs from the local storage system to a public cloud provider. Which of the following accounts will MOST likely be created to run the batch processes?

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

Answer: D

Explanation:
A service account is what will most likely be created to run the batch processes that migrate the storage system and batch jobs from the local storage system to a public cloud provider. A service account is a special type of account that is used to perform automated tasks or operations on a system or service, such as running scripts, applications, or processes. A service account can provide benefits such as:
? Security: A service account can have limited or specific permissions and roles that are required to perform the tasks or operations, which can prevent unauthorized or malicious access or actions.
? Efficiency: A service account can run the tasks or operations without any human intervention or interaction, which can save time and effort.
? Reliability: A service account can run the tasks or operations consistently and accurately, which can reduce errors or failures.

NEW QUESTION 171
- (Topic 2)
An administrator recently provisioned a file server in the cloud. Based on financial considerations, the administrator has a limited amount of disk space. Which of the following will help control the amount of space that is being used?

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

Answer: C

Explanation:
User quotas are what will help control the amount of space that is being used by a file server in the cloud that has a limited amount of disk space due to financial considerations. User quotas are the limits or restrictions that are imposed on the amount of space that each user can use or consume on a file server or storage device. User quotas can help to control the amount of space that is being used by:
? Preventing or reducing wastage or overuse of space by users who may store unnecessary or redundant files or data on the file server or storage device.
? Ensuring fair and equal distribution or allocation of space among users who may have different needs or demands for space on the file server or storage device.
? Monitoring and managing the usage or consumption of space by users who may need to be notified or alerted when they reach or exceed their quota on the file server or storage device.

NEW QUESTION 175
- (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 178
- (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 181
- (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.

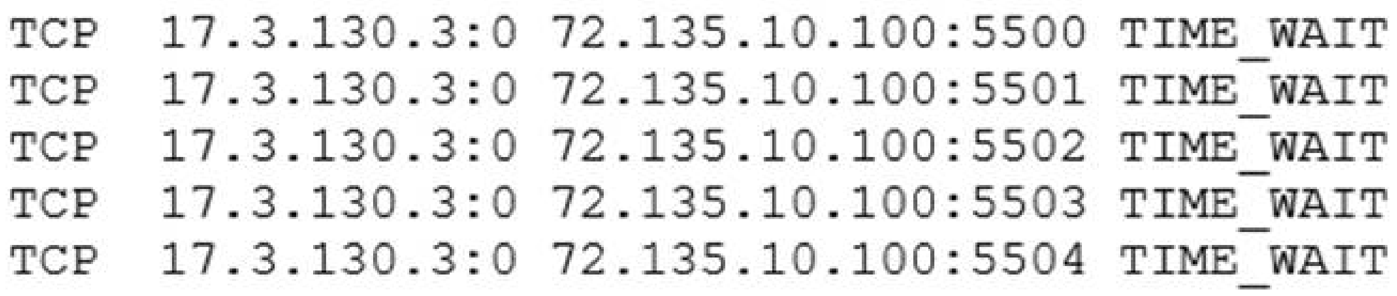
NEW QUESTION 182
- (Topic 2)
Which of the following actions should a systems administrator perform during the containment phase of a security incident in the cloud?

A. Deploy a new instance using a known-good base image.
B. Configure a firewall rule to block the traffic on the affected instance.
C. Perform a forensic analysis of the affected instance.
D. Conduct a tabletop exercise involving developers and systems administrators.

Answer: B

Explanation:
Configuring a firewall rule to block the traffic on the affected instance is what the administrator should perform during the containment phase of a security incident in the cloud. A security incident is an event or situation that affects or may affect the confidentiality, integrity, or availability of cloud resources or data. A security incident response is a process of managing and resolving a security incident using various phases, such as identification, containment, eradication, recovery, etc. The containment phase is where the administrator tries to isolate and prevent the spread or escalation of the security incident. Configuring a firewall rule to block the traffic on the affected instance can help to contain a security incident by cutting off any communication or interaction between the instance and other systems or networks, which may stop any malicious or unauthorized activity or access.

NEW QUESTION 185
- (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

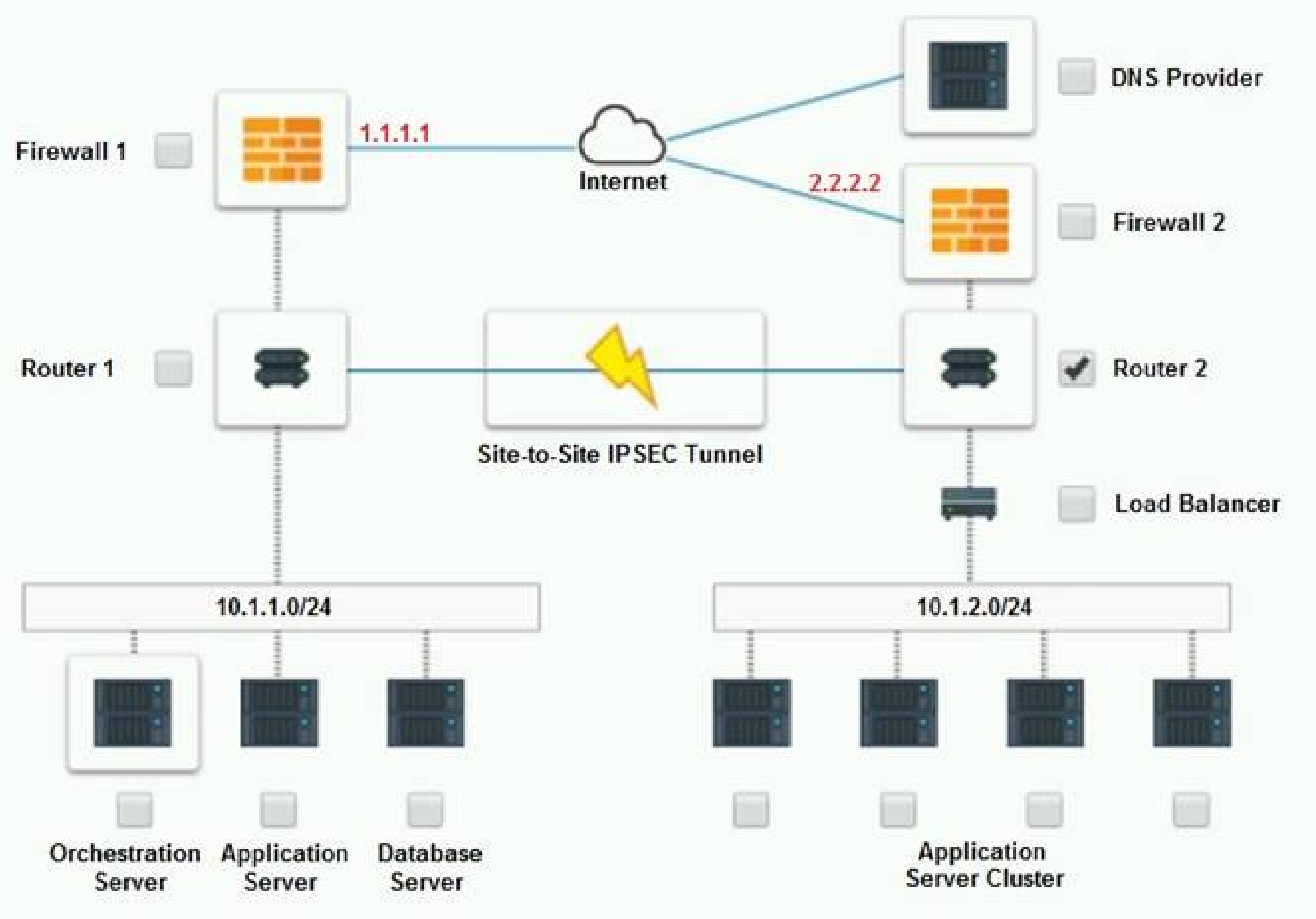
NEW QUESTION 189
- (Topic 1)
A systems administrator needs to configure SSO authentication in a hybrid cloud environment.
Which of the following is the BEST technique to use?

