# Exam Questions CV0-003

CompTIA Cloud+ Certification Exam

**https://www.2passeasy.com/dumps/CV0-003/**

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

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

**Answer:** D

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

**NEW QUESTION 2**
- (Topic 1)
An organization is running a database application on a SATA disk, and a customer is experiencing slow performance most of the time.
Which of the following should be implemented to improve application performance?

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

**Answer:** D

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

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

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

**Answer:** D

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

**NEW QUESTION 4**
- (Topic 1)
Which of the following strategies will mitigate the risk of a zero-day vulnerability MOST efficiently?

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

**Answer:** D

**Explanation:**
An incident response plan is a document or procedure that defines the roles, responsibilities, and actions to be taken in the event of a security incident or breach. Having a detailed incident response plan can help mitigate the risk of a zero-day vulnerability most efficiently, as it can provide a clear and consistent framework for identifying, containing, analyzing, and resolving any potential threats or exploits related to the unknown or unpatched vulnerability. Having a detailed incident

response plan can also help minimize the impact and damage of a security incident or breach, as it can enable timely and effective recovery and restoration processes. References: CompTIA Cloud+ Certification Exam Objectives, page 14, section 2.7

**NEW QUESTION 5**
- (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 6**
- (Topic 1)
Due to a policy change, a few of a customer’s application VMs have been migrated to synchronously replicated storage. The customer now reports that performance is lower. The systems administrator checks the resource usage and discovers CPU utilization is at 60% and available memory is at 30%.
Which of the following is the MOST likely cause?

A. There is not enough vCPU assigned
B. The application is not compatible with the new settings
C. The new configuration is adding latency
D. The memory of the VM is underallocated

**Answer:** C

**Explanation:**
Latency is the delay or time taken for data to travel from one point to another in a network or system. Latency can affect the performance of applications and processes that depend on fast and reliable data transfer. Synchronous replication is a method of data replication that ensures that data is written to two or more storage devices at the same time, providing high availability and consistency. However, synchronous replication can also introduce latency, as the write operation has to wait for the confirmation from all the replicated devices before completing. The new configuration of migrating some application VMs to synchronously replicated storage is most likely adding latency, which can lower the performance of the applications. References: [CompTIA Cloud+ Certification Exam Objectives], page 10, section 1.5

**NEW QUESTION 7**
- (Topic 1)
An administrator is performing an in-place upgrade on a quest VM operating system.
Which of the following can be performed as a quick method to roll back to an earlier state, if necessary?

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

**Answer:** D

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

**NEW QUESTION 8**
- (Topic 1)
An SQL injection vulnerability was reported on a web application, and the cloud platform
team needs to mitigate the vulnerability while it is corrected by the development team. Which of the following controls will BEST mitigate the risk of exploitation?

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

**Answer:** D

**Explanation:**
A web application firewall (WAF) is a type of network security device or software that monitors and filters HTTP traffic between a web application and the Internet. A WAF can help mitigate the risk of exploitation of an SQL injection vulnerability reported on a web application while it is corrected by the development team, as it

can detect and block any malicious requests or queries that attempt to inject SQL commands into the web application's database. A WAF can also help protect the web application from other common web-based attacks, such as cross-site scripting (XSS), remote file inclusion (RFI), or denial-of-service (DoS). References: CompTIA Cloud+ Certification Exam Objectives, page 14, section 2.7

**NEW QUESTION 9**
- (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 10**
- (Topic 1)
A systems administrator is deploying a GPU-accelerated VDI solution. Upon requests from several users, the administrator installs an older version of the OS on their virtual workstations. The majority of the VMs run the latest LTS version of the OS.
Which of the following types of drivers will MOST likely ensure compatibility will all virtual workstations?

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

**Answer:** D

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

**NEW QUESTION 10**
- (Topic 1)
An organization is hosting a DNS domain with private and public IP ranges. Which of the following should be implemented to achieve ease of management?

A. Network peering
B. A CDN solution
C. A SDN solution
D. An IPAM solution

**Answer:** D

**Explanation:**
An IP address management (IPAM) solution is a type of tool or system that automates and standardizes the allocation, tracking, and management of IP addresses in an IP network. An IPAM solution can help achieve ease of management for hosting a DNS domain with private and public IP ranges, as it can simplify and centralize the process of assigning and updating IP addresses for different DNS records or zones without manual intervention or errors. An IPAM solution can also help optimize DNS performance and security, as it can monitor and report any issues or conflicts related to IP addresses or DNS records. References: CompTIA Cloud+ Certification Exam Objectives, page 15, section 2.8
Reference: https://www.infoblox.com/glossary/ipam-ip-address-management/

**NEW QUESTION 13**
- (Topic 1)
A company has decided to get multiple compliance and security certifications for its public cloud environment. However, the company has few staff members to handle the extra workload, and it has limited knowledge of the current infrastructure.
Which of the following will help the company meet the compliance requirements as quickly as possible?

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

**Answer:** B

**Explanation:**
A cloud access security broker (CASB) is a type of security solution that acts as a gateway between cloud service users and cloud service providers. A CASB can help a company get multiple compliance and security certifications for its public cloud environment, as it can provide visibility, control, and protection for cloud data and applications. A CASB can also help the company handle the extra workload and overcome the limited knowledge of the current infrastructure, as it can

automate and simplify the enforcement of security policies and compliance requirements across multiple cloud services. References: CompTIA Cloud+ Certification Exam Objectives, page 14, section 2.7

**NEW QUESTION 15**
- (Topic 1)
An organization is implementing a new requirement to facilitate users with faster downloads of corporate application content. At the same time, the organization is also expanding cloud regions.
Which of the following would be suitable to optimize the network for this requirement?

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 18**
- (Topic 1)
A cloud administrator is switching hosting companies and using the same script that was previously used to deploy VMs in the new cloud. The script is returning errors that the command was not found.
Which of the following is the MOST likely cause of the script failure?

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

**Answer:** C

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

**NEW QUESTION 23**
- (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 26**
- (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 27**
- (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 31**
- (Topic 1)
A systems administrator notices that a piece of networking equipment is about to reach its end of support.
Which of the following actions should the administrator recommend?

A. Update the firmware
B. Migrate the equipment to the cloud
C. Update the OS
D. Replace the equipment

**Answer:** D

**Explanation:**
Replacing the equipment is the best action to take when a piece of networking equipment is about to reach its end of support. End of support means that the vendor or manufacturer will no longer provide technical assistance, updates, patches, or fixes for the equipment, which can affect its functionality, performance, security, and compatibility. Replacing the equipment with a newer model that has ongoing support can prevent any issues or risks associated with using outdated equipment.
References: CompTIA Cloud+ Certification Exam Objectives, page 18, section 3.5

**NEW QUESTION 35**
- (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 40**
- (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 41**
- (Topic 1)
A systems administrator needs to configure a set of policies to protect the data to comply with mandatory regulations.
Which of the following should the administrator implement to ensure DLP efficiently prevents the exposure of sensitive data in a cloud environment?

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

**Answer:** C

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

**NEW QUESTION 42**
- (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 43**
- (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 47**
- (Topic 1)
In an existing IaaS instance, it is required to deploy a single application that has different versions.
Which of the following should be recommended to meet this requirement?

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

**Answer:** A

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

**NEW QUESTION 50**
- (Topic 1)
Which of the following is relevant to capacity planning in a SaaS environment?

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

**Answer:** D

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

**NEW QUESTION 51**
- (Topic 1)
A cloud administrator is building a new VM for a network security appliance. The security appliance installer says the CPU clock speed does not meet the requirements.
Which of the following will MOST likely solve the issue?

A. Move the VM to a host with a faster CPU
B. Add more vCPUs to the VM
C. Enable CPU masking on the VM
D. Enable hyperthreading on the virtual host

**Answer:** A

**Explanation:**
Moving the VM to a host with a faster CPU is the best way to solve the issue of the security appliance installer saying the CPU clock speed does not meet the requirements when building a new VM for a network security appliance. Moving the VM to a host with a faster CPU can ensure that the VM meets the minimum CPU clock speed requirement for the security appliance, as it can use the physical CPU resources of the host. Moving the VM to a host with a faster CPU can also improve the performance and reliability of the security appliance, as it can reduce latency, contention, and overhead.
References: CompTIA Cloud+ Certification Exam Objectives, page 11, section 1.6

**NEW QUESTION 53**
- (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 55**
- (Topic 1)
An IaaS provider has numerous devices and services that are commissioned and decommissioned automatically on an ongoing basis. The cloud administrator needs to implement a solution that will help reduce administrative overhead.
Which of the following will accomplish this task?

