

# 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 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 3

- (Topic 1)

A DevOps administrator is automating an existing software development workflow. The administrator wants to ensure that prior to any new code going into production, tests confirm the new code does not negatively impact existing automation activities.

Which of the following testing techniques would be BEST to use?

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

**Answer:** B

#### Explanation:

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

Reference: <https://www.softwaretestinghelp.com/regression-testing-tools-and-methods/>

### NEW QUESTION 4

- (Topic 1)

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 5

- (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 6

- (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 7

- (Topic 1)

A company has decided to get multiple compliance and security certifications for its public cloud environment. However, the company has few staff members to handle the extra workload, and it has limited knowledge of the current infrastructure.

Which of the following will help the company meet the compliance requirements as quickly as possible?

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

**Answer: B**

#### Explanation:

A cloud access security broker (CASB) is a type of security solution that acts as a gateway between cloud service users and cloud service providers. A CASB can help a company get multiple compliance and security certifications for its public cloud environment, as it can provide visibility, control, and protection for cloud data and applications. A CASB can also help the company handle the extra workload and overcome the limited knowledge of the current infrastructure, as it can automate and simplify the enforcement of security policies and compliance requirements across multiple cloud services. References: CompTIA Cloud+ Certification Exam Objectives, page 14, section 2.7

#### NEW QUESTION 8

- (Topic 1)

A systems administrator needs to convert ten physical servers to virtual.

Which of the following would be the MOST efficient conversion method for the administrator to use?

- A. Rebuild the servers from scratch
- B. Use the vendor's conversion tool
- C. Clone the hard drive
- D. Restore from backup

**Answer: B**

#### Explanation:

A vendor's conversion tool is a type of software or utility that automates and simplifies the process of converting physical servers to virtual machines by capturing the configuration and data of the physical servers and creating virtual disks and files for the virtual machines. Using the vendor's conversion tool can be the most efficient conversion method for a systems administrator to use to convert ten physical servers to virtual, as it can save time and effort by avoiding manual steps or errors involved in rebuilding, cloning, or restoring the physical servers to virtual machines. Using the vendor's conversion tool can also ensure compatibility and consistency, as it can match the hardware and software requirements and settings of the physical servers to the virtual machines.

References: CompTIA Cloud+ Certification Exam Objectives, page 10, section 1.5

#### NEW QUESTION 9

- (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 10

- (Topic 1)

A cloud administrator recently deployed an update to the network drivers of several servers. Following the update, one of the servers no longer responds to remote login requests. The cloud administrator investigates the issue and gathers the following information:

? The cloud management console shows the VM is running and the CPU and memory utilization is at or near 0%.

? The cloud management console does not show an IP address for that server.

? A DNS lookup shows the hostname resolves to an IP address.

? The server is a member of the same security group as the others.

? The cloud administrator is able to log in remotely to the other servers without issue.

Which of the following is the MOST likely cause of the server being unavailable?

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

**Answer: A**

#### NEW QUESTION 10

- (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 11

- (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 14

- (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 15

- (Topic 1)

A company that utilizes an IaaS service provider has contracted with a vendor to perform a penetration test on its environment. The vendor is able to exploit the virtualization layer and obtain access to other instances within the cloud provider's environment that do not belong to the company.

Which of the following BEST describes this attack?

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

**Answer:** A

#### Explanation:

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

#### NEW QUESTION 19

- (Topic 1)

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

- A. Disk I/O limits
- B. Affinity rule
- C. CPU oversubscription
- D. RAM usage
- E. Insufficient GPU resources
- F. License issues

**Answer:** AC

#### Explanation:

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

#### NEW QUESTION 24

- (Topic 1)

In an existing IaaS instance, it is required to deploy a single application that has different versions.

Which of the following should be recommended to meet this requirement?

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

**Answer:** A

#### Explanation:

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

#### NEW QUESTION 26

- (Topic 1)

A company needs to rehost its ERP system to complete a datacenter migration to the public cloud. The company has already migrated other systems and configured VPN connections.