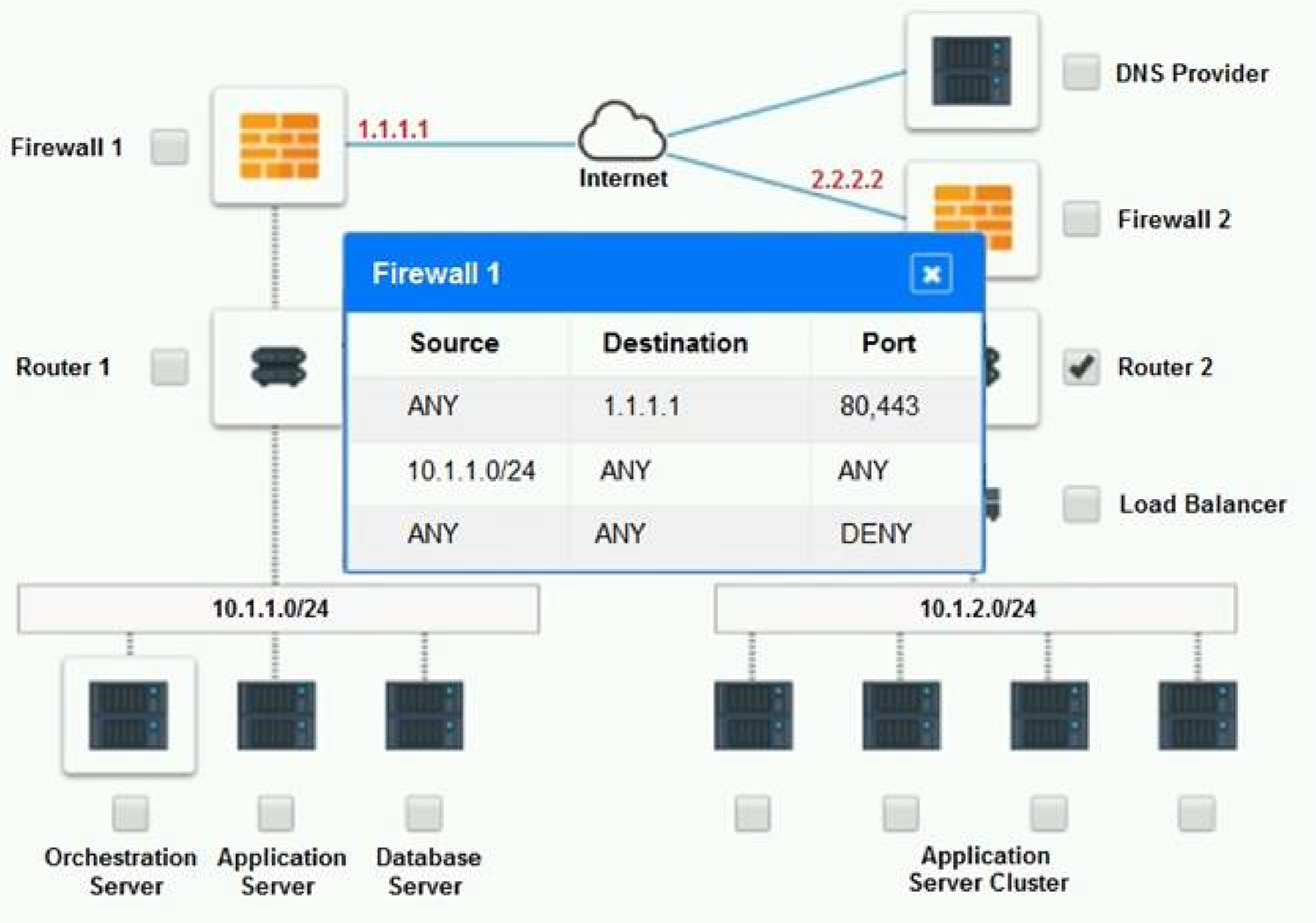
A. Access controls
B. Federation
C. Multifactor authentication
D. Certificate authentication

Answer: B

Explanation:
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. Federation can help configure SSO authentication in a hybrid cloud environment, as it can enable seamless and secure access to cloud-based and on- premises resources using the same identity provider and authentication method. 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