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

**Answer:** A

**Explanation:**
IP address management (IPAM) is a type of tool or system that automates and standardizes the allocation, tracking, and management of IP addresses in an IP network. IPAM can help reduce administrative overhead for an IaaS provider that has numerous devices and services that are commissioned and decommissioned automatically on an ongoing basis, as it can simplify and centralize the process of assigning and reclaiming IP addresses for different devices and services without manual intervention or errors. IPAM can also help optimize network performance and security, as it can monitor and report any issues or conflicts related to IP addresses. References: CompTIA Cloud+ Certification Exam Objectives, page 15, section 2.8
Reference: https://www.infoblox.com/glossary/ipam-ip-address-management/

**NEW QUESTION 60**
- (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 63**
- (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 67**
- (Topic 2)
A systems administrator is using a configuration management tool to perform maintenance tasks in a system. The tool is leveraging the target system's API to perform these maintenance tasks After a number of features and security updates are applied to the target system, the configuration management tool no longer works as expected. Which of the following is the MOST likely cause of the issue?

A. The target system's API functionality has been deprecated
B. The password for the service account has expired
C. The IP addresses of the target system have changed
D. The target system has failed after the updates

**Answer:** A

**Explanation:**
The target system’s API (Application Programming Interface) functionality has been deprecated is what will most likely cause the issue of configuration management tool no longer working as expected after using it to perform maintenance tasks in a system using its API, and applying features and security updates to it. An API is a set of rules or specifications that defines how different software components or systems can communicate and interact with each other. An API functionality is a feature or function that an API provides or supports, such as methods, parameters, responses, etc. An API functionality can be deprecated when it is no longer maintained or supported by the API provider or developer, and is replaced or removed by a newer or better functionality. The target system’s API functionality has been deprecated can cause the issue by making the configuration management tool unable to use or access the API functionality that it relies on to perform maintenance tasks in the system, which may result in errors or failures.

**NEW QUESTION 71**
- (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

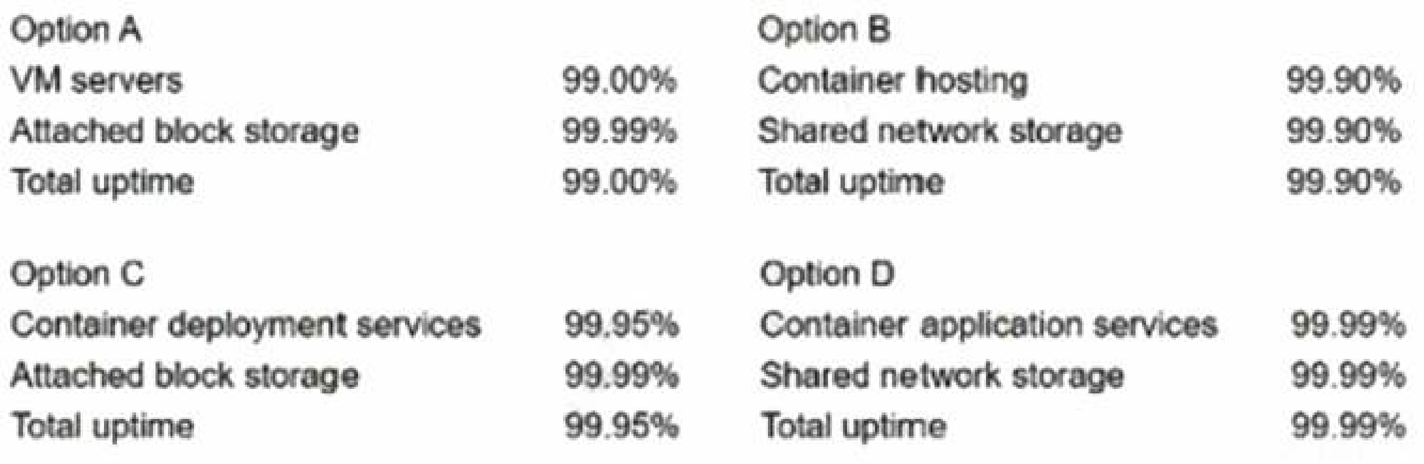
C. Subscription
D. Volume-based

**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 76**

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



| Option A | | Option B | |
|---|---|---|---|
| VM servers | 99.00% | Container hosting | 99.90% |
| Attached block storage | 99.99% | Shared network storage | 99.90% |
| Total uptime | 99.00% | Total uptime | 99.90% |
| Option C | | Option D | |
| Container deployment services | 99.95% | Container application services | 99.99% |
| Attached block storage | 99.99% | Shared network storage | 99.99% |
| Total uptime | 99.95% | Total uptime | 99.99% |

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

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

**Answer:** B

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

**NEW QUESTION 79**

- (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 80**

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

A. Install TLS certificates on the server.
B. Forward port 80 traffic to port 443.

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

**Answer:** ADE

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

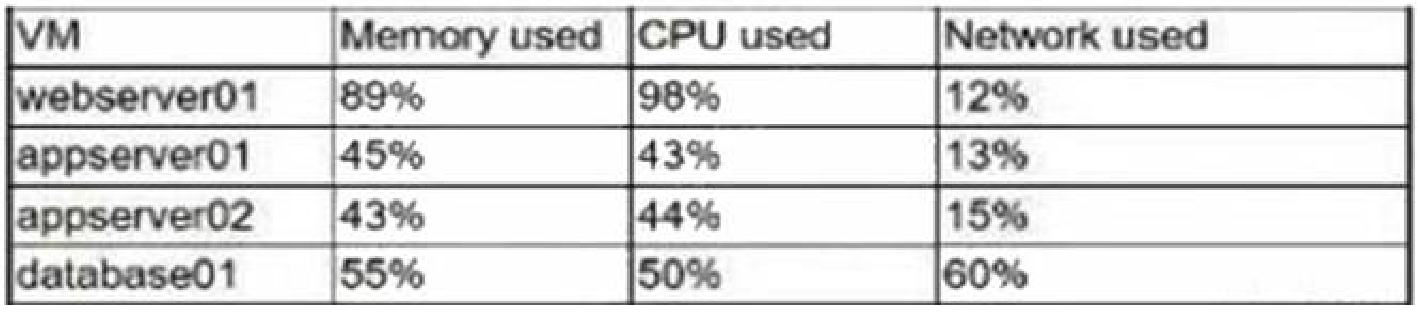
**NEW QUESTION 84**
- (Topic 2)
A company is concerned about the security of its data repository that contains customer PII. A systems administrator is asked to deploy a security control that will prevent the exfiltration of such data. Which of the following should the systems administrator implement?

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 89**
- (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 91**
- (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 95**
- (Topic 2)
A systems administrator has been asked to restore a VM from backup without changing the current VM's operating state. Which of the following restoration methods would BEST fit this scenario?

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

**Answer:** C

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

**NEW QUESTION 97**
- (Topic 2)
All of a company's servers are currently hosted in one cloud MSP. The company created a new cloud environment with a different MSP. A cloud engineer is now tasked with preparing for server migrations and establishing connectivity between clouds. Which of the following should the engineer perform FIRST?

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

**Answer:** C

**Explanation:**
Creating a VPN tunnel is the first action that the engineer should perform to
prepare for server migrations and establish connectivity between clouds. A VPN (Virtual Private Network) tunnel is a secure and encrypted connection that allows data to be transferred between two networks or locations over the public internet. Creating a VPN tunnel can enable communication and interoperability between different cloud environments, as well as protect data from interception or modification during migration.

**NEW QUESTION 102**
- (Topic 2)
A company has an in-house-developed application. The administrator wants to utilize cloud services for additional peak usage workloads. The application has a very unique stack of dependencies.
Which of the following cloud service subscription types would BEST meet these requirements?

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

**Answer:** D

**Explanation:**
IaaS (Infrastructure as a Service) is a cloud service model that provides basic computing resources such as servers, storage, network, etc., to the customers. The customers have full control and flexibility over these resources and can install and configure any software they need on them. IaaS is suitable for applications that have a unique stack of dependencies that may not be supported by other cloud service models.

**NEW QUESTION 103**
- (Topic 2)
A systems administrator is configuring updates on a system. Which of the following update branches should the administrator choose to ensure the system receives updates that are maintained for at least four years?

A. LTS
B. Canary
C. Beta
D. Stable

**Answer:** A

**Explanation:**
LTS (Long Term Support) is the update branch that the administrator should choose to ensure the system receives updates that are maintained for at least four years. An update branch is a category or group of updates that have different characteristics or features, such as frequency, stability, duration, etc. An update branch can help customers to choose the type of updates that suit their needs and preferences. LTS is an update branch that provides updates that are stable, reliable, and secure, and are supported for a long period of time, usually four years or more. LTS can help customers who value stability and security over new features or functions, and who do not want to change or upgrade their systems frequently.