Which of the following MOST likely needs to be analyzed before rehosting the ERP?

- A. Software
- B. Licensing
- C. Right-sizing
- D. The network

**Answer: D**

#### Explanation:

The network is the set of devices, connections, protocols, and configurations that enable communication and data transfer between different systems and applications. The network can affect the rehosting of an ERP system to complete a datacenter migration to the public cloud, as it can influence factors such as bandwidth, latency, availability, security, and compatibility. The network needs to be analyzed before rehosting the ERP system to ensure that the network requirements and specifications are met, the network performance and reliability are maintained or improved, and the network security and integrity are preserved or enhanced. References: CompTIA Cloud+ Certification Exam Objectives, page 18, section 3.5

#### NEW QUESTION 28

- (Topic 1)

An IaaS provider has numerous devices and services that are commissioned and decommissioned automatically on an ongoing basis. The cloud administrator needs to implement a solution that will help reduce administrative overhead.

Which of the following will accomplish this task?

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

**Answer: A**

#### Explanation:

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

Reference: <https://www.infoblox.com/glossary/ipam-ip-address-management/>

#### NEW QUESTION 33

- (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 38

- (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 41**

- (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 43**

- (Topic 2)

Which of the following should be considered for capacity planning?

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

**Answer:** A

**Explanation:**

These are the factors that should be considered for capacity planning in a cloud environment. Capacity planning is a process of estimating and allocating the necessary resources and performance to meet the current and future demands of cloud applications or services. Capacity planning can help to optimize costs, efficiency, and reliability of cloud resources or services. The factors that should be considered for capacity planning are:

- ? Requirements: These are the specifications or expectations of the cloud applications or services, such as functionality, availability, scalability, security, etc. Requirements can help to determine the type, amount, and quality of resources or services needed to meet the objectives and goals of the cloud applications or services.
- ? Licensing: This is the agreement or contract that grants customers the right to use or access certain cloud resources or services for a specific period or fee. Licensing can affect the cost, availability, and compliance of cloud resources or services. Licensing can help to determine the budget, duration, and scope of using or accessing cloud resources or services.
- ? Trend analysis: This is the technique of analyzing historical and current data to identify patterns, changes, or fluctuations in demand or usage of cloud resources or services. Trend analysis can help to predict and anticipate future demand or usage of cloud resources or services, as well as identify any opportunities or challenges that may arise.

**NEW QUESTION 44**

- (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 45

- (Topic 2)

A company is concerned about the security of its data repository that contains customer PII. A systems administrator is asked to deploy a security control that will prevent the exfiltration of such data. Which of the following should the systems administrator implement?

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

**Answer:** A

#### Explanation:

Reference: <https://cloud.google.com/blog/products/identity-security/4-steps-to-stop-data-exfiltration-with-google-cloud>

Implementing DLP (Data Loss Prevention) is the best solution to prevent the exfiltration of customer PII (Personally Identifiable Information) from a data repository. DLP is a security control that monitors, detects, and blocks sensitive data from leaving or being accessed by unauthorized parties. DLP can be applied at different levels, such as network, endpoint, storage, or cloud. DLP can help to protect customer PII from being leaked, stolen, or compromised.

#### NEW QUESTION 50

- (Topic 2)

Which of the following definitions of serverless computing BEST explains how it is different from using VMs?

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

**Answer:** D

#### Explanation:

This is the best definition of serverless computing that explains how it is different from using VMs (Virtual Machines). Serverless computing is a cloud service model that provides customers with a platform to run applications or functions without having to manage or provision any underlying infrastructure or resources, such as servers, storage, network, OS, etc. Serverless computing is different from using VMs in the following ways:

? Serverless computing allows developers to focus on writing code and organizations to focus on business, rather than spending time and effort on managing or scaling VMs or other infrastructure components.

? Serverless computing is event-driven and pay-per-use, which means that applications or functions are executed only when triggered by a specific event or request, and customers are charged only for the resources consumed during the execution time.