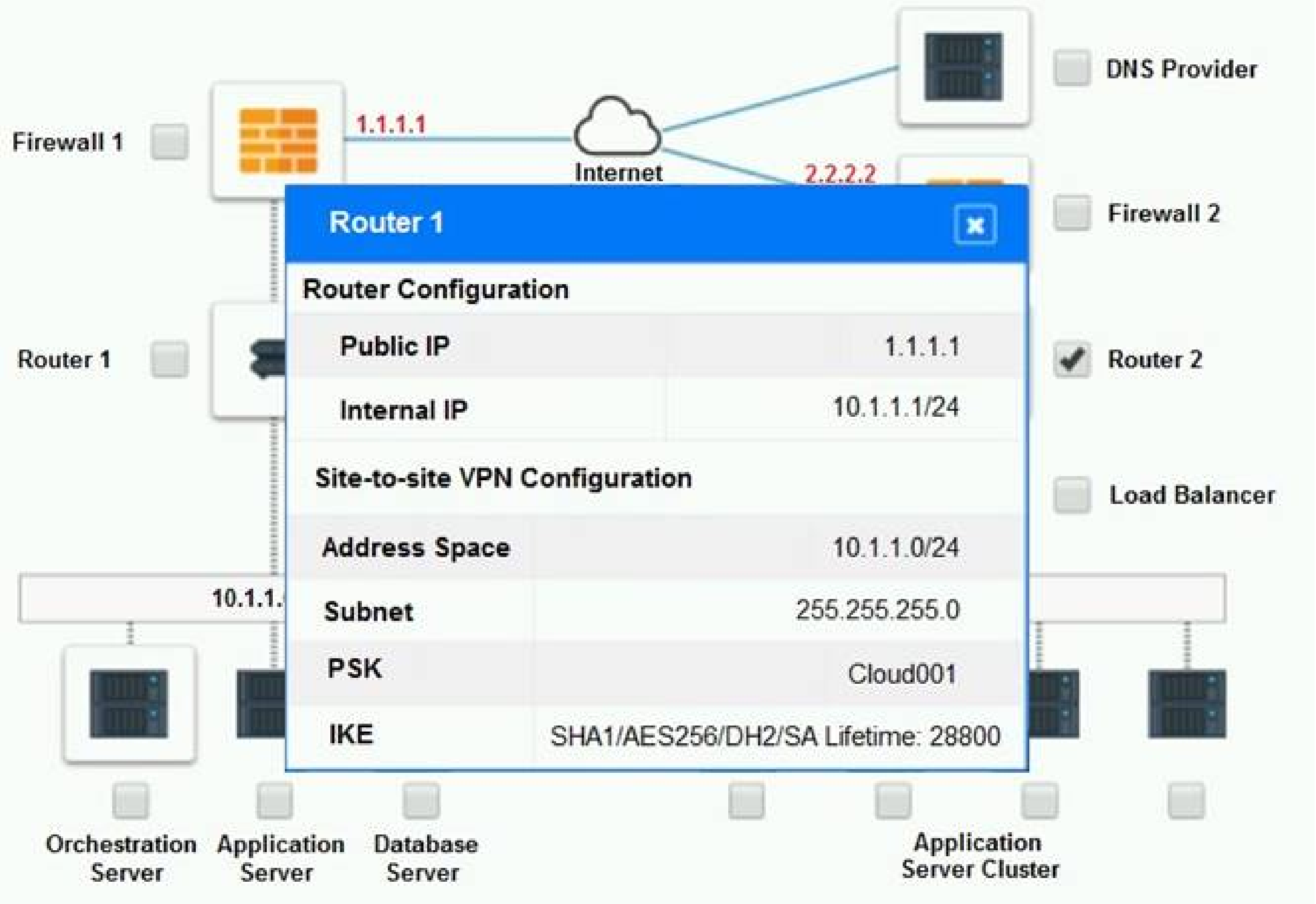
NEW QUESTION 191
SIMULATION - (Topic 1)
A company has decided to scale its e-commerce application from its corporate datacenter to a commercial cloud provider to meet an anticipated increase in demand during an upcoming holiday.
The majority of the application load takes place on the application server 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 ☒