**NEW QUESTION 108**
- (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 113**
- (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 116**
- (Topic 2)
A cloud administrator is setting up a new coworker for API access to a public cloud environment. The administrator creates a new user and gives the coworker access to a collection of automation scripts. When the coworker attempts to use a deployment script, a 403 error is returned. Which of the following is the MOST likely cause of the error?

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

**Answer:** B

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

**NEW QUESTION 119**
- (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 124**
- (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 127**
- (Topic 2)
A systems administrator is configuring network management but is concerned about confidentiality. Which of the following should the administrator configure to address this concern?

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

**Answer:** A

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

**NEW QUESTION 130**
- (Topic 2)
After a few new web servers were deployed, the storage team began receiving incidents in their queue about the web servers. The storage administrator wants to verify the incident tickets that should have gone to the web server team. Which of the following is the MOST likely cause of the issue?

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

**Answer:** C

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

**NEW QUESTION 132**
- (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 133**
- (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 137**
- (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 142**
- (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 147**
- (Topic 2)
A systems administrator is trying to reduce storage consumption. Which of the following file types would benefit the MOST from compression?

A. System files
B. User backups
C. Relational database
D. Mail database

**Answer:** B

**Explanation:**
User backups are the file type that would benefit the most from compression to reduce storage consumption. Compression is a process of reducing the size of data by removing redundant or unnecessary information or using algorithms to encode data more efficiently. Compression can save storage space and bandwidth, but it may also affect the quality or performance of data depending on the compression method and ratio. User backups are typically large files that contain various types of data, such as documents, images, videos, etc., that can be compressed without significant loss of quality or functionality.

**NEW QUESTION 148**
- (Topic 2)
A cloud administrator is upgrading a cloud environment and needs to update the automation script to use a new feature from the cloud provider. After executing the script, the deployment fails. Which of the following is the MOST likely cause?

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

**Answer:** A

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

**NEW QUESTION 151**
- (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 155**
- (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 158**
- (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 163**
- (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 166**
- (Topic 2)
A systems administrator is examining a managed hosting agreement and wants to determine how much data would be lost if a server had to be restored from backups. To which of the following metrics should the administrator refer?

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

**Answer:** C

**Explanation:**
RPO (Recovery Point Objective) is the metric that the administrator should refer to determine how much data would be lost if a server had to be restored from backups. RPO is a metric that measures how much data can be lost or how far back in time a recovery point can be without causing significant impact or damage. RPO can help to determine how much data would be lost by comparing the time of the disruption or disaster with the time of the last backup or snapshot. RPO can also help to determine how frequently backups or snapshots should be performed to minimize data loss.

**NEW QUESTION 171**
- (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 174**
- (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 175**
- (Topic 2)
Which of the following would be the BEST option for discussion of what individuals should do in an incident response or disaster recovery scenario?

A. A business continuity plan
B. Incident response/disaster recovery documentation

C. A tabletop exercise
D. A root cause analysis

**Answer:** C

**Explanation:**
A tabletop exercise is the best option for discussion of what individuals should do in an incident response or disaster recovery scenario. A tabletop exercise is a simulated scenario that involves key stakeholders and decision-makers who review and discuss their roles and responsibilities in response to an emergency situation or event. A tabletop exercise can help to test and evaluate plans, procedures, policies, training, and communication.

**NEW QUESTION 180**
- (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 184**
- (Topic 2)
An administrator has been informed that some requests are taking a longer time to respond than other requests of the same type. The cloud consumer is using multiple network service providers and is performing link load balancing for bandwidth aggregation. Which of the following commands will help the administrator understand the possible latency issues?

A. ping
B. ipconfig
C. traceroute
D. netstat

**Answer:** A

**Explanation:**
Ping is the command that will help the administrator understand the possible latency issues between different network service providers and link load balancing for bandwidth aggregation. Ping is a network utility that sends packets of data to a specific IP address or hostname and measures the time it takes for them to be sent back (round-trip time). Ping can help to test connectivity, availability, and latency of network devices or systems. Ping can help to understand latency issues by comparing the round-trip times between different network service providers and link load balancing devices, and identifying any delays or variations in response times.

**NEW QUESTION 187**
- (Topic 2)
A systems administrator is analyzing a report of slow performance in a cloud application. This application is working behind a network load balancer with two VMs, and each VM has its own digital certificate configured. Currently, each VM is consuming 85% CPU on average. Due to cost restrictions, the administrator cannot scale vertically or horizontally in the environment. Which of the following actions should the administrator take to decrease the CPU utilization? (Choose two.)

A. Configure the communication between the load balancer and the VMs to use a VPN.
B. Move the digital certificate to the load balancer.
C. Configure the communication between the load balancer and the VMs to use HTTP.
D. Reissue digital certificates on the VMs.
E. Configure the communication between the load balancer and the VMs to use HTTPS.
F. Keep the digital certificates on the VMs.

**Answer:** BC

**Explanation:**
Moving the digital certificate to the load balancer and configuring the communication between the load balancer and the VMs to use HTTP are two actions that will decrease the CPU utilization of the VMs that are running behind a network load balancer with two VMs, each with its own digital certificate configured. Moving the digital certificate to the load balancer will offload the SSL/TLS encryption and decryption tasks from the VMs to the load balancer, which can reduce the CPU overhead and improve performance. Configuring the communication between the load balancer and the VMs to use HTTP will eliminate the need for encryption and decryption between them, which can also reduce CPU consumption. However, this may introduce security risks if sensitive data is transmitted over HTTP.

**NEW QUESTION 188**
- (Topic 2)
A company is preparing a hypervisor environment to implement a database cluster. One of the requirements is to share the disks between the nodes of the cluster to access the same LUN. Which of the following protocols should the company use? (Choose two.)

A. CIFS
B. FTP
C. iSCSI

D. RAID 10
E. NFS
F. FC

**Answer:** CF

**Explanation:**
These are the protocols that should be used to share the disks between the nodes of a database cluster to access the same LUN (Logical Unit Number). A LUN is an identifier that represents a logical unit of storage, such as a disk, partition, volume, etc., that can be accessed by a host system or device. To share the disks between the nodes of a cluster, the following protocols can be used:
? iSCSI (Internet Small Computer System Interface): This is a protocol that allows SCSI commands to be sent over IP networks. iSCSI can enable block-level storage access over a network, which means that the host system or device can access the storage as if it were a local disk.
? FC (Fibre Channel): This is a protocol that provides high-speed and low-latency data transfer over optical fiber cables. FC can also enable block-level storage access over a network, which means that the host system or device can access the storage as if it were a local disk.

**NEW QUESTION 189**
- (Topic 2)
A development team recently completed testing changes to a company's web-based CMS in the sandbox environment. The cloud administrator deployed these CMS application changes to the staging environment as part of the next phase in the release life cycle. The deployment was successful, but after deploying the CMS application, the web page displays an error message stating the application is unavailable. After reviewing the application logs, the administrator sees an error message that the CMS is unable to connect to the database. Which of the following is the BEST action for the cloud administrator to perform to resolve the issue?

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

**Answer:** D

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

**NEW QUESTION 194**
- (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 197**
- (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 199**
- (Topic 2)
A company needs to access the cloud administration console using its corporate identity. Which of the following actions would MOST likely meet the requirements?

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

**Answer:** D

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

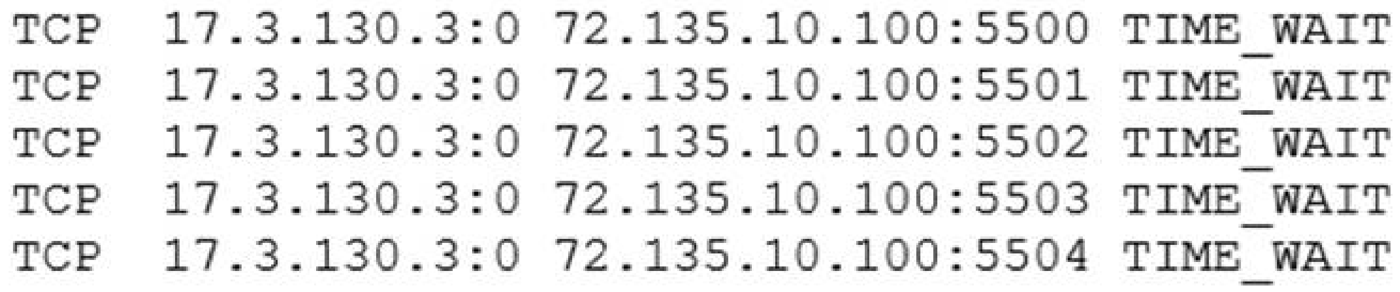
**NEW QUESTION 202**
- (Topic 2)
Which of the following actions should a systems administrator perform during the containment phase of a security incident in the cloud?