? Serverless computing is more scalable and flexible than using VMs, as it can automatically adjust the capacity and performance of applications or functions according to demand or workload, without requiring any manual intervention or configuration.

#### NEW QUESTION 55

- (Topic 2)

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

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

**Answer:** A

#### Explanation:

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

#### NEW QUESTION 60

- (Topic 2)

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

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

**Answer:** D

#### Explanation:



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

#### NEW QUESTION 64

- (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 67

- (Topic 2)

A company is planning to migrate applications to a public cloud, and the Chief Information Officer (CIO) would like to know the cost per business unit for the applications in the cloud. Before the migration, which of the following should the administrator implement FIRST to assist with reporting the cost for each business unit?

- A. An SLA report
- B. Tagging
- C. Quotas
- D. Showback

**Answer:** B

#### Explanation:

Tagging is what the administrator should implement first to assist with reporting the cost for each business unit for applications in a public cloud environment. Tagging is a technique that allows customers to assign metadata or labels to their cloud resources, such as applications, instances, volumes, etc., based on their attributes or criteria. Tagging can help customers to organize, manage, monitor, and report their cloud resources and costs by business unit, project, owner, environment, etc.

#### NEW QUESTION 68

- (Topic 2)

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

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

**Answer:** A

#### Explanation:

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

#### NEW QUESTION 69

- (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 74

- (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 78

- (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 82

- (Topic 2)

A systems administrator is troubleshooting performance issues with a VDI environment. The administrator determines the issue is GPU related and then increases the frame buffer on the virtual machines. Testing confirms the issue is solved, and everything is now working correctly. Which of the following should the administrator do NEXT?

- A. Consult corporate policies to ensure the fix is allowed
- B. Conduct internal and external research based on the symptoms
- C. Document the solution and place it in a shared knowledge base
- D. Establish a plan of action to resolve the issue

**Answer:** C

#### Explanation:

Documenting the solution and placing it in a shared knowledge base is what the administrator should do next after troubleshooting performance issues with a VDI (Virtual Desktop Infrastructure) environment, determining that the issue is GPU (Graphics Processing Unit) related, increasing the frame buffer on the virtual machines, and testing that confirms that the issue is solved and everything is now working correctly. Documenting the solution is a process of recording and describing what was done to fix or resolve an issue, such as actions, steps, methods, etc., as well as why and how it worked. Placing it in a shared knowledge base is a process of storing and organizing documented solutions in a central location or repository that can be accessed and used by others. Documenting the solution and placing it in a shared knowledge base can provide benefits such as:

? Learning: Documenting the solution and placing it in a shared knowledge base can help to learn from past experiences and improve skills and knowledge.

? Sharing: Documenting the solution and placing it in a shared knowledge base can help to share information and insights with others who may face similar issues or situations.

? Reusing: Documenting the solution and placing it in a shared knowledge base can help to reuse existing solutions for future issues or situations.

#### NEW QUESTION 84

- (Topic 2)

A systems administrator is trying to establish an RDP session from a desktop to a server in the cloud. However, the connection appears to be refused even though the VM is responding to ICMP echo requests. Which of the following should the administrator check FIRST?

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

**Answer:** A

#### Explanation:

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

#### NEW QUESTION 85

- (Topic 2)

A systems administrator is deploying a solution that includes multiple network I/O-intensive VMs. The solution design requires that vNICs of the VMs provide low-latency, near-native performance of a physical NIC and data protection between the VMs. Which of the following would BEST satisfy these requirements?

- A. SR-IOV
- B. GENEVE
- C. SDN
- D. VLAN

**Answer:** A

#### Explanation:

SR-IOV (Single Root Input/Output Virtualization) is what would best satisfy the requirements of low-latency, near-native performance of a physical NIC and data protection between VMs for multiple network I/O-intensive VMs. SR-IOV is a technology that allows a physical NIC to be partitioned into multiple virtual NICs that can be assigned to different VMs. SR-IOV can provide the following benefits:

? Low-latency: SR-IOV can reduce latency by bypassing the hypervisor and allowing direct communication between the VMs and the physical NIC, without any overhead or interference.

