

# Exam Questions CV0-003

CompTIA Cloud+ Certification Exam

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



### NEW QUESTION 1

- (Topic 1)

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

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

**Answer:** D

#### Explanation:

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

References: CompTIA Cloud+ Certification Exam Objectives, page 15, section 2.8

### NEW QUESTION 2

- (Topic 1)

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 3

- (Topic 1)

A cloud administrator checked out the deployment scripts used to deploy the sandbox environment to a public cloud provider. The administrator modified the script to add an application load balancer in front of the web-based front-end application. The administrator next used the script to recreate a new sandbox environment successfully, and the application was then using the new load balancer.

The following week, a new update was required to add more front-end servers to the sandbox environment. A second administrator made the necessary changes and checked out the deployment scripts. The second administrator then ran the script, but the application load balancer was missing from the new deployment. Which of the following is the MOST likely reason for this issue?

- A. The license limit on the number of server deployments allowed per month was exceeded
- B. The deployment script changes made by the first administrator were not checked in and committed
- C. The new server images were incompatible with the application load-balancer configuration
- D. The application load balancer exceeded the maximum number of servers it could use

**Answer:** B

#### Explanation:

Checking in and committing are actions that save and update the changes made to a file or code in a version control system or repository. Checking in and committing can help track and synchronize the changes made by different users or developers working on the same file or code. The deployment script changes made by the first administrator were not checked in and committed is the most likely reason for the issue of the application load balancer being missing from the new deployment after a second administrator made some changes and ran the script. If the first administrator did not check in and commit the changes made to add an application load balancer to the script, then those changes would not be reflected or available in the latest version of the script used by the second administrator. References: CompTIA Cloud+ Certification Exam Objectives, page 13, section 2.5

### NEW QUESTION 4

- (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 5

- (Topic 1)

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

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

**Answer: B**

#### Explanation:

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

#### NEW QUESTION 6

- (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 implemented. Reference: <https://www.ekransystem.com/en/blog/rbac-vs-abac>

#### NEW QUESTION 7

- (Topic 1)

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

Which of the following should the administrator recommend the user do FIRST?

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

**Answer: D**

#### Explanation:

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

#### NEW QUESTION 8

- (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 9**

- (Topic 1)

An administrator is performing an in-place upgrade on a guest 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 10**

- (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 10**

- (Topic 1)

An organization has the following requirements that need to be met when implementing cloud services:

? SSO to cloud infrastructure

? On-premises directory service

? RBAC for IT staff

Which of the following cloud models would meet these requirements?

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

**Answer: C**

**Explanation:**

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

**NEW QUESTION 15**

- (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 20**

- (Topic 1)

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

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

**Answer:** AF

**Explanation:**

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

**NEW QUESTION 23**

- (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\\_openshift\\_platform/13/html/network\\_functions\\_virtualization\\_planning\\_and\\_configuration\\_guide/part-sriov-nfv-configuration](https://access.redhat.com/documentation/en-us/red_hat_openshift_platform/13/html/network_functions_virtualization_planning_and_configuration_guide/part-sriov-nfv-configuration)

**NEW QUESTION 24**

- (Topic 1)

A systems administrator is configuring RAID for a new server. This server will host files for users and replicate to an identical server. While redundancy is necessary, the most important need is to maximize storage.

Which of the following RAID types should the administrator choose?

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 28**

- (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 30

- (Topic 1)

A company has developed a cloud-ready application. Before deployment, an administrator needs to select a deployment technology that provides a high level of portability and is lightweight in terms of footprint and resource requirements.

Which of the following solutions will be BEST to help the administrator achieve the requirements?

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

**Answer:** A

#### Explanation:

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

Reference: <https://blog.netapp.com/blogs/containers-vs-vms/>

### NEW QUESTION 34

- (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 35

- (Topic 1)

A systems administrator is creating a playbook to run tasks against a server on a set schedule.

Which of the following authentication techniques should the systems administrator use within the playbook?

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

**Answer:** C

#### Explanation:

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

### NEW QUESTION 38

- (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 40

- (Topic 1)

A company has deployed a new cloud solution and is required to meet security compliance.

Which of the following will MOST likely be executed in the cloud solution to meet security requirements?

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

**Answer:** C

#### Explanation:

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

References: CompTIA Cloud+ Certification Exam Objectives, page 14, section 2.7

#### NEW QUESTION 43

- (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 46

- (Topic 1)

A cloud administrator is reviewing a new application implementation document. The administrator needs to make sure all the known bugs and fixes are applied, and unwanted

ports and services are disabled.

Which of the following techniques would BEST help the administrator assess these business requirements?

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

**Answer:** D

#### Explanation:

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

#### NEW QUESTION 49

- (Topic 1)

A company has a cloud infrastructure service, and the cloud architect needs to set up a DR site.

Which of the following should be configured in between the cloud environment and the DR site?

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

**Answer:** D

#### Explanation:

Replication is a process of copying or synchronizing data from one location to another to ensure consistency and availability. Replication can help set up a disaster recovery (DR) site for a cloud environment, as it can enable data backup and recovery in case of a failure or outage in the primary site. Replication can also improve performance and reliability, as it can reduce latency and load by distributing data across multiple sites. Replication should be configured between the

cloud environment and the DR site to ensure data protection and continuity. References: CompTIA Cloud+ Certification Exam Objectives, page 10, section 1.5

#### NEW QUESTION 50

- (Topic 1)

A media company has made the decision to migrate a physical, internal file server to the cloud and use a web-based interface to access and manage the files. The users must be able to use their current corporate logins.

Which of the following is the MOST efficient way to achieve this goal?

- A. Deploy a VM in a cloud, attach storage, and copy the files across
- B. Use a SaaS service with a directory service federation
- C. Deploy a fileshare in a public cloud and copy the files across
- D. Copy the files to the object storage location in a public cloud

**Answer: B**

#### Explanation:

Software as a service (SaaS) is a type of cloud service model that provides software applications over the Internet that are hosted and managed by a cloud service provider. Directory service 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. Using a SaaS service with a directory service federation can help migrate an internal file server to the cloud and use a web-based interface to access and manage the files, as it can eliminate the need for maintaining an on-premises file server and enable seamless and secure access to cloud-based files using the same corporate logins. References: CompTIA Cloud+ Certification Exam Objectives, page 8, section 1.2

#### NEW QUESTION 54

- (Topic 1)

A systems administrator recently upgraded the processors in a web application host. Upon the next login, the administrator sees a new alert regarding the license being out of compliance.

Which of the following licensing models is the application MOST likely using?

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

**Answer: C**

#### Explanation:

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

Reference: [https://download.microsoft.com/download/3/d/4/3d42bdc2-6725-4b29-b75a-a5b04179958b/percorelicensing\\_definitions\\_vlbrief.pdf](https://download.microsoft.com/download/3/d/4/3d42bdc2-6725-4b29-b75a-a5b04179958b/percorelicensing_definitions_vlbrief.pdf)

#### NEW QUESTION 56

- (Topic 1)

A cloud architect wants to minimize the risk of having systems administrators in an IaaS compute instance perform application code changes. The development group should be the only group allowed to modify files in the directory.

Which of the following will accomplish the desired objective?