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 205**
- (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 208**
- (Topic 1)
Company A has acquired Company B and is in the process of integrating their cloud resources. Company B needs access to Company A's cloud resources while retaining its IAM solution.
Which of the following should be implemented?

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

D. Directory service

**Answer:** C

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

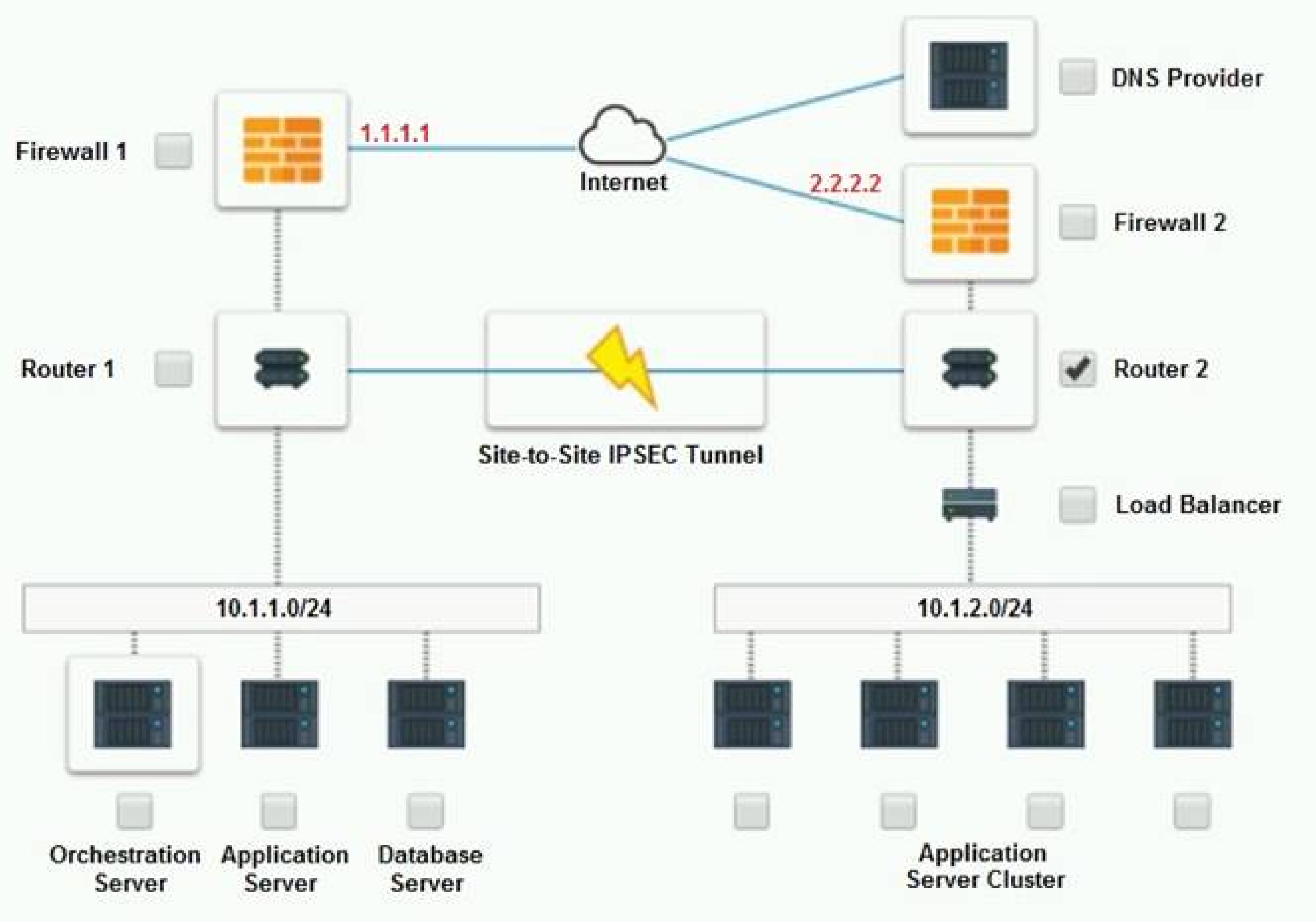
**NEW QUESTION 212**
- (Topic 1)
A systems administrator needs to configure SSO authentication in a hybrid cloud environment.
Which of the following is the BEST technique to use?

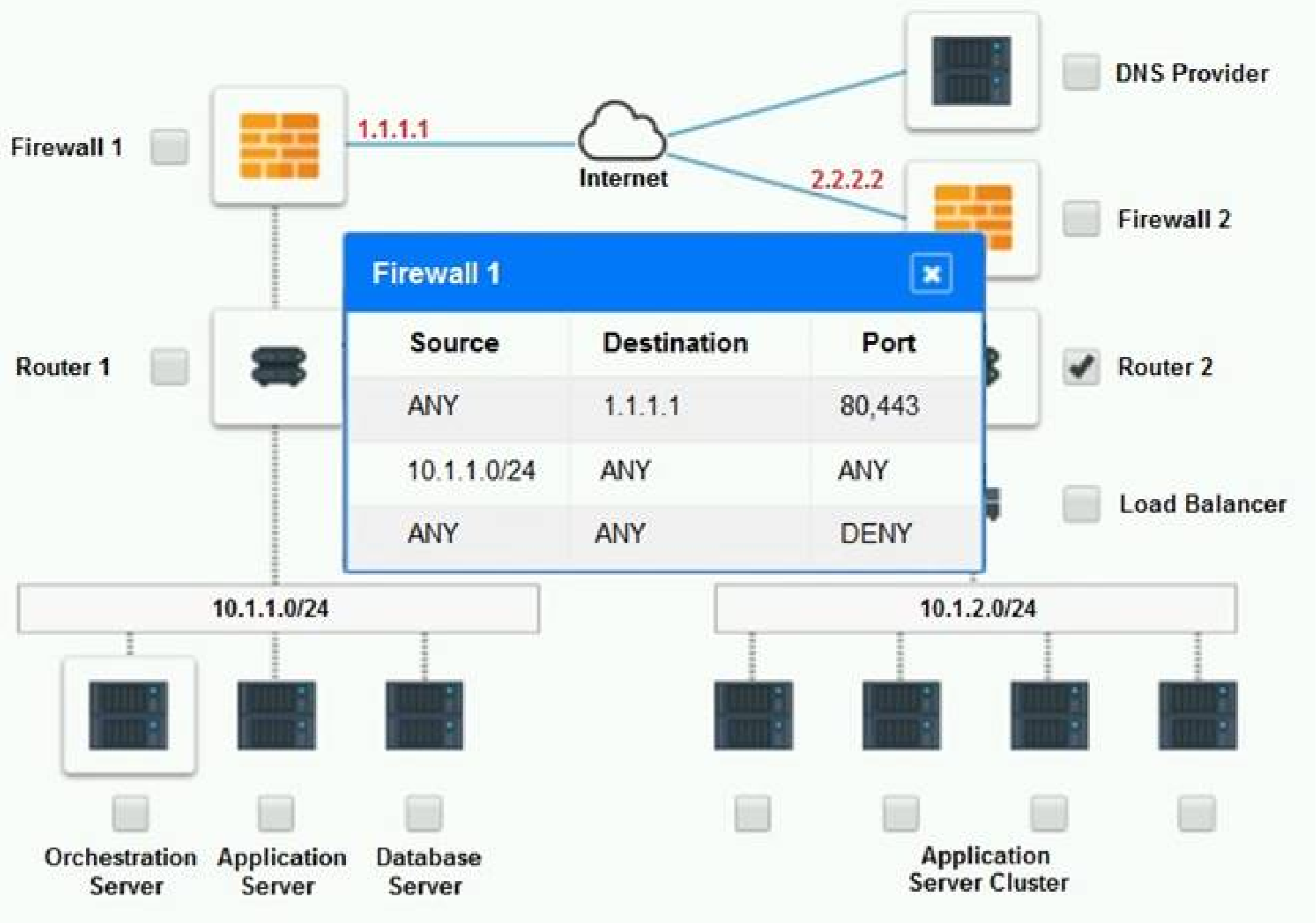
A. Access controls
B. Federation
C. Multifactor authentication
D. Certificate authentication