Source	Destination	Port
ANY	1.1.1.1	80,443
10.1.1.0/24	ANY	ANY
ANY	ANY	DENY



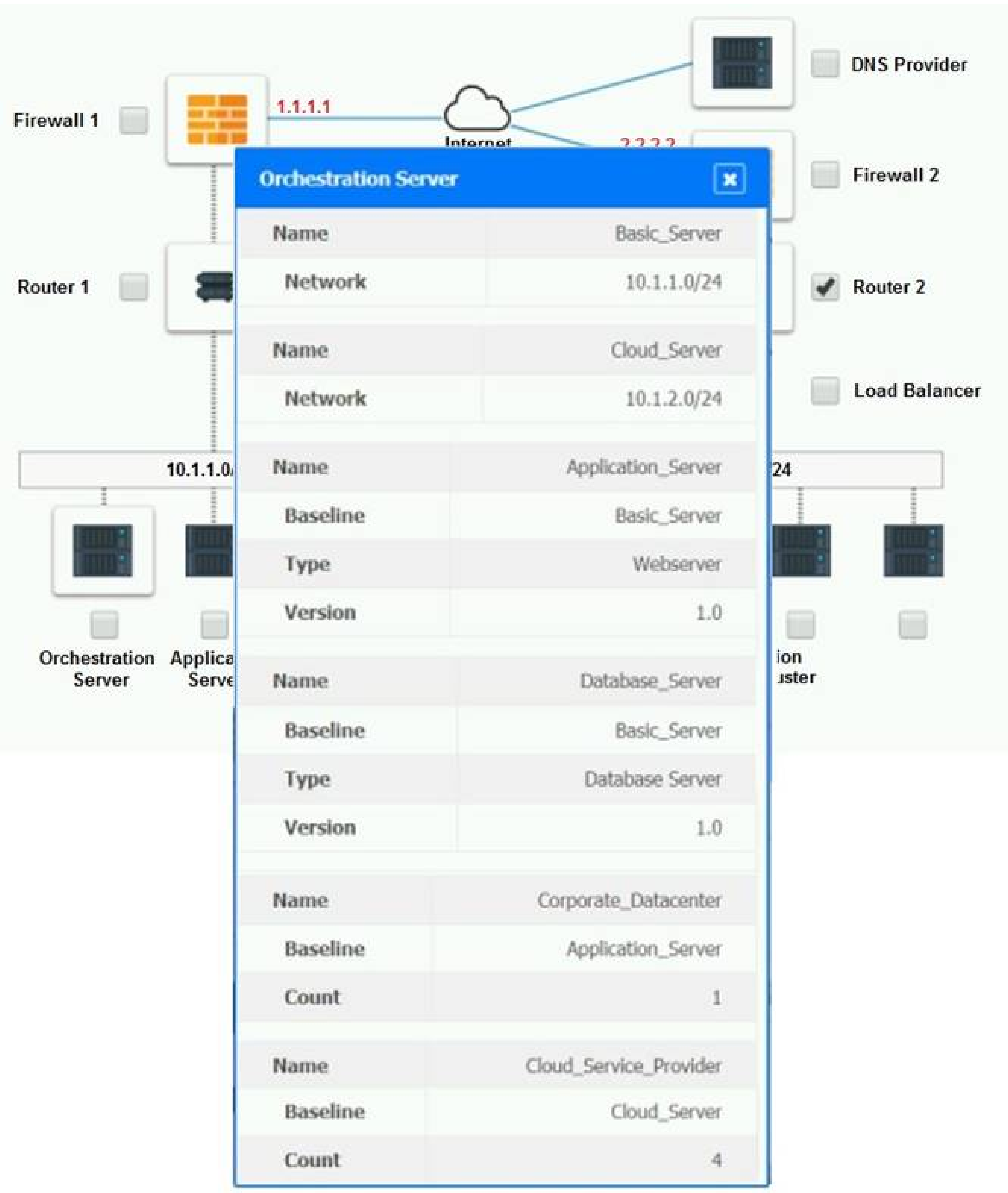
Router 1

Router Configuration

Public IP	1.1.1.1
Internal IP	10.1.1.1/24

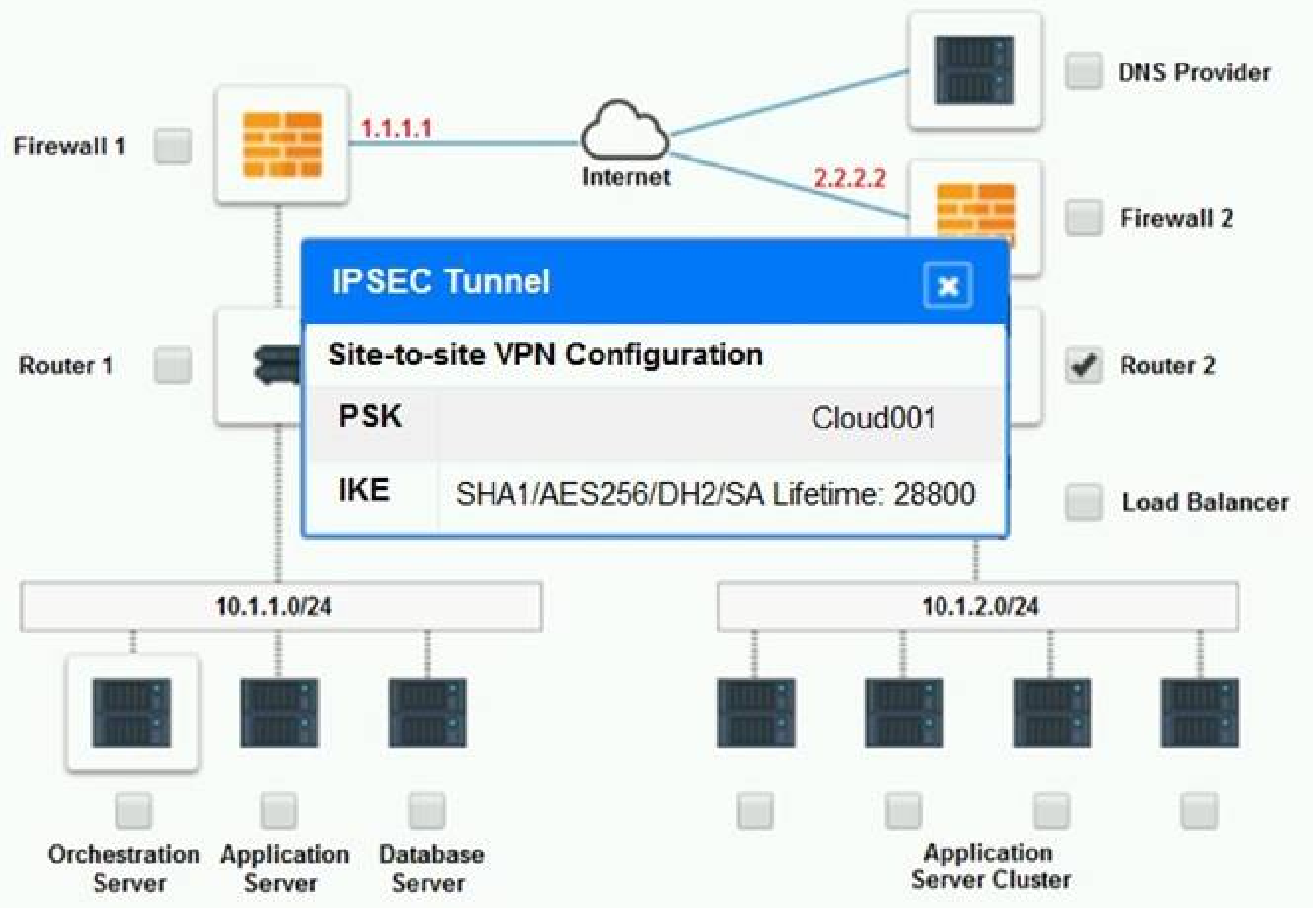
Site-to-site VPN Configuration

Address Space	10.1.1.0/24
Subnet	255.255.255.0
PSK	Cloud001
IKE	SHA1/AES256/DH2/SA Lifetime: 28800