? Near-native performance: SR-IOV can provide near-native performance by allowing the VMs to use the full capacity and functionality of the physical NIC, without any emulation or translation.

? Data protection: SR-IOV can provide data protection by isolating and securing the network traffic between the VMs and the physical NIC, without any exposure or leakage.

#### NEW QUESTION 88

- (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 91

- (Topic 2)

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

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

**Answer:** D

#### Explanation:

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

#### NEW QUESTION 95

- (Topic 2)

A company needs to migrate the storage system and batch jobs from the local storage system to a public cloud provider. Which of the following accounts will MOST likely be created to run the batch processes?

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

**Answer:** D

#### Explanation:

A service account is what will most likely be created to run the batch processes that migrate the storage system and batch jobs from the local storage system to a public cloud provider. A service account is a special type of account that is used to perform automated tasks or operations on a system or service, such as running scripts, applications, or processes. A service account can provide benefits such as:

? Security: A service account can have limited or specific permissions and roles that are required to perform the tasks or operations, which can prevent unauthorized or malicious access or actions.

? Efficiency: A service account can run the tasks or operations without any human intervention or interaction, which can save time and effort.

? Reliability: A service account can run the tasks or operations consistently and accurately, which can reduce errors or failures.

#### NEW QUESTION 96

- (Topic 2)

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

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

**Answer: C**

#### Explanation:

User quotas are what will help control the amount of space that is being used by a file server in the cloud that has a limited amount of disk space due to financial considerations. User quotas are the limits or restrictions that are imposed on the amount of space that each user can use or consume on a file server or storage device. User quotas can help to control the amount of space that is being used by:

? Preventing or reducing wastage or overuse of space by users who may store unnecessary or redundant files or data on the file server or storage device.

? Ensuring fair and equal distribution or allocation of space among users who may have different needs or demands for space on the file server or storage device.

? Monitoring and managing the usage or consumption of space by users who may need to be notified or alerted when they reach or exceed their quota on the file server or storage device.

#### NEW QUESTION 101

- (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 106

- (Topic 2)

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

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

**Answer: A**

#### Explanation:

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

#### NEW QUESTION 109

- (Topic 2)

A company recently experienced a power outage that lasted 30 minutes. During this time, a whole rack of servers was inaccessible, even though the servers did not lose power.

Which of the following should be investigated FIRST?

- A. Server power
- B. Rack power
- C. Switch power
- D. SAN power

**Answer: C**



**Explanation:**

If a whole rack of servers was inaccessible during a power outage, even though the servers did not lose power, it is likely that the switch that connects them to the network lost power. Without network connectivity, the servers would not be able to communicate with other devices or services. The administrator should investigate the switch power source and ensure it has a backup power supply or UPS.

**NEW QUESTION 113**

- (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 114**

- (Topic 2)

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

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 119**

- (Topic 2)

Which of the following will provide a systems administrator with the MOST information about potential attacks on a cloud IaaS instance?

- A. Network flows
- B. FIM
- C. Software firewall
- D. HIDS

**Answer:** D

**Explanation:**

HIDS (Host-based Intrusion Detection System) is the tool that will provide the administrator with the most information about potential attacks on a cloud IaaS instance. HIDS is a software or agent that monitors and analyzes the activities and events on a host system or device, such as a cloud instance. HIDS can detect and alert on any malicious or anomalous behavior, such as unauthorized access, malware infection, configuration changes, etc., that may indicate an attack or compromise.

**NEW QUESTION 120**

- (Topic 2)

Which of the following actions should a systems administrator perform during the containment phase of a security incident in the cloud?

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

**Answer:** B

**Explanation:**

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

### NEW QUESTION 123

- (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 125

- (Topic 1)

A cloud engineer is responsible for managing two cloud environments from different MSPs. The security department would like to inspect all traffic from the two cloud environments.

Which of the following network topology solutions should the cloud engineer implement to reduce long-term maintenance?