**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

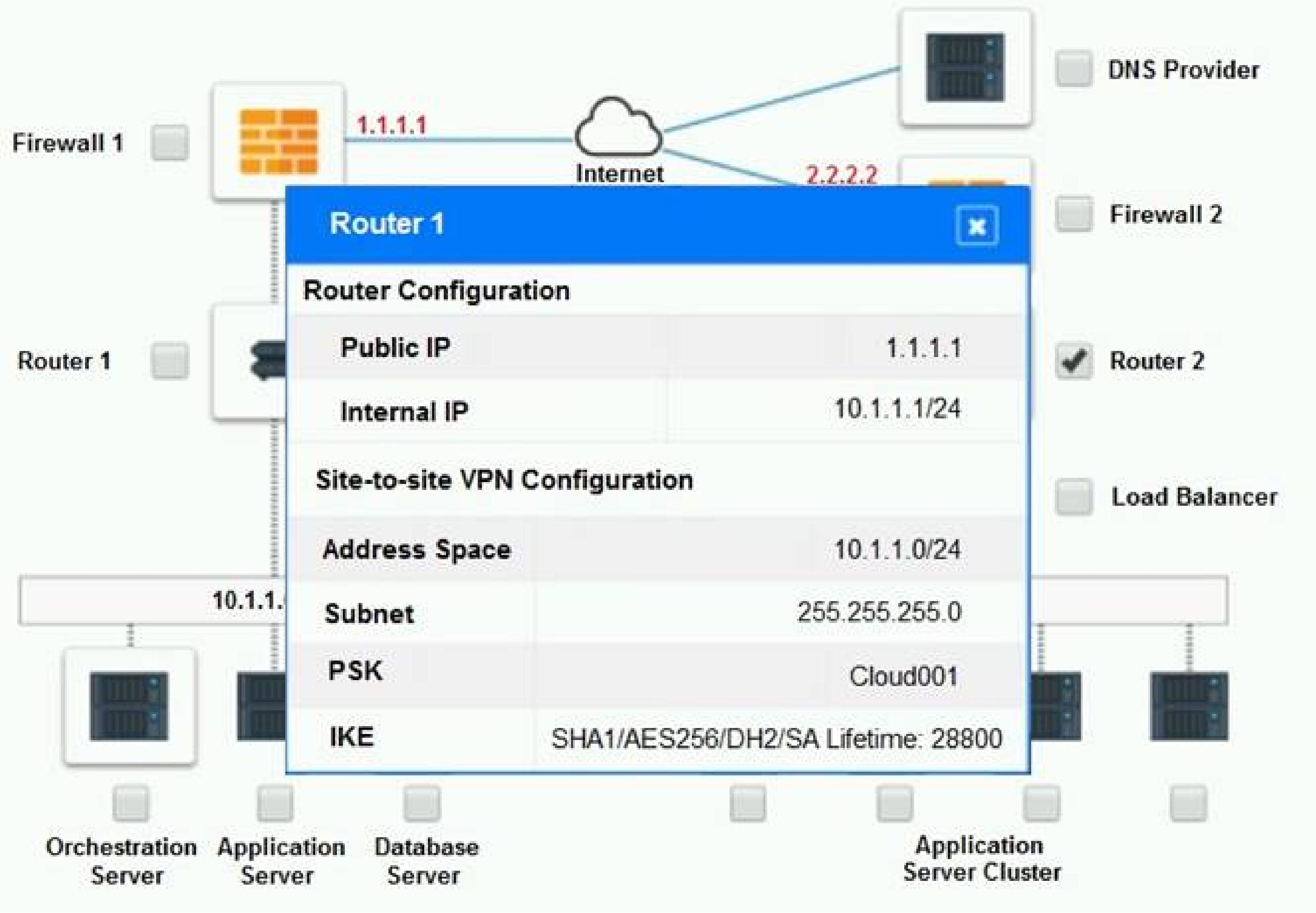
**NEW QUESTION 215**
SIMULATION - (Topic 1)
A company has decided to scale its e-commerce application from its corporate datacenter to a commercial cloud provider to meet an anticipated increase in demand during an upcoming holiday.
The majority of the application load takes place on the application 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 |