Orchestration Server

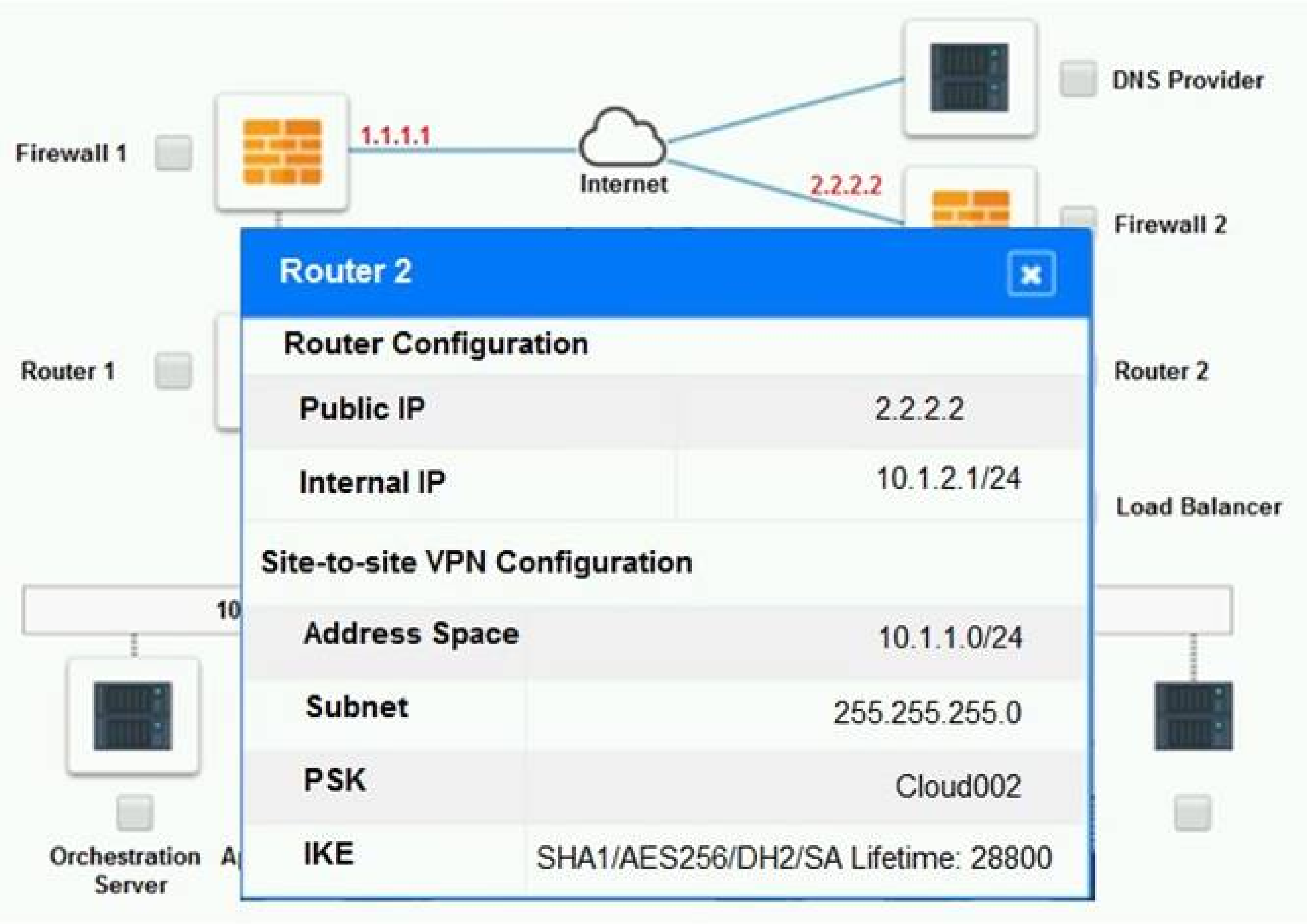
Name	Basic_Server
Network	10.1.1.0/24
Name	Cloud_Server
Network	10.1.2.0/24
Name	Application_Server
Baseline	Basic_Server
Type	Webserver
Version	1.0
Name	Database_Server
Baseline	Basic_Server
Type	Database Server
Version	1.0
Name	Corporate_Datacenter
Baseline	Application_Server
Count	1
Name	Cloud_Service_Provider
Baseline	Cloud_Server
Count	4