- A. Remove the file write permissions for the application service account.
- B. Restrict the file write permissions to the development group only.
- C. Add access to the fileshare for the systems administrator's group.
- D. Deny access to all development user accounts

**Answer: B**

#### Explanation:

File write permissions are permissions that control who can modify or delete files in a directory or system. Restricting the file write permissions to the development group only can help minimize the risk of having systems administrators in an IaaS compute instance perform application code changes, as it can prevent anyone other than the development group from altering or removing any files in the directory where the application code is stored. Restricting the file write permissions can also help maintain consistency and integrity, as it can ensure that only authorized and qualified users can make changes to the application code. References: CompTIA Cloud+ Certification Exam Objectives, page 14, section 2.7

#### NEW QUESTION 60

- (Topic 2)

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

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

**Answer: B**

#### Explanation:

Moving the virtual machine to flash storage and testing again is what the administrator should do next to resolve the issue of disk-related performance issue with a virtual database server that has been identified as being caused by a lack of IOPS on the existing spinning disk storage. IOPS (Input/Output Operations Per Second) is a measure of how fast a storage device can read and write data. IOPS can affect performance of a virtual database server by determining how quickly it

can access and process data from storage. Spinning disk storage is a type of storage device that uses rotating magnetic disks to store data. Spinning disk storage has lower IOPS than flash storage, which is a type of storage device that uses solid-state memory chips to store data. Flash storage has higher IOPS than spinning disk storage, which means that it can read and write data faster and more efficiently than spinning disk storage. Moving the virtual machine to flash storage and testing again can help to resolve the issue by increasing the IOPS and improving the performance of the virtual database server.

#### NEW QUESTION 63

- (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 64

- (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 68

- (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 70

- (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 71**

- (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 72**

- (Topic 2)

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

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

**Answer: C**

**Explanation:**

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

**NEW QUESTION 74**

- (Topic 2)

Users are experiencing slow response times from an intranet website that is hosted on a cloud platform. There is a site-to-site VPN connection to the cloud provider over a link of 100Mbps.

Which of the following solutions will resolve the issue the FASTEST?

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

**Answer: B**

**Explanation:**

Ordering a direct link to the provider is the fastest solution to resolve the issue of slow response times from an intranet website that is hosted on a cloud platform.

A direct link is a dedicated, high-bandwidth, low-latency connection between the customer's network and the cloud provider's network. It bypasses the public internet and provides better performance, security, and reliability. Examples of direct links are AWS Direct Connect, Azure ExpressRoute, Google Cloud Interconnect, etc.

#### NEW QUESTION 75

- (Topic 2)

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

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

**Answer:** A

#### Explanation:

Checking the logs on the VM is the next step that the administrator should take if the cloud SQL database has stopped running after an update deployment. Logs are records of events and activities that occur on a system or application. Logs can provide useful information for troubleshooting and identifying the root cause of an issue. The administrator should look for any errors, warnings, or messages that indicate what happened to the SQL database service and why it stopped running.

#### NEW QUESTION 78

- (Topic 2)

Which of the following cloud services is fully managed?

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

**Answer:** E

#### Explanation:

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

#### NEW QUESTION 83

- (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 88

- (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 93

- (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 96

- (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 98

- (Topic 2)

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

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

**Answer:** B

#### Explanation:

CASB (Cloud Access Security Broker) is what should be deployed to monitor and control the use of multiple SaaS-based business applications in a cloud environment. SaaS (Software as a Service) is a cloud service model that provides customers with access to software applications hosted on remote servers over a network or internet connection. SaaS can provide customers with convenience, flexibility, and scalability, but it may also introduce security risks such as data breaches, leaks, losses, etc., especially if customers have multiple SaaS subscriptions from different providers. CASB is a tool or service that acts as an intermediary between customers and SaaS providers. CASB can help to monitor and control the use of multiple SaaS subscriptions by providing features such as:

? Visibility: CASB can provide visibility into what SaaS applications are being used, by whom, when, where, how, etc., as well as identify any unauthorized or suspicious activities.

? Compliance: CASB can provide compliance with various laws, regulations, standards, policies, etc., that apply to SaaS applications and data, such as GDPR, HIPAA, PCI DSS, etc., as well as enforce them using rules or actions.

? Security: CASB can provide security for SaaS applications and data by detecting and preventing any threats or attacks, such as malware, phishing, ransomware, etc., as well as protecting them using encryption, authentication, authorization, etc.

### NEW QUESTION 102

- (Topic 2)

A systems administrator has finished installing monthly updates to servers in a cloud environment. The administrator notices certain portions of the playbooks are no longer functioning. Executing the playbook commands manually on a server does not work as well. There are no other reports of issues. Which of the following is the MOST likely cause of this issue?

- A. Change management failure
- B. Service overload
- C. Patching failure
- D. Job validation issues
- E. Deprecated features

**Answer:** E

#### Explanation:

Deprecated features are features that are no longer supported or recommended by the software vendor or provider. They may be removed or replaced by newer features in future updates or versions. If a playbook relies on deprecated features, it may stop functioning after an update or patch is applied to the software. The administrator should check the release notes or documentation of the software to identify and replace any deprecated features in the playbook.

#### NEW QUESTION 106

- (Topic 2)

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

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

**Answer:** C

#### Explanation:

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

#### NEW QUESTION 107

- (Topic 2)

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

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

**Answer:** CF

#### Explanation:

These are the components of the hypervisors that should be upgraded by the administrator who is performing upgrades to all the hypervisors in the environment. A hypervisor is a software or hardware that allows multiple VMs (Virtual Machines) to run on a single physical host or server. A hypervisor consists of various components, such as:

? The firmware: This is the software that controls the basic functions and operations of the hardware or device. The firmware can affect the performance, compatibility, and security of the hypervisor and the VMs. The firmware should be upgraded to ensure that it supports the latest features and functions of the hardware or device, as well as fix any bugs or vulnerabilities.

? The operating system: This is the software that manages the resources and activities of the hypervisor and the VMs. The operating system can affect the functionality, reliability, and efficiency of the hypervisor and the VMs. The operating system should be upgraded to ensure that it supports the latest applications and services of the hypervisor and the VMs, as well as improve stability and performance.

#### NEW QUESTION 110

- (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 115

- (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 120

- (Topic 2)

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

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

**Answer:** A

#### Explanation:

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

#### NEW QUESTION 122

- (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 126

- (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 128

- (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 132**

- (Topic 2)

Which of the following service models would be used for a database in the cloud?

- A. PaaS
- B. IaaS
- C. CaaS
- D. SaaS

**Answer:** A

**Explanation:**

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

**NEW QUESTION 133**

- (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 138**

- (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 143**

- (Topic 2)

A systems administrator is creating a VM and wants to ensure disk space is not allocated to the VM until it is needed. Which of the following techniques should the administrator use to ensure?

- A. Deduplication
- B. Thin provisioning
- C. Software-defined storage
- D. iSCSI storage

**Answer:** B

**Explanation:**

Thin provisioning is the technique that ensures disk space is not allocated to the VM until it is needed. Thin provisioning is a storage allocation method that assigns disk space to a VM on demand, rather than in advance. Thin provisioning can improve storage utilization and efficiency by avoiding overprovisioning and wasting disk space. Thin provisioning can also allow for more flexibility and scalability of storage resources.

**NEW QUESTION 146**

- (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 149**

- (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 151**

- (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 154**

- (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 159**

- (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 164

- (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 168

- (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 173

- (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 174

- (Topic 2)

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

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

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

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

**Answer: A**

**Explanation:**

To ensure the web servers in the public subnet allow only secure communications and remediate any possible issue, the analyst should remove rules 1, 2, and 5 from the stateful configuration. These rules are allowing insecure or unnecessary traffic to or from the web servers, which may pose security risks or performance issues. The rules are:

? Rule 1: This rule allows inbound traffic on port 80 (HTTP) from any source to any destination. HTTP is an unencrypted and insecure protocol that can expose web traffic to interception, modification, or spoofing. The analyst should remove this rule and use HTTPS (port 443) instead, which encrypts and secures web traffic.