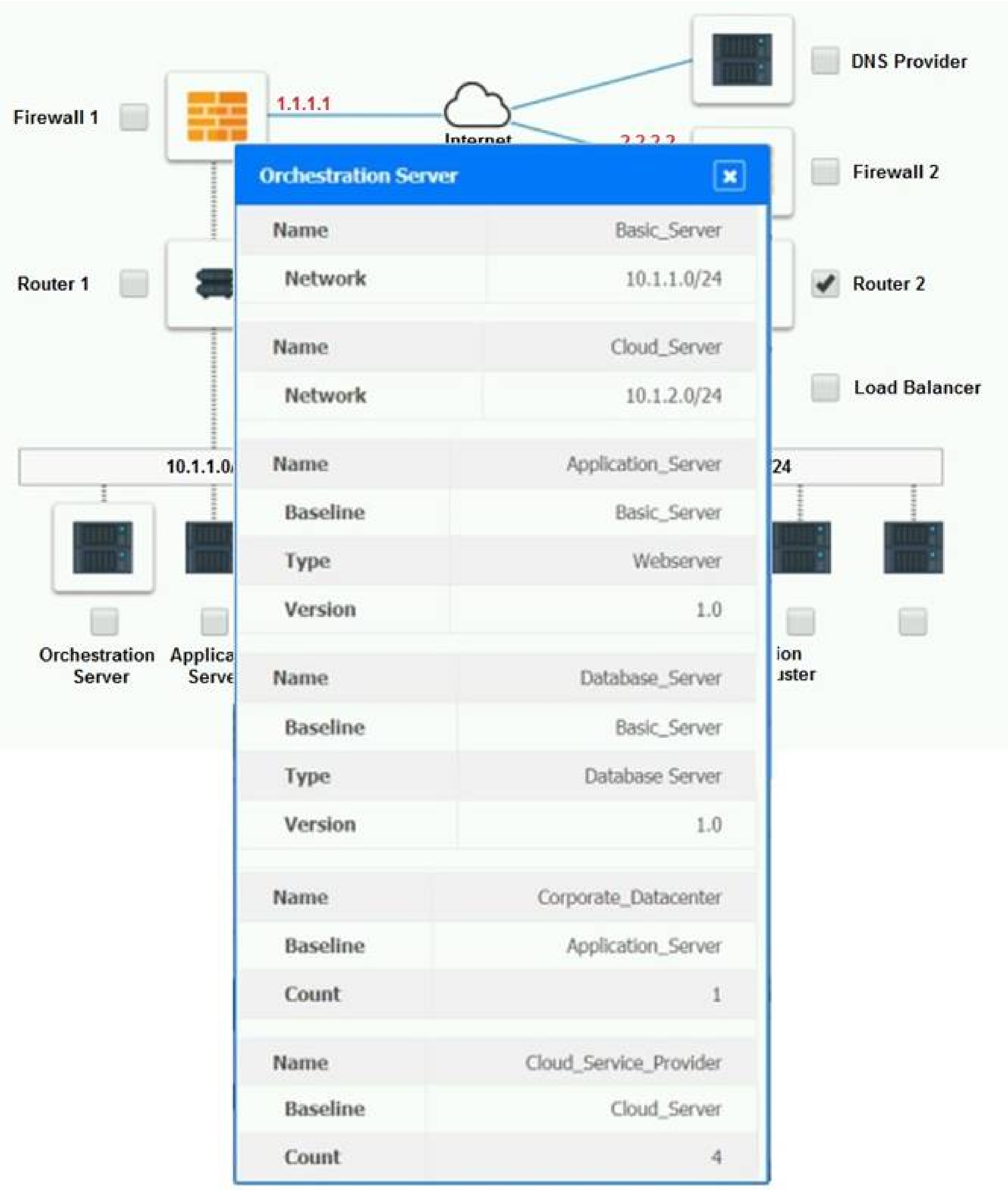
Router 1 ☒

Router Configuration

| | |
|---|---|
| Public IP | 1.1.1.1 |
| Internal IP | 10.1.1.1/24 |

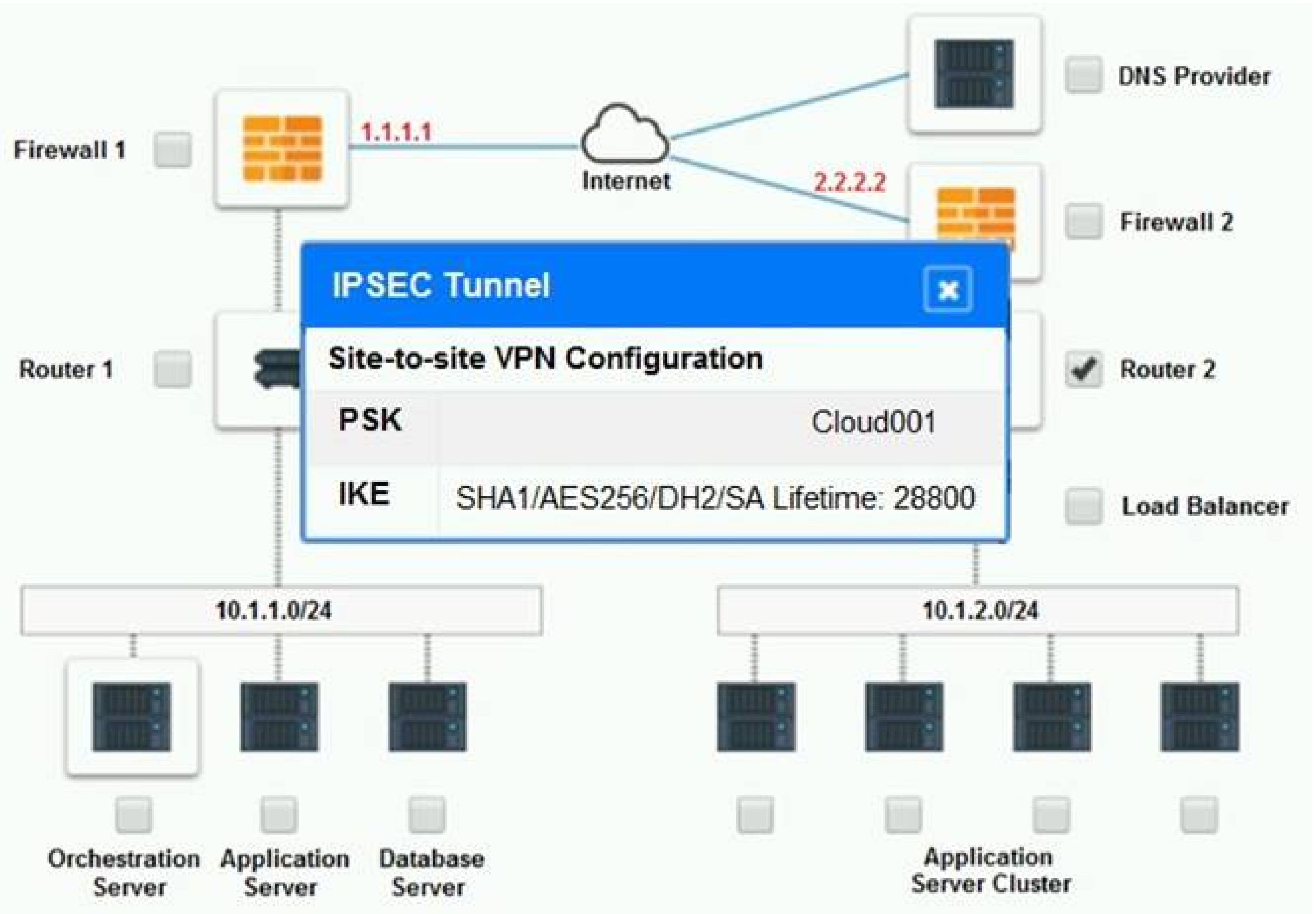
Site-to-site VPN Configuration

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



Orchestration Server

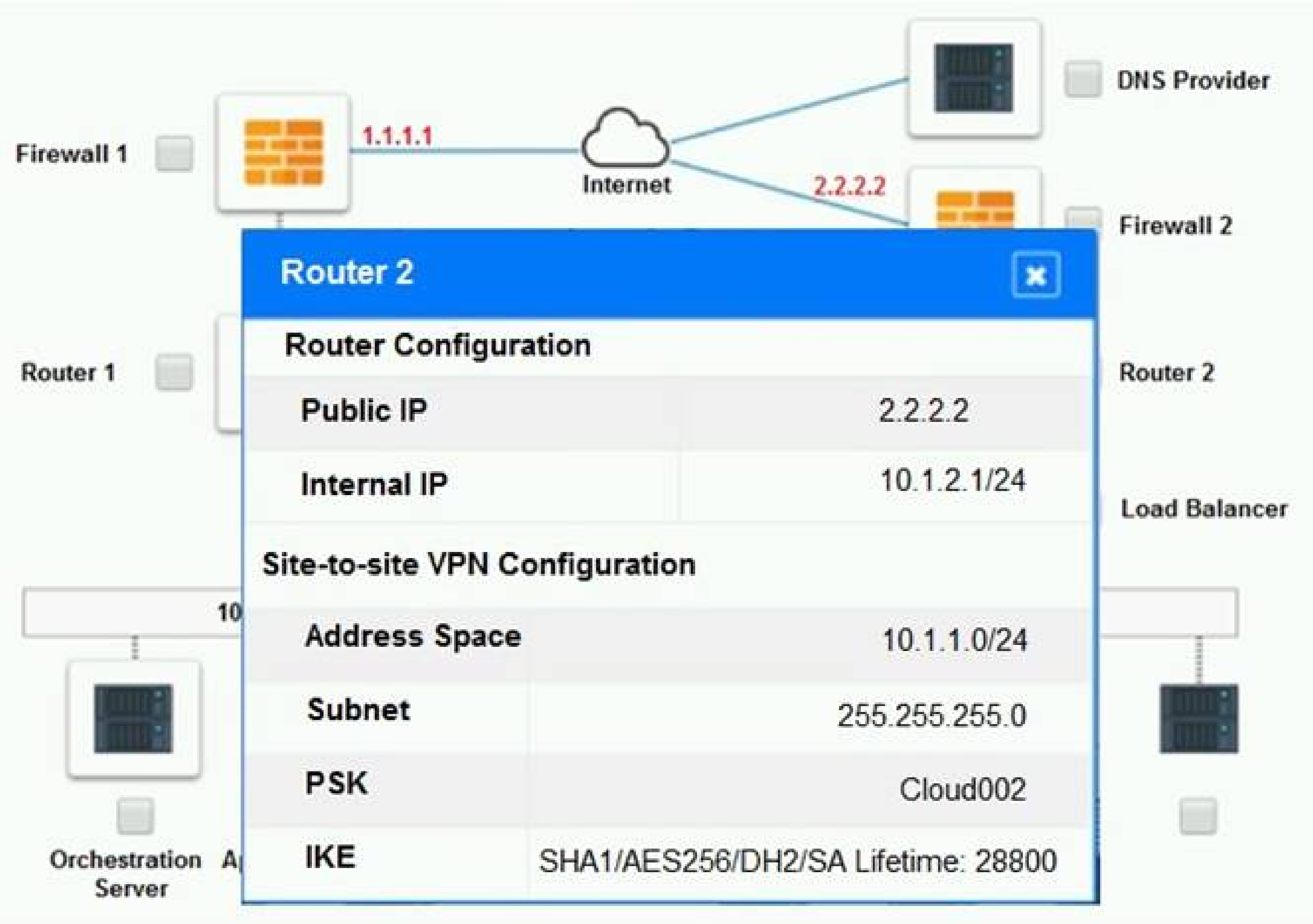
| | |
|---|---|
| Name | Basic_Server |
| Network | 10.1.1.0/24 |
| Name | Cloud_Server |
| Network | 10.1.2.0/24 |
| Name | Application_Server |
| Baseline | Basic_Server |
| Type | Webserver |
| Version | 1.0 |
| Name | Database_Server |
| Baseline | Basic_Server |
| Type | Database Server |
| Version | 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 |