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

**Answer: D**

#### Explanation:

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

### NEW QUESTION 129

- (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 130

- (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 135

- (Topic 1)

A cloud administrator needs to implement a mechanism to monitor the expense of the company's cloud resources. Which of the following is the BEST option to execute this task with minimal effort?

- A. Ask the cloud provider to send a daily expense report
- B. Set custom notifications for exceeding budget thresholds
- C. Use the API to collect expense information from cloud resources
- D. Implement a financial tool to monitor cloud resource expenses

**Answer: B**

#### Explanation:

Setting custom notifications for exceeding budget thresholds is the best option to execute the task of monitoring the expense of the company's cloud resources with minimal effort, as it can automate and simplify the process of tracking and alerting the cloud administrator about any overspending or wastage of cloud resources. Setting custom notifications can also help optimize the cost and performance of cloud resources, as it can enable timely and proactive actions to adjust or optimize the resource allocation or consumption based on the budget limits. References: CompTIA Cloud+ Certification Exam Objectives, page 13, section 2.5

#### NEW QUESTION 136

- (Topic 1)

A systems administrator in a large enterprise needs to alter the configuration of one of the finance department's database servers. Which of the following should the administrator perform FIRST?

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

**Answer: B**

#### Explanation:

The SA would do the other three regardless of the need to alter configurations. In this situation, the SA would have to present the change to the CCB in order to do the alteration.

There is no clarification on whether the change management process has been gone through. Any changes, regardless of how small or big, must go through the change management process. This allows proposals to be heard by end-users, management, and possibly stockholders. From there, it will be reviewed and either approved or denied, with reasons specified. From there, the administrator(s) can do whatever processes are necessary.

Change management is a process or procedure that defines the steps, roles, and responsibilities for implementing, documenting, and communicating any changes or updates to a system or service. Change management can help ensure that any changes or updates are done in a controlled and consistent manner, minimizing any risks or impacts to the system or service. Performing change management is the first thing that a systems administrator should do before altering the configuration of one of the finance department's database servers, as it can ensure that the change request is approved, authorized, tested, and verified before applying it to the database server. References: CompTIA Cloud+ Certification Exam Objectives, page 13, section 2.5

#### NEW QUESTION 139

- (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 141

- (Topic 1)

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

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

**Answer: C**

**Explanation:**

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

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

**NEW QUESTION 143**

- (Topic 1)

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

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

**Answer:** BD

**Explanation:**

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

**NEW QUESTION 144**

- (Topic 4)

A security analyst is investigating a recurring alert. The alert is reporting an insecure firewall configuration state after every cloud application deployment. The process of identifying the issue, requesting a fix, and waiting for the developers to manually patch the environment is being repeated multiple times. In an effort to identify the root issue, the following logs were collected:

Deploying template app prod. •yaml Instance DB successfully created DB keys successfully stored on vault

Instance WebApp successfully created Access rules successfully applied Access—keys successfully created

Which of the following options will provide a permanent fix for the issue?

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

**Answer:** A

**Explanation:**

The issue of an insecure firewall configuration state after every cloud application deployment is likely caused by a flaw in the IaC code used during the deployment. IaC stands for Infrastructure as Code, which is a method of managing and provisioning IT infrastructure using code, rather than manual configuration<sup>1</sup>. IaC allows teams to automate the setup and management of their infrastructure, making it more efficient and consistent. However, if the IaC code contains errors, vulnerabilities, or misconfigurations, it can result in security issues or compliance violations in the deployed infrastructure<sup>2</sup>. Therefore, to provide a permanent fix for the issue, the IaC code used during the deployment should be validated and tested to ensure that it meets the security requirements and best practices for firewall configuration. The IaC code can be validated using tools such as Azure Resource Manager Template Toolkit, AWS CloudFormation Linter, or Terraform Validate. These tools can check the syntax and semantics of the IaC code, and identify any potential errors or inconsistencies before deployment

**NEW QUESTION 145**

- (Topic 4)

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

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

**Answer:** E

**Explanation:**

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

**NEW QUESTION 150**

- (Topic 4)

Which of the following are advantages of a public cloud? (Select TWO).