IPSEC Tunnel ☒

Site-to-site VPN Configuration

PSK	Cloud001
IKE	SHA1/AES256/DH2/SA Lifetime: 28800



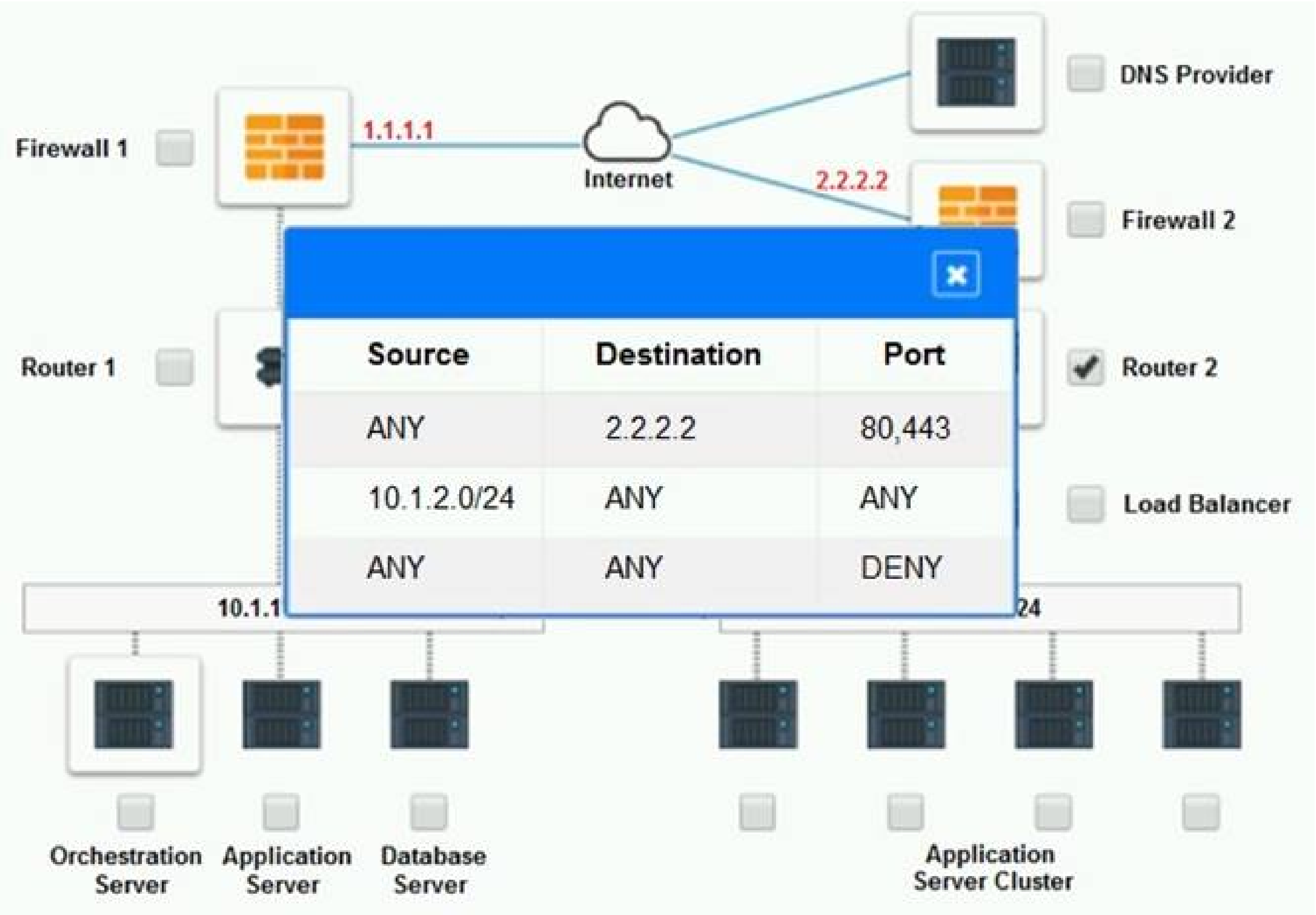
Router 2 ☒

Router Configuration

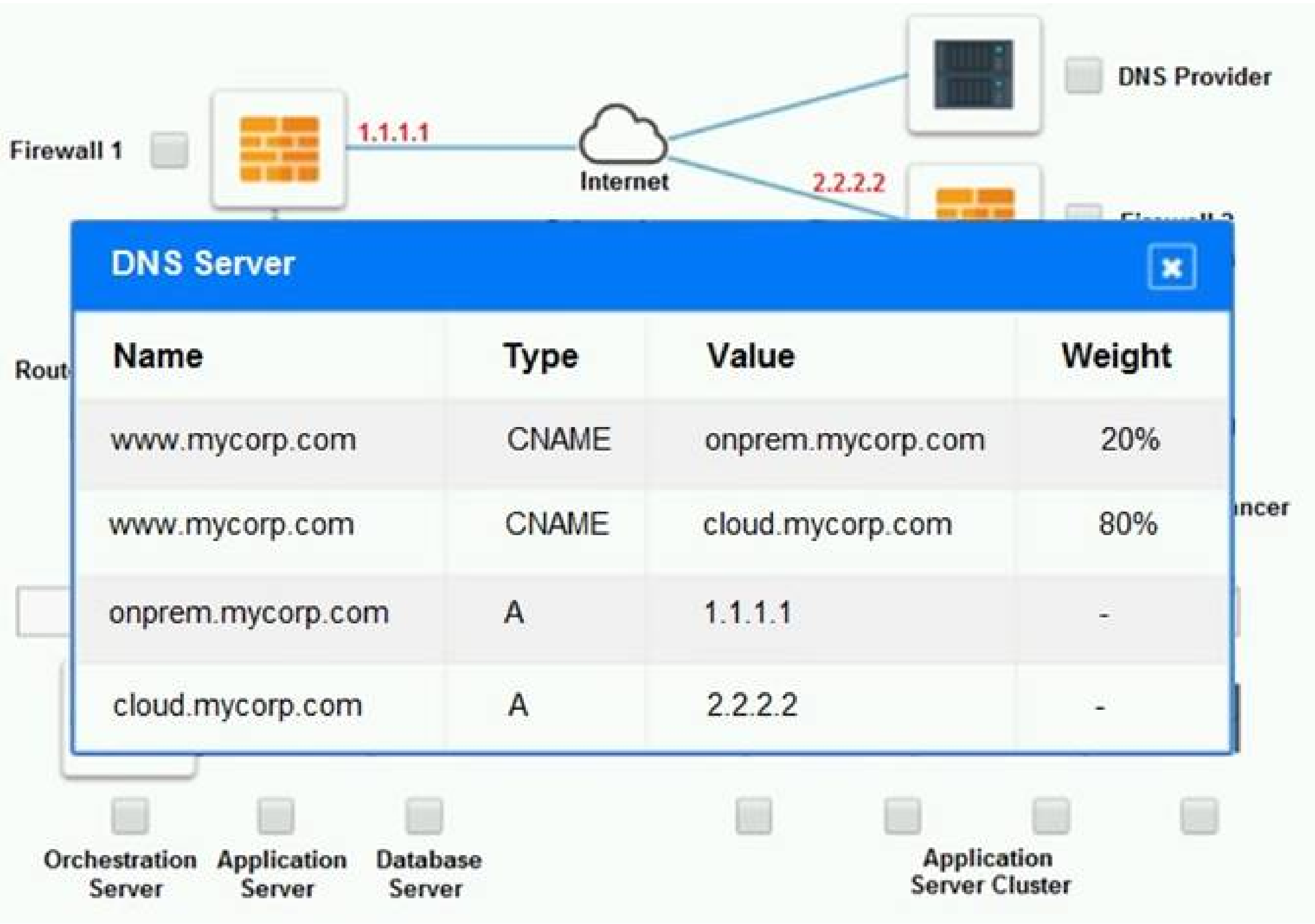
Public IP	2.2.2.2
Internal IP	10.1.2.1/24

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



Source	Destination	Port
ANY	2.2.2.2	80,443
10.1.2.0/24	ANY	ANY
ANY	ANY	DENY



DNS Server

Name	Type	Value	Weight
www.mycorp.com	CNAME	onprem.mycorp.com	20%
www.mycorp.com	CNAME	cloud.mycorp.com	80%
onprem.mycorp.com	A	1.1.1.1	-
cloud.mycorp.com	A	2.2.2.2	-

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.

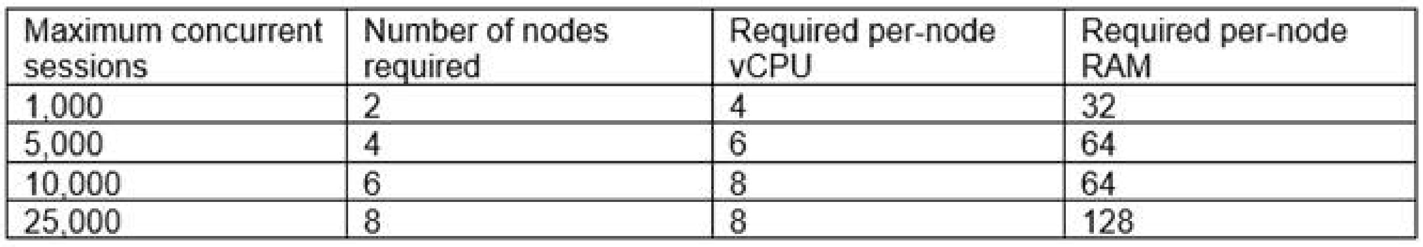
□ Add the Application Server at on-premises to the Load Balancer.

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 192
- (Topic 1)
A company is utilizing a private cloud solution that is hosted within its datacenter. The company wants to launch a new business application, which requires the resources below:



Maximum concurrent sessions	Number of nodes required	Required per-node vCPU	Required per-node RAM
1,000	2	4	32
5,000	4	6	64
10,000	6	8	64
25,000	8	8	128

The current private cloud has 30 vCPUs and 512GB RAM available. The company is looking for a quick solution to launch this application, with expected maximum sessions to be close to 24,000 at launch and an average of approximately 5,000 sessions.
Which of the following solutions would help the company accommodate the new workload in the SHORTEST amount of time and with the maximum financial benefits?