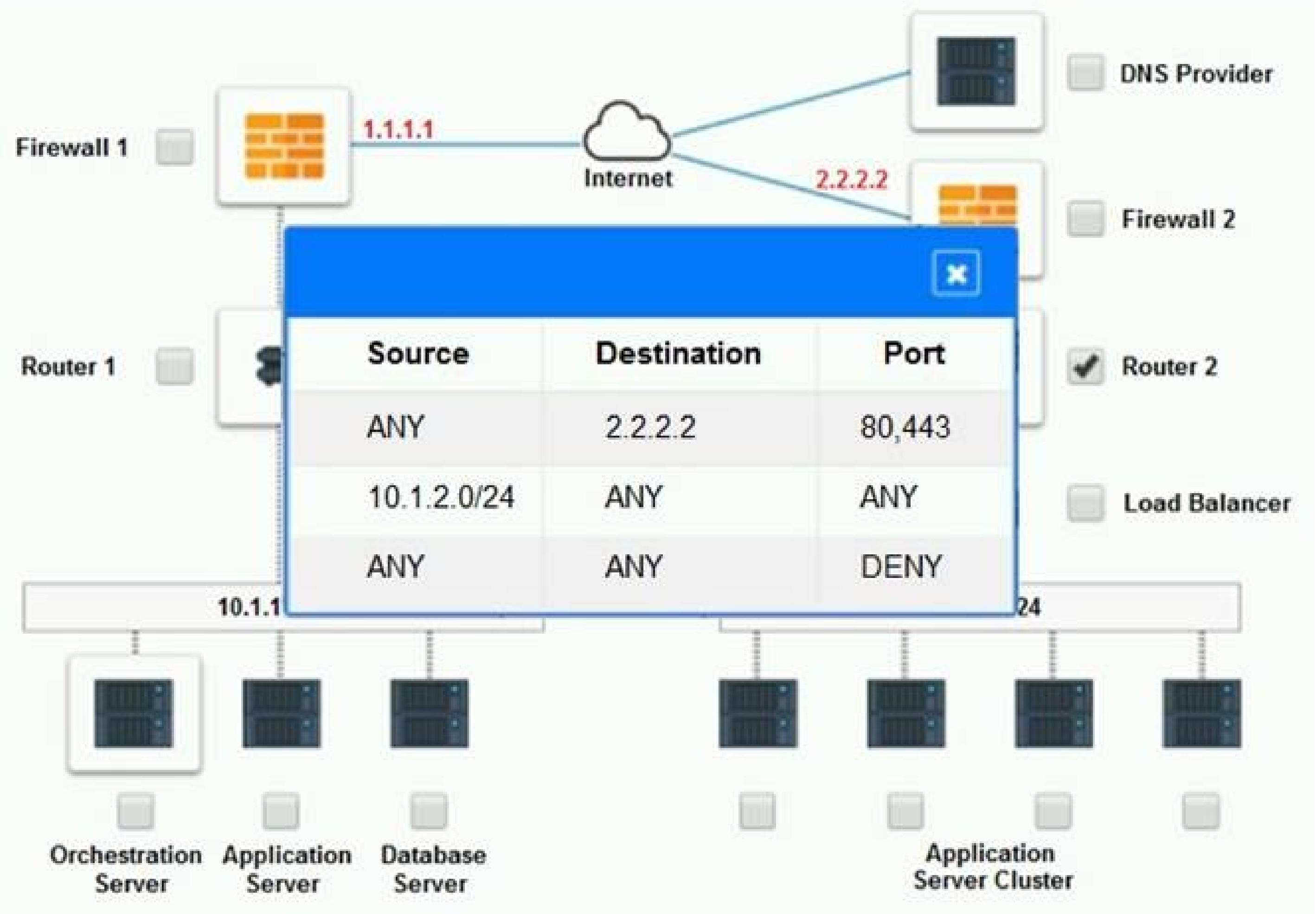
Router 2

Router Configuration

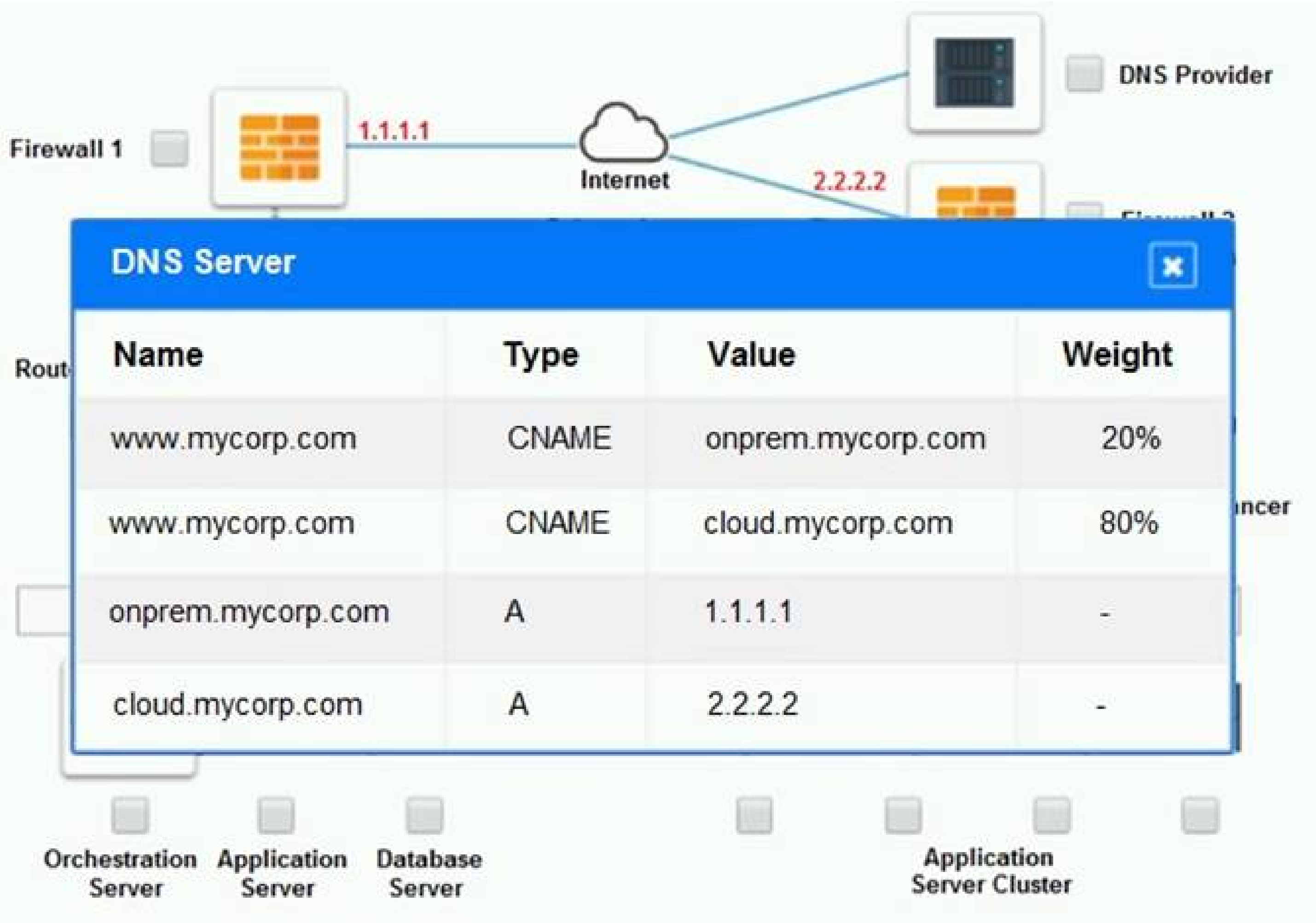
| | |
|---|---|
| Public IP | 2.2.2.2 |
| Internal IP | 10.1.2.1/24 |

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 |



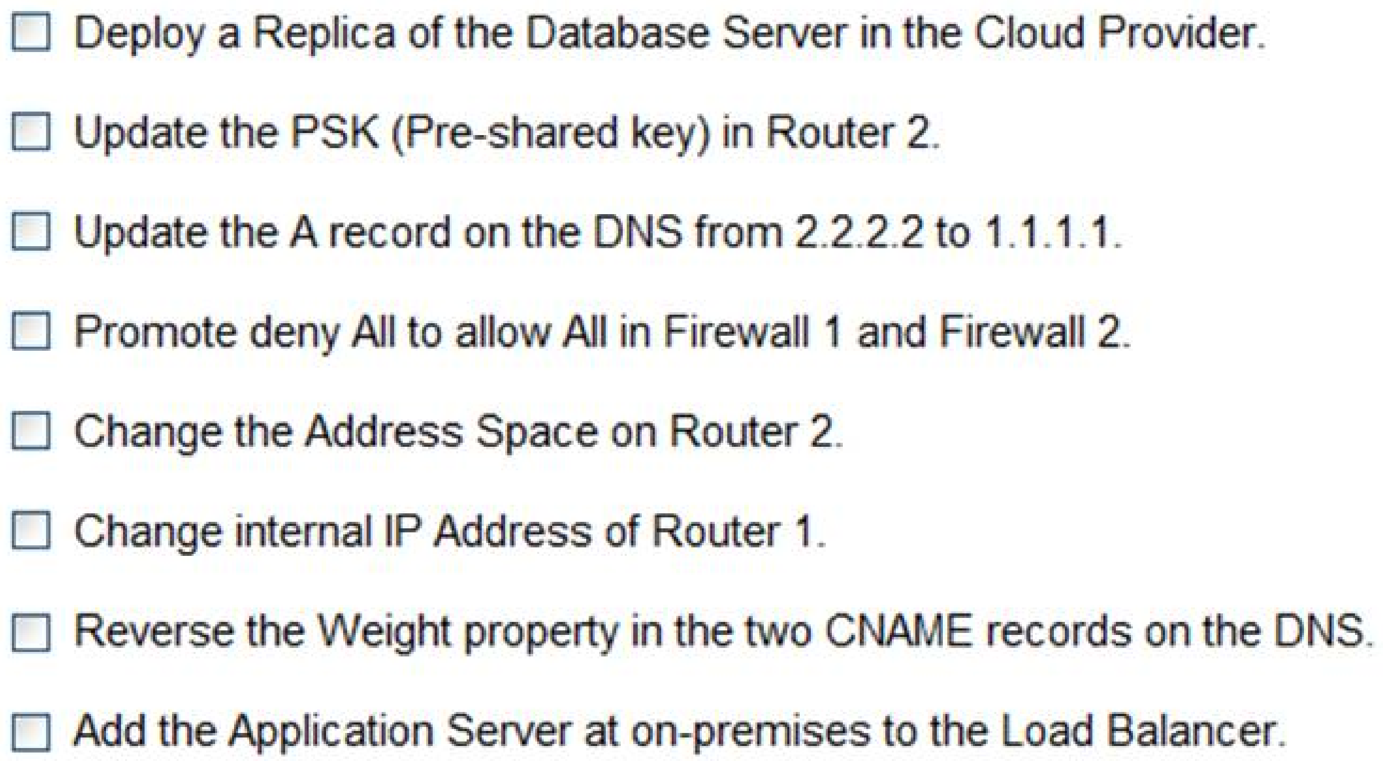
| Source | Destination | Port |
|---|---|---|
| ANY | 2.2.2.2 | 80,443 |
| 10.1.2.0/24 | ANY | ANY |
| ANY | ANY | DENY |