? Rule 2: This rule allows outbound traffic on port 25 (SMTP) from any source to any destination. SMTP is a protocol that is used to send email messages. The web servers in the public subnet do not need to send email messages, as this is not their function. The analyst should remove this rule and block outbound SMTP traffic, which may prevent spamming or phishing attacks from compromised web servers.

? Rule 5: This rule allows inbound traffic on port 22 (SSH) from any source to any destination. SSH is a protocol that allows remote access and management of systems or devices using a command-line interface. The web servers in the public subnet do not need to allow SSH access from any source, as this may expose them to unauthorized or malicious access. The analyst should remove this rule and restrict SSH access to specific sources, such as the administrator's workstation or a bastion host.

**NEW QUESTION 177**

- (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 182**

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).

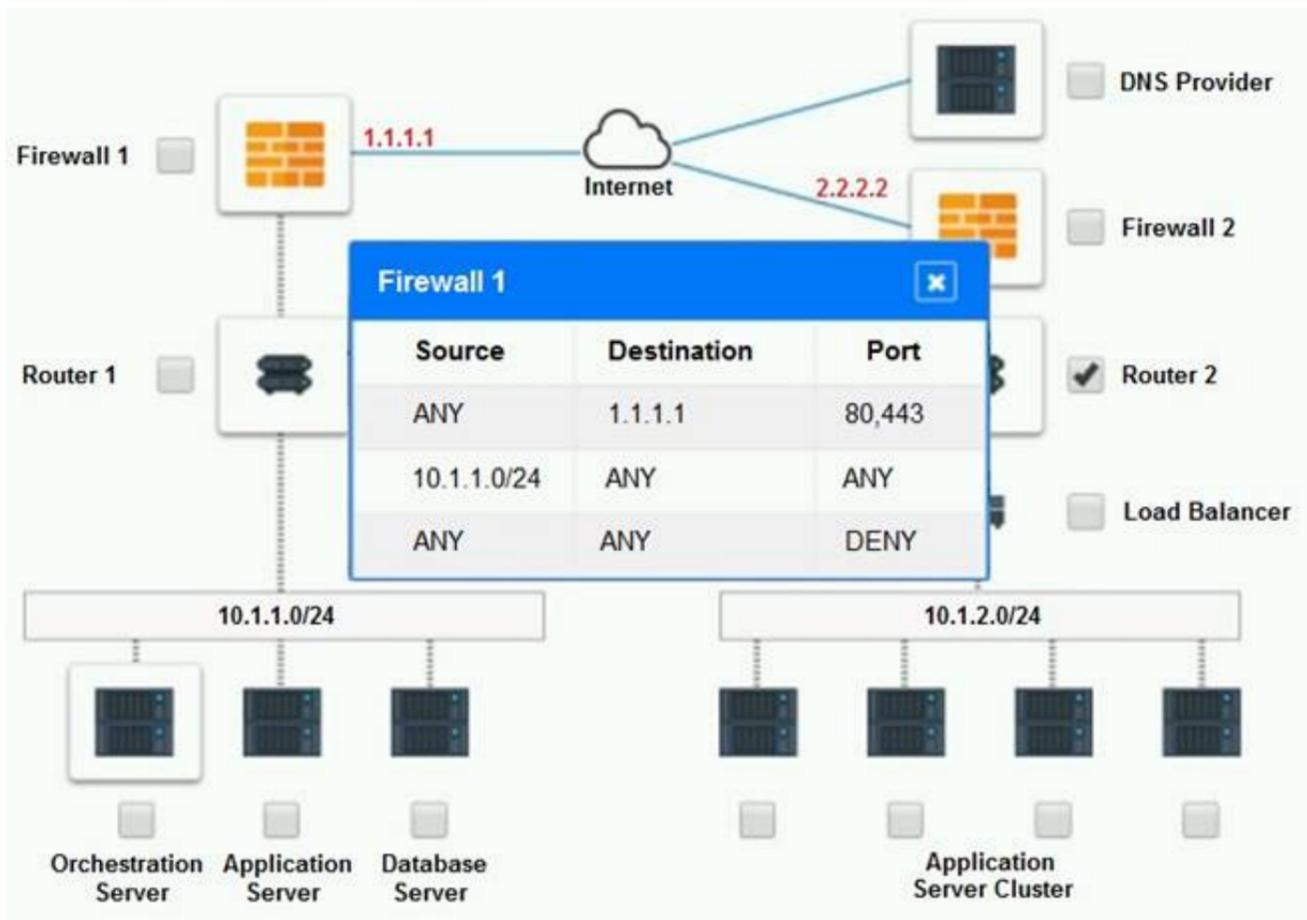
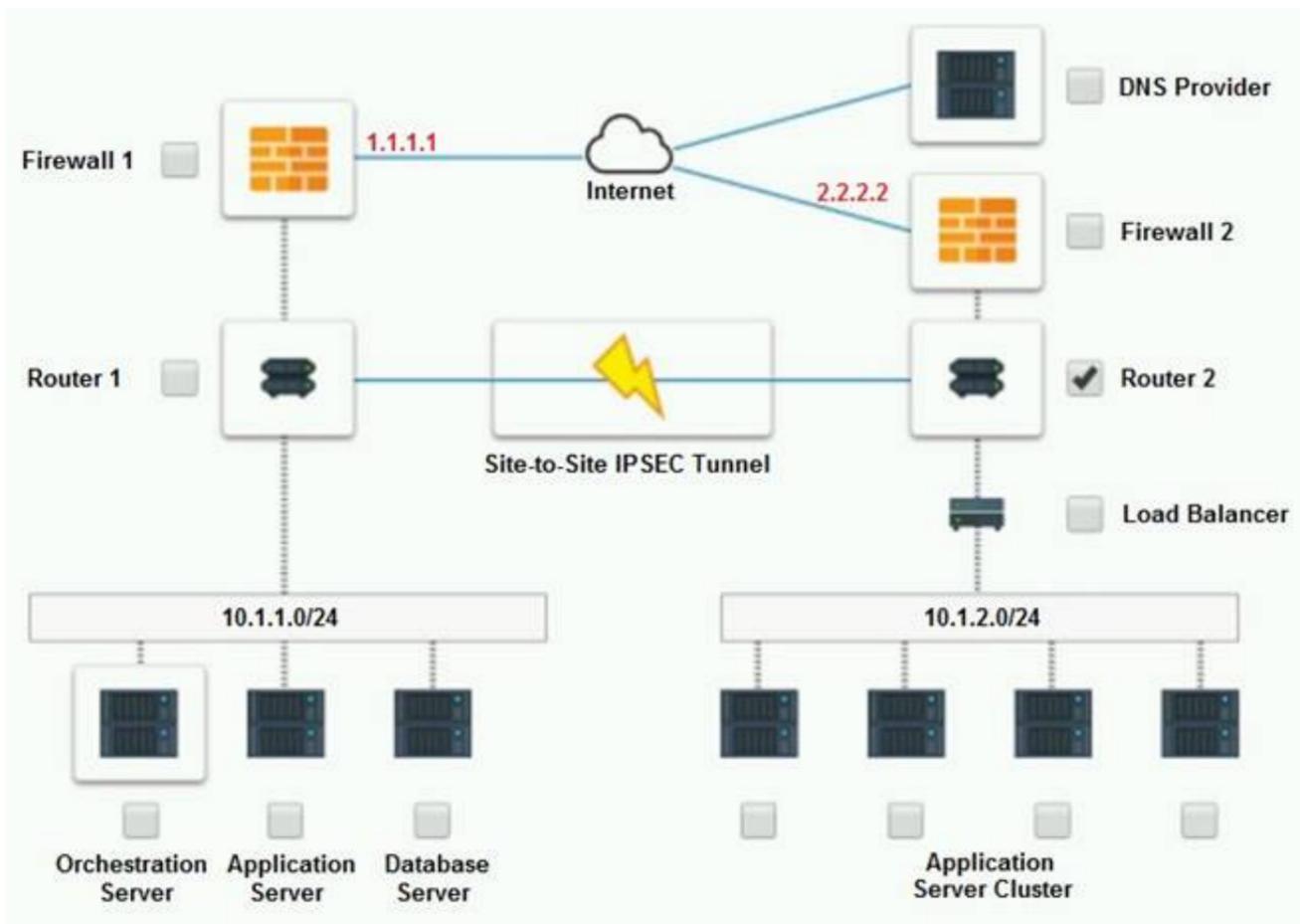
Part 2:

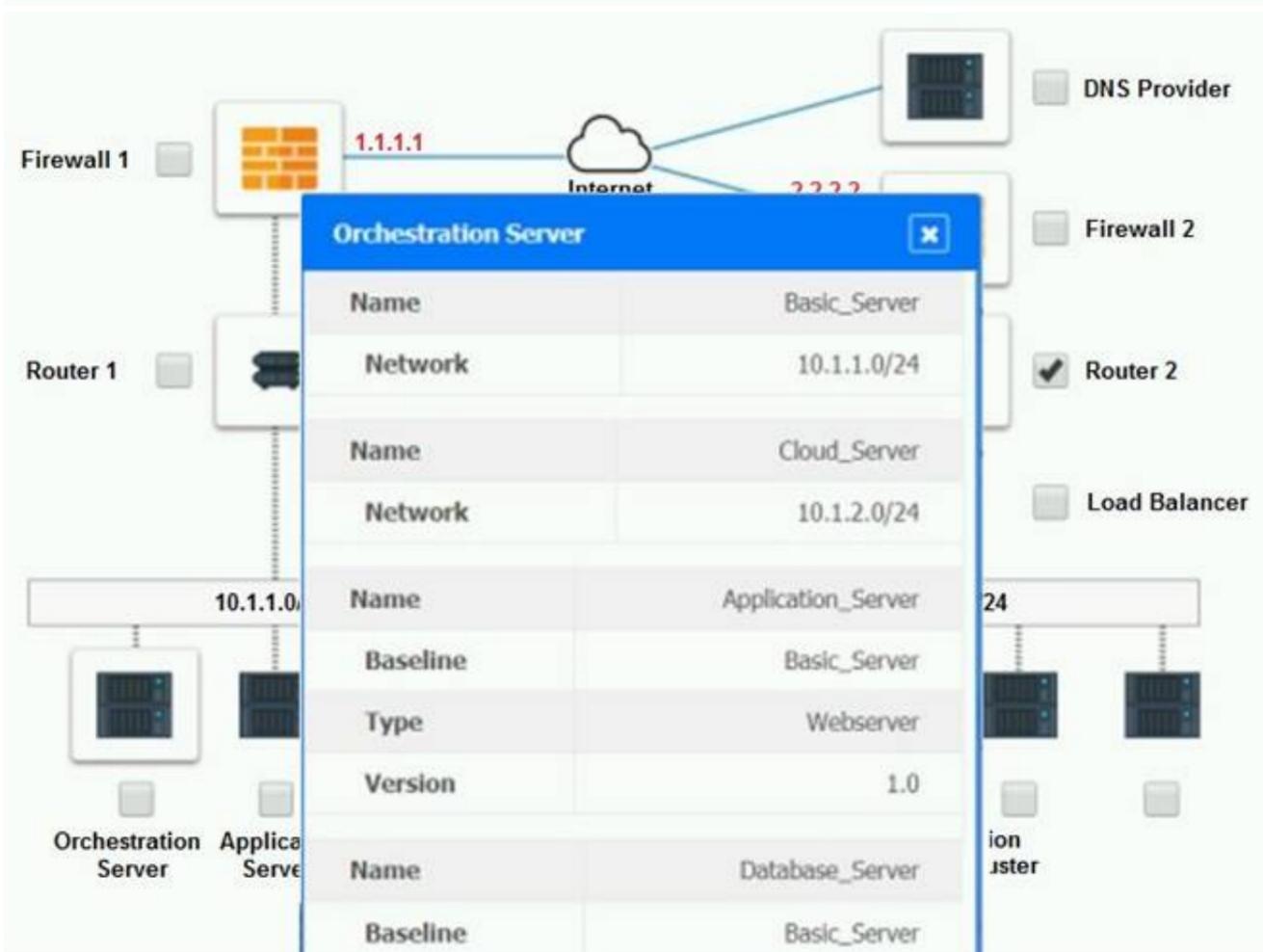
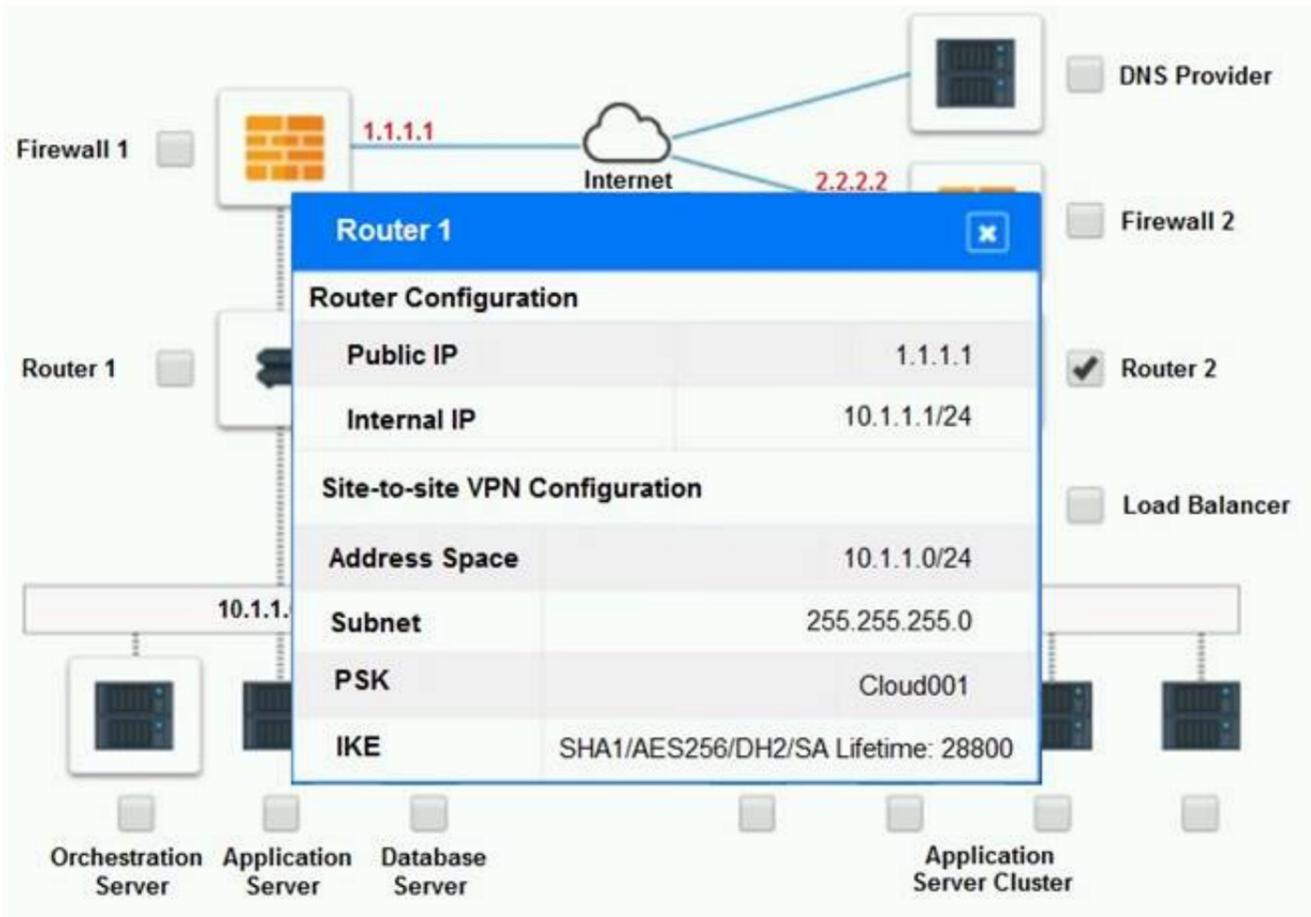
- \_ Identify the correct options to provide adequate configuration for hybrid cloud architecture.