- A. Full control of hardware
- B. Reduced monthly costs
- C. Decreased network latency



- D. Pay as you use
- E. Availability of self-service
- F. More secure data

**Answer:** BD

**Explanation:**

The correct answers are B and D.

\* B. Reduced monthly costs: One of the main advantages of public cloud is that it lowers the costs of IT infrastructure and maintenance for the customers. They do not need to purchase, install, or manage any hardware or software, and they only pay for the resources they use. This can result in significant savings compared to owning and operating a private cloud or an on-premise data center<sup>1234</sup>

\* D. Pay as you use: Another benefit of public cloud is that it offers a flexible and scalable pricing model based on the actual usage of the customers. They can adjust their resource consumption according to their changing needs and demands, and only pay for what they use. This eliminates the need for upfront capital investment or long-term contracts, and allows customers to optimize their spending and performance<sup>1234</sup>

**NEW QUESTION 154**

- (Topic 4)

A systems administrator is trying to connect to a remote KVM host. The command line appears as follows:

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

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

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

**Answer:** B

**Explanation:**

The answer is B. Running the command with elevated privileges. According to the web search results, the error message “End of file while reading data: sh: 1: nc: not found: Input/output error” indicates that the remote host does not have the nc (netcat) command installed or available in the PATH<sup>12</sup>. The nc command is used by libvirt to establish a connection between the client and the server. To fix this error, the administrator should install nc on the remote host or ensure that it is in the PATH. However, to do this, the administrator needs to have elevated privileges, such as sudo or root, on the remote host. Therefore, the administrator should try running the command with elevated privileges, such as sudo virsh remotehost or su -c ‘virsh remotehost’. This will allow the administrator to install nc or modify the PATH on the remote host and then connect to it using libvirt.

**NEW QUESTION 156**

- (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 159**

- (Topic 4)

Which of the following enables CSPs to offer unlimited capacity to customers?

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

**Answer:** C

**Explanation:**

The correct answer is C. Economies of scale.

Economies of scale are the cost advantages that CSPs can achieve by increasing the size and scale of their operations. By spreading the fixed costs of infrastructure, software, and personnel over a larger customer base and data volume, CSPs can reduce the average cost per unit of service and offer unlimited capacity to customers at competitive prices<sup>1</sup>. Adequate budget is not a sufficient condition for offering unlimited capacity, as CSPs still need to optimize their resource utilization and efficiency to meet the growing demand for data storage and processing.

Global data center distribution is a strategy that CSPs use to improve their service availability, reliability, and performance by locating their servers closer to their customers and reducing network latency. However, this does not necessarily imply unlimited capacity, as CSPs still need to manage the trade-offs between data center size, cost, and power consumption.

Agile project management is a methodology that CSPs use to deliver their services faster, better, and cheaper by adopting iterative, incremental, and collaborative approaches. However, this does not directly affect their capacity, as CSPs still need to scale their infrastructure and software to handle the increasing data load.

#### NEW QUESTION 162

- (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 167

- (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 171

- (Topic 4)

A cloud engineer is migrating a customer's web servers from a hypervisor platform to a CSP environment. The engineer needs to decouple the infrastructure and components during the migration to reduce the single points of failure. Which of the following storage options should the cloud engineer migrate the content to in order to improve availability?

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

**Answer:** C

#### Explanation:

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

#### NEW QUESTION 176

- (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 177**

- (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 appliance
- 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 181**

- (Topic 4)

A company is concerned it will run out of VLANs on its private cloud platform in the next couple months, and the product currently offered to customers requires the company to allocate three dedicated, segmented tiers. Which of the following can the company implement to continue adding new customers and to maintain the required level of isolation from other tenants?

- A. GRE
- B. SR-IOV
- C. VXLAN
- D. IPSec

**Answer:** C

**Explanation:**

One possible solution for the company to continue adding new customers and to maintain the required level of isolation from other tenants is to implement VXLAN.