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 217**
- (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 218**
- (Topic 1)
A cloud architect is designing the VPCs for a new hybrid cloud deployment. The business requires the following:
? High availability
? Horizontal auto-scaling
? 60 nodes peak capacity per region
? Five reserved network IP addresses per subnet
? /24 range
Which of the following would BEST meet the above requirements?

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

**Answer:** C

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

**NEW QUESTION 219**
- (Topic 1)
A systems administrator is deploying a solution that requires a virtual network in a private cloud environment. The solution design requires the virtual network to transport multiple payload types.
Which of the following network virtualization options would BEST satisfy the requirement?

A. VXLAN
B. STT
C. NVGRE
D. GENEVE

**Answer:** D

**Explanation:**
Generic Network Virtualization Encapsulation (GENEVE) is a type of network virtualization technology that creates logical networks or segments that span across multiple physical networks or locations. GENEVE can satisfy the requirement of transporting multiple payload types in a virtual network in a private cloud environment, as it can support various network protocols and services by using a flexible and extensible header format that can encapsulate different types of payloads within UDP packets. GENEVE can also provide interoperability and compatibility, as it can integrate with existing network virtualization technologies such as VXLAN, STT, or NVGRE. References: CompTIA Cloud+ Certification Exam Objectives, page 15, section 2.8

**NEW QUESTION 220**
- (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 221**
- (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 224**
- (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 229**
- (Topic 1)
A systems administrator is deploying a new storage array for backups. The array provides 1PB of raw disk space and uses 14TB nearline SAS drives. The solution must tolerate at least two failed drives in a single RAID set.
Which of the following RAID levels satisfies this requirement?

A. RAID 0
B. RAID 1
C. RAID 5
D. RAID 6
E. RAID 10

**Answer:** D

**Explanation:**
RAID 6 is a type of RAID level that uses block-level striping with two parity blocks distributed across all member disks. RAID 6 can provide redundancy and fault tolerance, as it can survive the failure of up to two disks without losing any data. RAID 6 can also support large data sets and high-capacity disks, as it can offer more usable space and better performance than other RAID levels with similar features, such as RAID 5 or RAID 10. RAID 6 is the best RAID level for a systems administrator to use when deploying a new
storage array for backups that provides 1PB of raw disk space and uses 14TB nearline SAS drives and must tolerate at least two failed drives in a single RAID set. References: CompTIA Cloud+ Certification Exam Objectives, page 9, section 1.4

**NEW QUESTION 231**
- (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 232**
- (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 235**
- (Topic 1)
Which of the following will mitigate the risk of users who have access to an instance modifying the system configurations?

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

**Answer:** D

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

**NEW QUESTION 237**
- (Topic 1)
An organization’s web server farm, which is hosted in the cloud with DNS load balancing, is experiencing a spike in network traffic. This has caused an outage of the organization’s web server infrastructure.
Which of the following should be implemented to prevent this in the future as a mitigation method?

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

**Answer:** D

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

**NEW QUESTION 240**
- (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 241**
- (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 244**
- (Topic 1)
A systems administrator is configuring a storage array.
Which of the following should the administrator configure to set up mirroring on this array?

A. RAID 0
B. RAID 1
C. RAID 5
D. RAID 6

**Answer:** B

**Explanation:**
RAID 1 is a type of RAID level that creates an exact copy or mirror of data on two or more disks. RAID 1 can provide redundancy and fault tolerance, as it can survive the failure of one disk without losing any data. RAID 1 can also improve read performance, as it can access data from multiple disks simultaneously. The administrator should configure RAID 1 to set up mirroring on a storage array. References: CompTIA Cloud+ Certification Exam Objectives, page 9, section 1.4

**NEW QUESTION 249**
- (Topic 1)
The human resources department was charged for a cloud service that belongs to another department. All other cloud costs seem to be correct.
Which of the following is the MOST likely cause for this error?

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

**Answer:** D

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

**NEW QUESTION 250**
- (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 251**
- (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 253**
- (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 a technique that collects and analyzes data about the services and resource utilization on VMs in a cloud environment. Performance monitoring can help the systems administrator to gather information about the CPU, memory, disk, network, and application performance of the VMs, as well as identify any bottlenecks, errors, or anomalies that may affect the cloud service quality. Performance monitoring can be implemented using various tools or agents that can collect and report the performance metrics from the VMs to a centralized dashboard or console. Performance monitoring can also help the systems administrator to optimize, troubleshoot, and plan the cloud resources and services. References: CompTIA Cloud+ CV0-003 Certification Study Guide, Chapter 5, Objective 5.1: Given a scenario, monitor cloud resources and services.

**NEW QUESTION 256**
- (Topic 4)
Which of the following are advantages of a public cloud? (Select TWO).

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

**Answer:** BD

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

investment or long-term contracts, and allows customers to optimize their spending and performance1234

**NEW QUESTION 258**
- (Topic 4)
A systems administrator is deploying a new version of a website. The website is deployed in the cloud using a VM cluster. The administrator must then deploy the new version into one VM first. After a period of time, if there are no issues detected, a second VM will be updated. This process must continue until all the VMS are updated. Which of the following upgrade methods is being implemented?

A. Canary
B. Blue-green
C. Rolling
D. Staging

**Answer:** C

**Explanation:**
The upgrade method that is being implemented by the systems administrator is rolling. A rolling upgrade is a type of upgrade that applies the new version of a software or service to a subset of nodes or instances at a time, while the rest of the nodes or instances continue to run the old version. This way, the upgrade can be performed gradually and incrementally, without causing downtime or disruption to the entire system. A rolling upgrade can also help to monitor and test the new version for any issues or errors, and roll back to the old version if needed12.
A canary upgrade is a type of upgrade that applies the new version of a software or service to a small and selected group of users or customers, before rolling it out to the rest of the population. This way, the upgrade can be evaluated for its performance, functionality, and feedback, and any problems or bugs can be fixed before affecting the majority of users or customers34.
A blue-green upgrade is a type of upgrade that involves having two identical environments, one running the old version (blue) and one running the new version (green) of a software or service. The traffic is switched from the blue environment to the green environment once the new version is ready and tested. This way, the upgrade can be performed quickly and seamlessly, without any downtime or risk of failure. The blue environment can also serve as a backup in case of any issues with the green environment5 .
A staging upgrade is a type of upgrade that involves having a separate environment that mimics the production environment, where the new version of a software or service is deployed and tested before moving it to the production environment. This way, the upgrade can be verified and validated for its compatibility, security, and quality, and any defects or errors can be resolved before affecting the live system .

**NEW QUESTION 263**
- (Topic 4)
A company uses multiple SaaS-based cloud applications. All the applications require authentication upon access. An administrator has been asked to address this issue and enhance security. Which of the following technologies would be the BEST solution?

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

**Answer:** A

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

**NEW QUESTION 264**
......