A. Configure auto-scaling within the private cloud
B. Set up cloud bursting for the additional resources
C. Migrate all workloads to a public cloud provider
D. Add more capacity to the private cloud

Answer: B

Explanation:
Cloud Bursting can be used for both compute and storage. This question is about compute capability. "Compute Bursting" unleashes the high-performance compute capabilities of the cloud for processing locally created datasets. (reference: https://www.ctera.com/it-initiatives/cloud-bursting/)
https://azure.microsoft.com/en-us/overview/what-is-cloud-bursting/

NEW QUESTION 196
- (Topic 1)
A cloud engineer is responsible for managing two cloud environments from different MSPs. The security department would like to inspect all traffic from the two cloud environments.
Which of the following network topology solutions should the cloud engineer implement to reduce long-term maintenance?

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

Answer: D

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

NEW QUESTION 198
- (Topic 1)
A systems administrator is troubleshooting network throughput issues following a deployment. The network is currently being overwhelmed by the amount of traffic between the database and the web servers in the environment.
Which of the following should the administrator do to resolve this issue?

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

Answer: C

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

NEW QUESTION 201
- (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 205
- (Topic 1)
A systems administrator is building a new virtualization cluster. The cluster consists of five virtual hosts, which each have flash and spinning disks. This storage is shared among all the virtual hosts, where a virtual machine running on one host may store data on another host.
This is an example of:

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

Answer: C

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

NEW QUESTION 209
- (Topic 1)
A systems administrator wants to have near-real-time information on the volume of data being exchanged between an application server and its clients on the Internet.
Which of the following should the systems administrator implement to achieve this objective?

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

Answer: D

Explanation:
Network flows are records of network traffic that capture information such as source and destination IP addresses, ports, protocols, timestamps, and byte and packet counts. Network flows can provide near-real-time information on the volume of data being exchanged between a system and its clients on the Internet, as they can measure and monitor the amount and rate of network traffic for each connection or session. Network flows can also help analyze network performance, troubleshoot network issues, and detect network anomalies or security incidents. A systems administrator should implement network flows to achieve the objective of having near-real-time information on the volume
of data being exchanged between an application server and its clients on the Internet. References: CompTIA Cloud+ Certification Exam Objectives, page 16, section 3.2

NEW QUESTION 213
- (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 218
- (Topic 1)
A cloud administrator recently noticed that a number of files stored at a SaaS provider's file-sharing service were deleted. As part of the root cause analysis, the administrator noticed the parent folder permissions were modified last week. The administrator then used a test user account and determined the permissions on the files allowed everyone to have write access.
Which of the following is the best step for the administrator to take NEXT?

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

Answer: D

Explanation:
Permissions are rules or settings that determine what actions users can perform on files or resources in a system or service. Permissions can help control and restrict access to files or resources based on various criteria, such as user identity, role, group, or ownership. Defining and configuring the proper permissions for the file-sharing service is the best step for the administrator to take next after discovering that sales group members can access the financial application due to being part of the finance group and having write access to all files in the file-sharing service. Defining and configuring the proper permissions can prevent unauthorized or accidental access or modification of files or resources by limiting or granting access based on specific criteria.
References: CompTIA Cloud+ Certification Exam Objectives, page 14, section 2.7

NEW QUESTION 222
- (Topic 1)
A systems administrator in a large enterprise needs to alter the configuration of one of the finance department's database servers.
Which of the following should the administrator perform FIRST?

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

Answer: B

Explanation:
The SA would do the other three regardless of the need to alter configurations. In this situation, the SA would have to present the change to the CCB in order to do the alteration.
There is no clarification on whether the change management process has been gone
through. Any changes, regardless of how small or big, must go through the change management process. This allows proposals to be heard by end-users, management, and possibly stockholders. From there, it will be reviewed and either approved or denied, with reasons specified. From there, the administrator(s) can do whatever processes are necessary.
Change management is a process or procedure that defines the steps, roles, and responsibilities for implementing, documenting, and communicating any changes or updates to a system or service. Change management can help ensure that any changes or updates are done in a controlled and consistent manner, minimizing any risks or impacts to the system or service. Performing change management is the first thing that a systems administrator should do before altering the configuration of one of the finance department's database servers, as it can ensure that the change request is approved, authorized, tested, and verified before applying it to the database server. References: CompTIA Cloud+ Certification Exam Objectives, page 13, section 2.5

NEW QUESTION 226
- (Topic 1)
An OS administrator is reporting slow storage throughput on a few VMs in a private IaaS cloud. Performance graphs on the host show no increase in CPU or memory. However, performance graphs on the storage show a decrease of throughput in both IOPS and MBps but not much increase in latency. There is no increase in workload, and latency is stable on the NFS storage arrays that are used by those VMs.
Which of the following should be verified NEXT?

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

Answer: D

Explanation:
The network is the set of devices, connections, protocols, and configurations that enable communication and data transfer between different systems and

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

NEW QUESTION 230

- (Topic 1)

A systems administrator is using VMs to deploy a new solution that contains a number of application VMs.
Which of the following would provide high availability to the application environment in case of hypervisor failure?

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

Answer: A

Explanation:

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

NEW QUESTION 235

- (Topic 1)

Lateral-moving malware has infected the server infrastructure.
Which of the following network changes would MOST effectively prevent lateral movement in the future?

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

Answer: C

Explanation:

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

NEW QUESTION 237

- (Topic 1)

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

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

Answer: D

Explanation:

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

NEW QUESTION 241

- (Topic 1)

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

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

Answer: BD

Explanation:

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

NEW QUESTION 245
- (Topic 1)
An organization is required to set a custom registry key on the guest operating system. Which of the following should the organization implement to facilitate this requirement?

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

Answer: A

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

NEW QUESTION 249
- (Topic 1)
A cloud administrator is planning to migrate a globally accessed application to the cloud.
Which of the following should the cloud administrator implement to BEST reduce latency for all users?

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

Answer: A

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

NEW QUESTION 250
- (Topic 4)
A security analyst is investigating a recurring alert. The alert is reporting an insecure firewall configuration state after every cloud application deployment. The process of identifying the issue, requesting a fix, and waiting for the developers to manually patch the environment is being repeated multiple times. In an effort to identify the root issue, the following logs were collected:
Deploying template app prod. •yaml Instance DB successfully created DB keys successfully stored on vault
Instance WebApp successfully created Access rules successfully applied Access—keys successfully created
Which of the following options will provide a permanent fix for the issue?