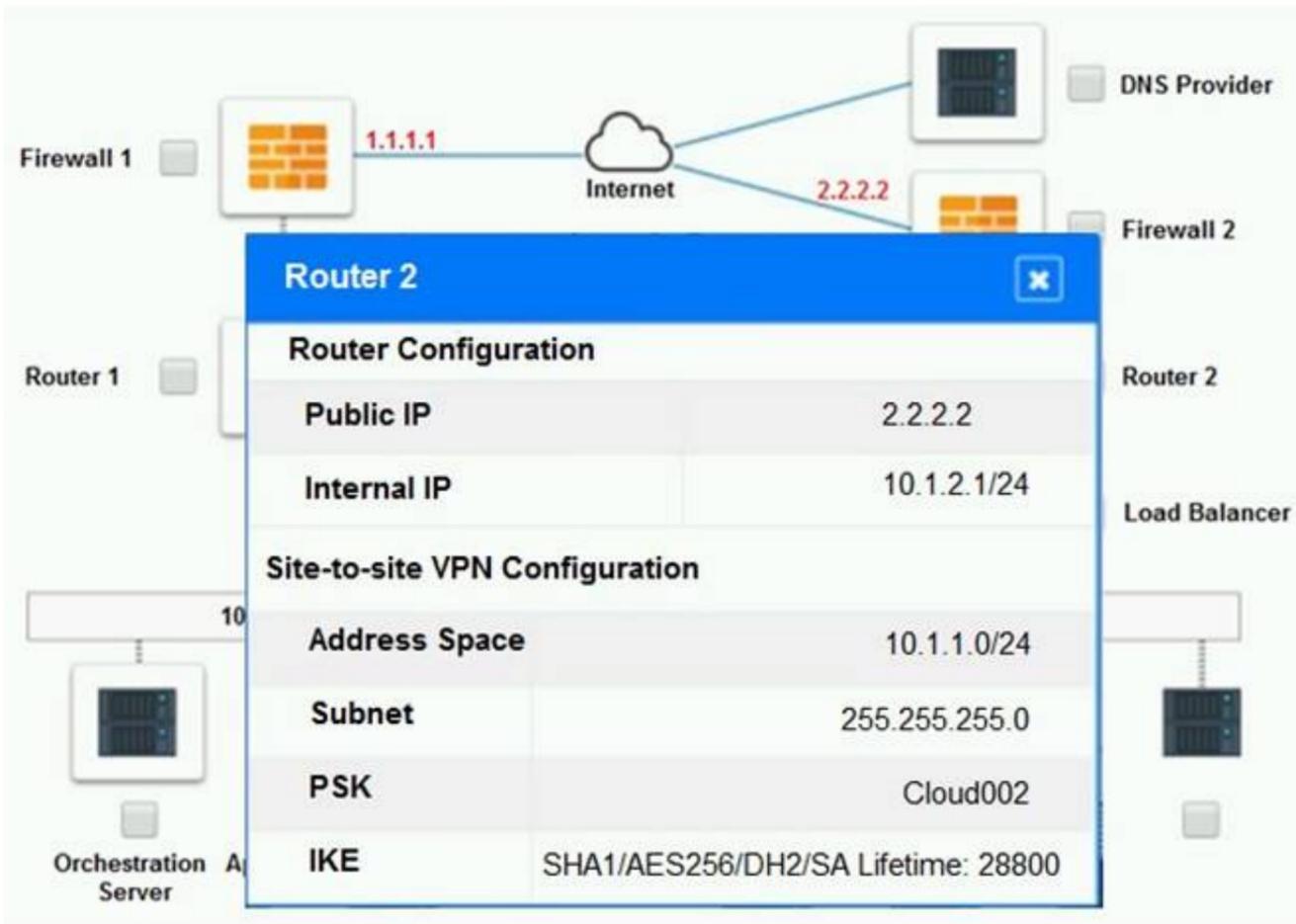
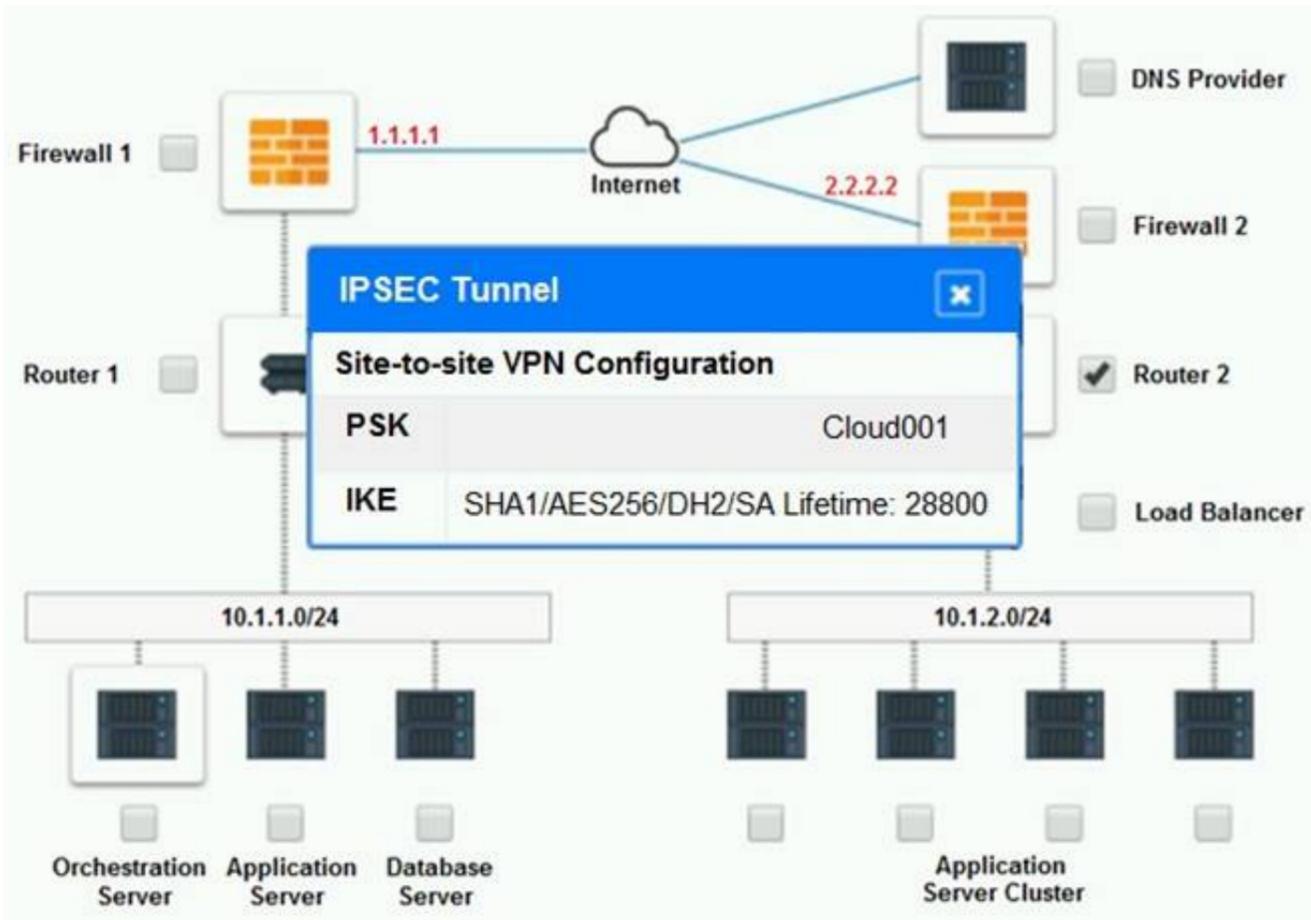
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