VXLAN is a network virtualization technology that can extend VLAN by adding a 24-bit segment ID, which allows up to 16 million unique virtual segments. VXLAN can encapsulate layer 2 Ethernet frames within layer 3 IP packets, and tunnel them across the underlying network. VXLAN can provide logical isolation and security for different tenants, as well as scalability and flexibility for large cloud computing environments<sup>1</sup>.

#### NEW QUESTION 182

- (Topic 4)

A systems administrator needs to connect the companys network to a public cloud services provider. Which of the following will BEST ensure encryption in transit for data transfers?

- A. Identity federation
- B. A VPN tunnel
- C. A proxy solution
- D. A web application firewall

**Answer: B**

#### Explanation:

The answer is A. SAML. SAML (Security Assertion Markup Language) is a standard for exchanging authentication and authorization data between different parties, such as a user and a service provider. In a federated cluster, SAML can be used to enable single sign-on (SSO) for users across multiple clusters or cloud providers. SAML relies on the exchange of XML-based assertions that contain information about the user's identity, attributes, and entitlements. If the users' API access tokens have become invalid, it could be because the SAML assertions have expired, been revoked, or corrupted. The administrator should check the SAML configuration and logs to determine the cause of this issue.

Some possible sources of information about SAML and federated clusters are:

? Authenticating | Kubernetes: This page provides an overview of authenticating users in Kubernetes, including using SAML for federated identity.

? Authenticating to the Kubernetes API server - Google Cloud: This page explains how to authenticate to the Kubernetes API server on Google Cloud, including using SAML for federated identity with Google Cloud Identity Platform.

? Error 403 User not authorized when trying to access Azure Databricks API through Active Directory - Stack Overflow: This page discusses a similar issue of users getting an error when trying to access Azure Databricks API using SAML and Active Directory.

#### NEW QUESTION 187

- (Topic 4)

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

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

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

- A. Remove rules 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: B**

#### Explanation:

The correct answer is B. Remove rules 1, 3, and 4.

The objective is to ensure the web servers in the public subnet allow only secure communications. This means that only HTTPS traffic should be allowed on port 443, which is the standard port for secure web connections. HTTPS traffic uses the TCP protocol and encrypts the data between the client and the server.

Rule 1 allows all TCP traffic on any port from any source. This is too permissive and exposes the web servers to potential attacks or unauthorized access. Rule 1 should be removed to restrict the TCP traffic to only port 443.

Rule 3 allows all UDP traffic on any port from any source. UDP is a connectionless protocol that does not guarantee reliable or secure delivery of data. UDP is typically used for streaming media, voice over IP (VoIP), or online gaming, but not for web servers. Rule 3 should be removed to prevent unnecessary or malicious UDP traffic.

Rule 4 allows all ICMP traffic from any source. ICMP is a protocol that is used for diagnostic or control purposes, such as ping or traceroute. ICMP traffic can be used by attackers to scan or probe the network for vulnerabilities or information. Rule 4 should be removed to block ICMP traffic and reduce the attack surface.

Rule 2 allows TCP traffic on port 443 from any source. This is the desired rule that allows secure web communications using HTTPS. Rule 2 should be kept.

Rule 5 denies all other traffic that does not match any of the previous rules. This is the default rule that provides a catch-all protection for the web servers. Rule 5 should be kept. Therefore, the analyst should remove rules 1, 3, and 4 to accomplish the objective.

#### NEW QUESTION 188

- (Topic 4)

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



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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 192**

- (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 login
- D. DNS
- E. DHCP
- F. LDAP

**Answer:** AB

**Explanation:**

Telnet and FTP are two services that should be disabled on a cloud server because they are insecure and vulnerable to attacks. Telnet and FTP use plain text to transmit data over the network, which means that anyone who can intercept the traffic can read or modify the data, including usernames, passwords, commands, files, etc. This can lead to data breaches, unauthorized access, or malicious actions on the server<sup>1</sup>.