A. Validate the Iac code used during the deployment.
B. Avoid the use of a vault to store database passwords.
C. Rotate the access keys that were created during deployment.
D. Recommend that the developers do not create multiple resources at once.

Answer: A

Explanation:
The issue of an insecure firewall configuration state after every cloud application deployment is likely caused by a flaw in the IaC code used during the deployment. IaC stands for Infrastructure as Code, which is a method of managing and provisioning IT infrastructure using code, rather than manual configuration1. IaC allows teams to automate the setup and management of their infrastructure, making it more efficient and consistent. However, if the IaC code contains errors, vulnerabilities, or misconfigurations, it can result in security issues or compliance violations in the deployed infrastructure2. Therefore, to provide a permanent fix for the issue, the IaC code used during the deployment should be validated and tested to ensure that it meets the security requirements and best practices for firewall configuration. The IaC code can be validated using tools such as Azure Resource Manager Template Toolkit, AWS CloudFormation Linter, or Terraform Validate. These tools can check the syntax and semantics of the IaC code, and identify any potential errors or inconsistencies before deployment

NEW QUESTION 254
- (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 259
- (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 260
- (Topic 4)
A web consultancy group currently works in an isolated development environment. The group uses this environment for the creation of the final solution, but also for showcasing it to customers, before commissioning the sites in production. Recently, customers of newly commissioned sites have reported they are not receiving the final product shown by the group, and the website is performing in unexpected ways. Which of the following additional environments should the group adopt and include in its process?

A. Provide each web consultant a local environment on their device.
B. Require each customer to have a blue-green environment.
C. Leverage a staging environment that is tightly controlled for showcasing.
D. Initiate a disaster recovery environment to fail to in the event of reported issues.

Answer: C

Explanation:
A staging environment is a type of development environment that is used to test and demonstrate the final product before deploying it to the production environment. A staging environment can help the web consultancy group avoid the issues of delivering a different or faulty product to the customers, as it can ensure that the product is fully functional, compatible, and secure. A staging environment can also help the group showcase the product to the customers in a realistic and controlled way, as it can mimic the production environment and avoid any interference from other development activities. A staging environment can be leveraged by using cloud services that allow for easy provisioning, scaling, and deployment of web applications

NEW QUESTION 264
- (Topic 4)
A company's marketing department is running a rendering application on virtual desktops. Currently, the application runs slowly, and it takes a long time to refresh the screen. The virtualization administrator is tasked with resolving this issue. Which of the following is the BEST solution?

A. GPU passthrough
B. Increased memory
C. Converged infrastructure
D. An additional CPU core

Answer: A

Explanation:
GPU passthrough is a technique that allows a virtual machine to access and use the physical GPU of the host machine directly. This can improve the performance and quality of graphics-intensive applications, such as rendering, gaming, or video editing, that run on the virtual machine123.
GPU passthrough can help resolve the issue of the rendering application running slowly and taking a long time to refresh the screen on the virtual desktops. By enabling GPU passthrough, the virtualization administrator can allow the rendering application to leverage the full power and features of the host GPU, rather than relying on the limited and shared resources of a virtual GPU. This can result in faster rendering, smoother animations, and higher resolution12

NEW QUESTION 266
- (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 269
- (Topic 4)
A systems administrator is reviewing the logs from a company's IDS and notices a large amount of outgoing traffic from a particular server. The administrator then runs a scan on the server, which detects malware that cannot be removed. Which of the following should the administrator do first?

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

Answer: B

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

NEW QUESTION 274
- (Topic 4)
A systems administrator is attempting to gather information about services and resource utilization on VMS in a cloud environment. Which of the following will BEST accomplish this objective?

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

Answer: E

Explanation:
Performance monitoring is the process of collecting and analyzing metrics related to the performance and availability of resources in a cloud environment1. Performance monitoring can help a systems administrator to gather information about services and resource utilization on VMs in a cloud environment by providing the following benefits2:
? Identify and troubleshoot performance issues and bottlenecks before they affect the end users or business operations.
? Optimize the resource allocation and configuration to meet the performance requirements and SLAs of the services.
? Plan for future capacity and scalability needs based on the historical trends and patterns of resource utilization.
? Compare the performance and costs of different cloud service providers, regions, and SKUs.
Some of the tools and services that can help with performance monitoring in a cloud environment are3:
? Azure Monitor: A comprehensive service that provides a unified view of the health,
performance, and availability of your Azure resources, applications, and services. Azure Monitor collects metrics, logs, and traces from various sources and provides analysis, visualization, alerting, and automation capabilities.
? Azure Advisor: A personalized service that provides recommendations to optimize your Azure resources for performance, security, cost, reliability, and operational excellence. Azure Advisor analyzes your resource configuration and usage data and suggests best practices to improve your cloud environment.
? Azure Application Insights: A service that monitors the performance and usage of your web applications and services. Application Insights collects telemetry data such as requests, dependencies, exceptions, page views, custom events, and metrics from your application code and provides powerful analytics, diagnostics, and alerting features.
? Azure Log Analytics: A service that collects and analyzes data from various sources such as Azure Monitor, Azure services, VMs, containers, applications, and other cloud or on-premises systems. Log Analytics enables you to query, visualize, and correlate log data using the Kusto Query Language (KQL) and create custom dashboards and reports.
Syslog is a standard protocol for sending log messages from network devices to a central server. Syslog can help with logging and auditing activities in a cloud environment, but it does not provide performance monitoring capabilities. Therefore, option A is incorrect. SNMP (Simple Network Management Protocol) is a protocol for collecting and organizing information about managed devices on a network. SNMP can help with network management and monitoring in a cloud environment, but it does not provide comprehensive performance monitoring for VMs and services. Therefore, option B is incorrect.
CMDB (Configuration Management Database) is a database that stores information about the configuration items (CIs) in an IT environment. CMDB can help with configuration management and change management in a cloud environment, but it does not provide performance monitoring capabilities. Therefore, option C is incorrect.
Service management is a set of processes and practices that aim to deliver value to customers by providing quality services that meet their needs and expectations. Service management can help with service design, delivery, support, and improvement in a cloud environment, but it does not provide performance monitoring capabilities. Therefore, option D is incorrect.

NEW QUESTION 279
- (Topic 4)
A company is using laaS services from two different providers: one for its primary site, and the other for a secondary site. The primary site is completely

inaccessible, and the management team has decided to run through the BCP procedures. Which of the following will provide the complete asset information?

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

Answer: B

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

NEW QUESTION 284
......