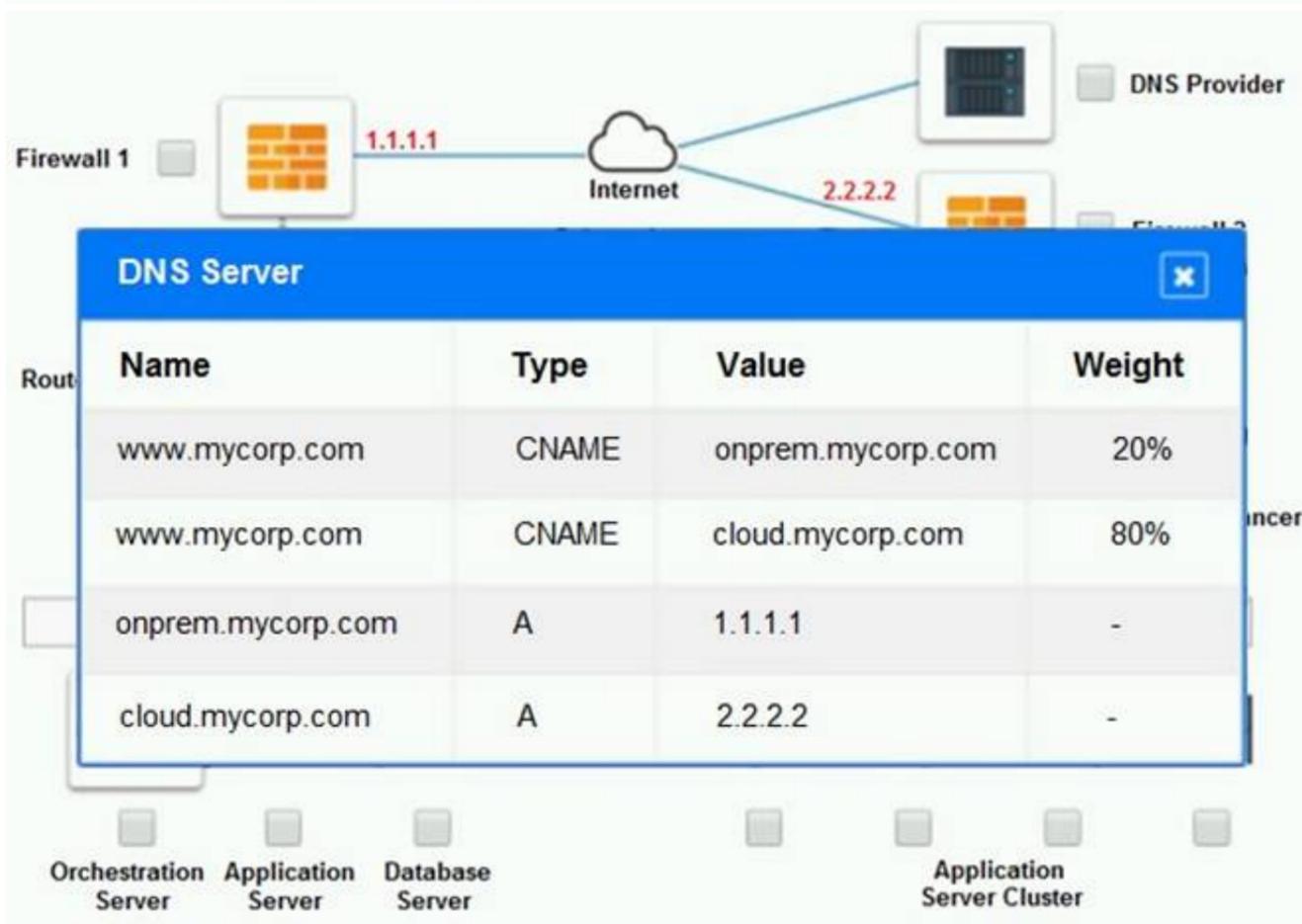
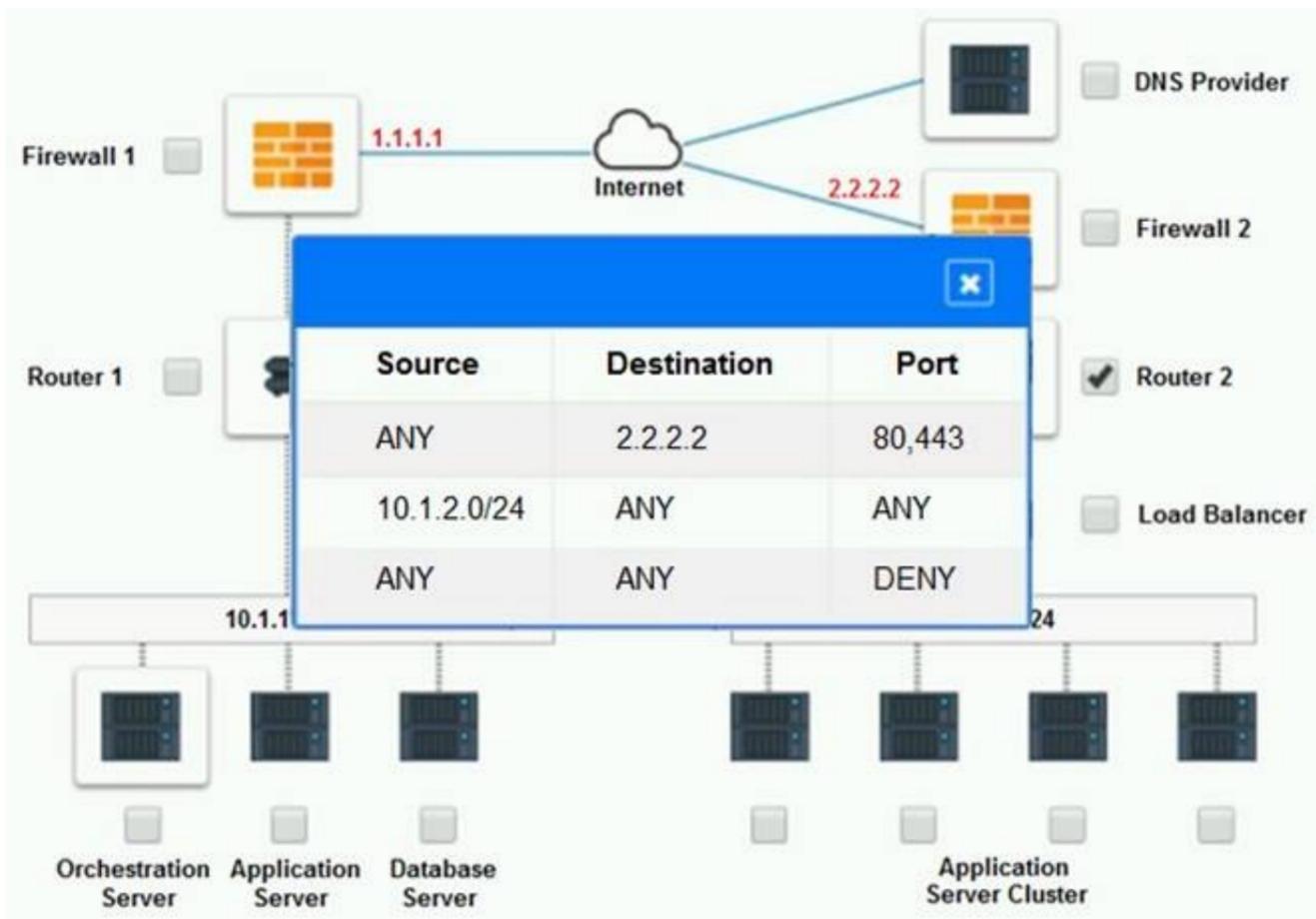
Part 1:

Cloud Hybrid Network Diagram









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 187**

- (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 191**

- (Topic 1)

An IaaS application has a two-hour RTO and a four-hour RPO. The application takes one hour to back up its data or restore from a local backup file. A systems administrator is tasked with configuring the backup policy.

Which of the following should the administrator configure to achieve the application requirements with the LEAST cost?

A. Back up to long-term storage every night

B. Back up to object storage every three hours

C. Back up to long-term storage every four hours

D. Back up to object storage every hour

**Answer:** B

**Explanation:**

Object storage is a type of storage service that stores data as objects with unique identifiers and metadata in a flat namespace or structure. Backing up to object storage every three hours can help achieve the application requirements with the least cost for an IaaS application that has a two-hour RTO and a four-hour RPO, as it can provide scalable, durable, and cost-effective storage for backup data while meeting the recovery time and point objectives. Backing up to object storage every three hours can ensure that the backup data is no more than four hours old and can be restored within two hours in case of a disaster or failure. References: CompTIA Cloud+ Certification Exam Objectives, page 9, section 1.4

**NEW QUESTION 194**

- (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 199**

- (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 201**

- (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](https://en.wikipedia.org/wiki/Central_processing_unit)

**NEW QUESTION 203**

- (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 204**

- (Topic 1)

A SaaS provider wants to maintain maximum availability for its service. Which of the following should be implemented to attain the maximum SLA?

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 205**

- (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 207**

- (Topic 1)

A systems administrator is using VMs to deploy a new solution that contains a number of application VMs.

Which of the following would provide high availability to the application environment in case of hypervisor failure?

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 211**

- (Topic 1)

A systems administrator for an e-commerce company will be migrating the company's main website to a cloud provider. The principal requirement is that the website must be highly available.

Which of the following will BEST address this requirement?

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 213**

- (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 216**

- (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 220**

- (Topic 1)

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

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 225**

- (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 228**

- (Topic 1)

An organization has multiple VLANs configured to segregate the network traffic. Following is the breakdown of the network segmentation:

- ? Production traffic (10.10.0.0/24)
- ? Network backup (10.20.0.0/25)
- ? Virtual IP network (10.20.0.128/25)

The following configuration exists on the server:

Server name	Interface	IP address	Gateway
COMPSRV01	Production	10.10.0.12/24	10.10.0.1
COMPSRV01	Network backup	10.20.0.12/25	10.10.0.1

The backup administrator observes that the weekly backup is failing for this server. Which of the following commands should the administrator run to identify the issue?

- A. ROUTE PRINT
- B. NETSTAT -A
- C. IPCONFIG /ALL
- D. NET SM

**Answer:** A

**Explanation:**

ROUTE PRINT is a command that displays the routing table of a system, which shows the destination network, the gateway, the interface, and the metric for each route. ROUTE PRINT can help identify the issue of the weekly backup failing for this server, as it can show if there is a valid route to the network backup segment (10.20.0.0/25) from the production traffic segment (10.10.0.0/24). If there is no route or an incorrect route, the backup will fail to reach the destination. The administrator can use ROUTE PRINT to verify and troubleshoot the routing configuration of the server. References: CompTIA Cloud+ Certification Exam Objectives, page 16, section 3.2

Reference: <https://www.toolbox.com/tech/operating-systems/blogs/using-the-route-print-command-in-windows-7-022310/>

**NEW QUESTION 231**

- (Topic 1)

A cloud administrator is planning to migrate a globally accessed application to the cloud.

Which of the following should the cloud administrator implement to BEST reduce latency for all users?

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 233**

- (Topic 4)

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

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 238**

- (Topic 4)

A cloud engineer is deploying a server in a cloud platform. The engineer reviews a security scan report. Which of the following recommended services should be disabled? (Select two).

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

**Answer:** AB

**Explanation:**

Telnet and FTP are recommended services to be disabled when deploying a server in a cloud platform, as they are insecure protocols that transmit data in plain text and expose credentials and sensitive information to potential attackers<sup>12</sup>. Remote log-in, DNS, DHCP, and LDAP are not necessarily recommended to be disabled, as they may provide useful functionality for the server and the cloud environment. However, they should be configured properly and secured with encryption, authentication, and authorization mechanisms<sup>34</sup>.

References: CompTIA Cloud+ CV0-003 Exam Objectives, Objective 4.2: Given a scenario, apply security configurations and compliance controls ; CompTIA Quick Start Guide to Tackling Cloud Security Concerns<sup>3</sup>

#### NEW QUESTION 243

- (Topic 4)

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

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

**Answer:** A

#### Explanation:

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

#### NEW QUESTION 244

- (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 needed<sup>12</sup>.

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 customers<sup>34</sup>.

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 environment<sup>5</sup>.

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 249

- (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 254

- (Topic 4)

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

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 255**

- (Topic 4)

An organization deployed an application using a cloud provider's internal managed certificates. Developers are unable to retrieve data when calling the API from any machine.

The following error message is in the log:

12-04-2023-10:05:25, SSL Negotiation Error 12-04-2023-10:05:28,Invalid Certificate

12-04-2023-10:05:29, TLS Handshake Failed 12-04-2023-10:05:30,Connection Closed

Which of the following is the most likely cause of the error?

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 257**

- (Topic 4)

A cloud administrator must ensure all servers are in compliance with the company's security policy Which of the following should the administrator check FIRST?

- A. The application version
- B. The OS version
- C. Hardened baselines
- D. Password policies

**Answer:** C

**Explanation:**

Hardened baselines are a set of security best practices that reduce the vulnerability of a system to exploits by reducing its attack surface<sup>1</sup>. They are also known as security configurations or benchmarks, and they provide a standard level of system hardening for an organization<sup>23</sup>.

Checking the hardened baselines of the servers is the first step that a cloud administrator should take to ensure compliance with the company's security policy.

This is because hardened baselines can help to:

Identify and eliminate common vulnerabilities and exposures (CVEs) that attackers can exploit<sup>1</sup>.

Remove unnecessary or unused services, accounts, software, and ports that can increase the attack surface<sup>23</sup>.

Apply appropriate settings and controls for encryption, authentication, authorization, firewall, and logging<sup>23</sup>.

Streamline audits and testing by reducing complexity and providing a reliable benchmark<sup>23</sup>.

**NEW QUESTION 259**

- (Topic 4)

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

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

**Answer:** A

**Explanation:**

GPU passthrough is a technique that allows a virtual machine to access and use the physical GPU of the host machine directly. This can improve the performance and quality of graphics-intensive applications, such as rendering, gaming, or video editing, that run on the virtual machine<sup>123</sup>.

GPU passthrough can help resolve the issue of the rendering application running slowly and taking a long time to refresh the screen on the virtual desktops. By enabling GPU passthrough, the virtualization administrator can allow the rendering application to leverage the full power and features of the host GPU, rather than relying on the limited and shared resources of a virtual GPU. This can result in faster rendering, smoother animations, and higher resolution<sup>12</sup>

**NEW QUESTION 260**

- (Topic 4)

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

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

**Answer: B**

**Explanation:**

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

References: [CompTIA Cloud+ Study Guide], page 236.

**NEW QUESTION 261**

- (Topic 4)

The Chief Information Officer of a financial services company wants to ensure stringent security measures are maintained while migrating customer financial information from a private cloud to the public cloud. The cloud engineer must deploy automated validation and verification checks to prevent unauthorized disclosure of financial information. Which of the following should be configured during the migration?

- A. ACL
- B. VPN
- C. P2V
- D. VDI

**Answer: B**

**Explanation:**

One possible answer is: B. VPN

A VPN (Virtual Private Network) is a technology that creates a secure and encrypted connection between a remote device and a private network over the internet. A VPN can help prevent unauthorized disclosure of financial information during the migration from a private cloud to the public cloud, as it can protect the data in transit from interception, tampering, or leakage. A VPN can also help maintain compliance with data privacy regulations, such as GDPR or PCI DSS, by ensuring that the data is only accessible by authorized parties<sup>12</sup>.

ACL (Access Control List) is a method of controlling access to resources based on user or group permissions. ACL can help enforce security policies and restrict access to sensitive data, but it does not encrypt or protect the data in transit<sup>3</sup>.

P2V (Physical to Virtual) is a process of converting a physical machine into a virtual machine. P2V can help migrate workloads from on-premises servers to cloud servers, but it does not ensure the security of the data during the migration<sup>4</sup>.

VDI (Virtual Desktop Infrastructure) is a technology that provides users with virtual desktops hosted on a centralized server. VDI can help improve the performance, availability, and manageability of desktop environments, but it does not address the security of the data during the migration<sup>5</sup>.

**NEW QUESTION 264**

- (Topic 4)

A systems administrator is attempting to gather information about services and resource utilization on VMS in a cloud environment. Which of the following will BEST accomplish this objective?

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

**Answer: E**

**Explanation:**

Performance monitoring is the process of collecting and analyzing metrics related to the performance and availability of resources in a cloud environment<sup>1</sup>.

Performance monitoring can help a systems administrator to gather information about services and resource utilization on VMs in a cloud environment by providing the following benefits<sup>2</sup>:

? Identify and troubleshoot performance issues and bottlenecks before they affect the end users or business operations.

? Optimize the resource allocation and configuration to meet the performance requirements and SLAs of the services.

? Plan for future capacity and scalability needs based on the historical trends and patterns of resource utilization.

? Compare the performance and costs of different cloud service providers, regions, and SKUs.

Some of the tools and services that can help with performance monitoring in a cloud environment are<sup>3</sup>:

? Azure Monitor: A comprehensive service that provides a unified view of the health, performance, and availability of your Azure resources, applications, and services. Azure Monitor collects metrics, logs, and traces from various sources and provides analysis, visualization, alerting, and automation capabilities.

? Azure Advisor: A personalized service that provides recommendations to optimize your Azure resources for performance, security, cost, reliability, and operational excellence. Azure Advisor analyzes your resource configuration and usage data and suggests best practices to improve your cloud environment.

? Azure Application Insights: A service that monitors the performance and usage of your web applications and services. Application Insights collects telemetry data such as requests, dependencies, exceptions, page views, custom events, and metrics from your application code and provides powerful analytics, diagnostics, and alerting features.

? Azure Log Analytics: A service that collects and analyzes data from various sources such as Azure Monitor, Azure services, VMs, containers, applications, and other cloud or on-premises systems. Log Analytics enables you to query, visualize, and correlate log data using the Kusto Query Language (KQL) and create custom dashboards and reports.

Syslog is a standard protocol for sending log messages from network devices to a central server. Syslog can help with logging and auditing activities in a cloud environment, but it does not provide performance monitoring capabilities. Therefore, option A is incorrect. SNMP (Simple Network Management Protocol) is a

protocol for collecting and organizing information about managed devices on a network. SNMP can help with network management and monitoring in a cloud environment, but it does not provide comprehensive performance monitoring for VMs and services. Therefore, option B is incorrect.

CMDB (Configuration Management Database) is a database that stores information about the configuration items (CIs) in an IT environment. CMDB can help with configuration management and change management in a cloud environment, but it does not provide performance monitoring capabilities. Therefore, option C is incorrect.

Service management is a set of processes and practices that aim to deliver value to customers by providing quality services that meet their needs and expectations. Service management can help with service design, delivery, support, and improvement in a cloud environment, but it does not provide performance monitoring capabilities. Therefore, option D is incorrect.

#### NEW QUESTION 265

- (Topic 4)

A cloud administrator needs to deploy a security virtual appliance in a private cloud environment, but this appliance will not be part of the standard catalog of items for other users to request. Which of the following is the BEST way to accomplish this task?

- A. Create an empty V
- B. import the hard disk of the virtual applianc
- C. and configure the CPU and memory.
- D. Acquire the build scripts from the vendor and recreate the appliance using the baseline templates
- E. Import the virtual appliance into the environment and deploy it as a VM
- F. Convert the virtual appliance to a template and deploy a new VM using the template.

**Answer:** C

#### Explanation:

The correct answer is C. Import the virtual appliance into the environment and deploy it as a VM.

A virtual appliance is a pre-packaged and pre-configured software solution that runs on a virtual machine (VM). A virtual appliance typically consists of an operating system, an application, and any required dependencies, and is designed to provide a specific function or service. A virtual appliance can be distributed as a single file or a set of files that can be imported into a virtualization platform, such as VMware, Hyper-V, or KVM .

A cloud administrator can deploy a security virtual appliance in a private cloud environment by importing the virtual appliance into the environment and deploying it as a VM. This is the best way to accomplish this task because it preserves the original configuration and functionality of the virtual appliance, and does not require any additional installation or customization. The cloud administrator can also control the access and visibility of the virtual appliance, and prevent other users from requesting it from the standard catalog of items .

Creating an empty VM, importing the hard disk of the virtual appliance, and configuring the CPU and memory is not the best way to accomplish this task because it involves more steps and complexity than importing the virtual appliance as a whole. It also introduces the risk of losing or corrupting some data or settings during the import process, or misconfiguring the CPU and memory for the virtual appliance.

Acquiring the build scripts from the vendor and recreating the appliance using the baseline templates is not the best way to accomplish this task because it involves more time and effort than importing the virtual appliance directly. It also depends on whether the vendor provides the build scripts or not, and whether they are compatible with the baseline templates or not.

Converting the virtual appliance to a template and deploying a new VM using the template is not the best way to accomplish this task because it adds an unnecessary step of creating a template from the virtual appliance. It also does not prevent other users from accessing or requesting the template from the catalog of items.

#### NEW QUESTION 269

.....

## THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual CV0-003 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the CV0-003 Product From:

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

### Money Back Guarantee

#### **CV0-003 Practice Exam Features:**

- \* CV0-003 Questions and Answers Updated Frequently
- \* CV0-003 Practice Questions Verified by Expert Senior Certified Staff
- \* CV0-003 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- \* CV0-003 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year