Instead of Telnet and FTP, more secure alternatives should be used, such as SSH (Secure Shell) and SFTP (Secure File Transfer Protocol). SSH and SFTP use encryption to protect the data in transit and provide authentication and integrity checks for the communication. SSH and SFTP can prevent eavesdropping, tampering, or spoofing of the data and ensure the confidentiality and privacy of the server<sup>2</sup>.

The other options are not services that should be disabled on a cloud server:

? Option C: Remote login. Remote login is a service that allows users to access a remote server from another location using a network connection. Remote login can be useful for managing, configuring, or troubleshooting a cloud server without having to physically access it. Remote login can be secured by using encryption, authentication, authorization, and logging mechanisms<sup>3</sup>.

? Option D: DNS (Domain Name System). DNS is a service that translates human-friendly domain names into IP addresses that can be used to communicate over the Internet. DNS is essential for resolving the names of the cloud resources and services that are hosted on the cloud platform. DNS can be secured by using DNSSEC (DNS Security Extensions), which add digital signatures to DNS records to verify their authenticity and integrity.

? Option E: DHCP (Dynamic Host Configuration Protocol). DHCP is a service that assigns IP addresses and other network configuration parameters to devices on a network. DHCP can simplify the management of IP addresses and avoid conflicts or errors in the network. DHCP can be secured by using DHCP snooping, which filters out unauthorized DHCP messages and prevents rogue DHCP servers from assigning IP addresses.

? Option F: LDAP (Lightweight Directory Access Protocol). LDAP is a service that stores and organizes information about users, devices, and resources on a network. LDAP can provide identity management and access control for the cloud environment. LDAP can be secured by using LDAPS (LDAP over SSL/TLS), which encrypts the LDAP traffic and provides authentication and integrity checks.

**NEW QUESTION 196**

- (Topic 4)

An integration application that communicates between different application and database servers is currently hosted on a physical machine. A P2V migration needs to be done to reduce the hardware footprint. Which of the following should be considered to maintain the same level of network throughput and latency in the virtual server?

- A. Upgrading the physical server NICs to support 10Gbps
- B. Adding more vCPU
- C. Enabling SR-IOV capability
- D. Increasing the VM swap/paging size

**Answer:** C

**Explanation:**

SR-IOV stands for Single Root I/O Virtualization, which is a technology that allows a physical network adapter to be partitioned into multiple virtual functions (VFs) that can be directly assigned to virtual machines (VMs). This way, the network traffic bypasses the software layer of the hypervisor and the virtual switch, and goes directly from the VM to the physical adapter. This reduces the CPU overhead, the network latency, and the packet loss, and improves the network throughput and scalability. SR-IOV can achieve near-native performance for network-intensive applications, such as an integration application that communicates between different application and database servers. By enabling SR-IOV capability on the physical server and the virtual server, the P2V migration can maintain the same level of network throughput and latency as the original physical machine. References: High performance network virtualization with SR-IOV; Supercharge Your Network Throughput via Single Root I/O Virtualization (SR-IOV); Overview of Single Root I/O Virtualization (SR-IOV).

**NEW QUESTION 198**

- (Topic 4)

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

- A. A PaaS solution

- B. A hybrid solution
- C. An IaaS solution
- D. A SaaS solution

Answer: A

Explanation:

A PaaS solution, or platform as a service, is a cloud computing service that provides a complete, ready-to-use, cloud-hosted platform for developing, running, maintaining and managing applications1. A PaaS solution would meet the company’s goal of maximizing scalability, availability, and security, while requiring no infrastructure administration, because:

Scalability: A PaaS solution can automatically scale up or down the resources needed to run the application based on the demand and traffic. The company does not need to worry about provisioning or managing servers, storage, network, or load balancers23.

Availability: A PaaS solution can ensure high availability and reliability of the application by replicating it across multiple regions and zones. The company does not need to worry about backup, recovery, or failover23.

Security: A PaaS solution can provide built-in security features such as encryption, authentication, authorization, and firewall. The company does not need to worry about installing or updating security patches or software23.

No infrastructure administration: A PaaS solution can abstract away the underlying infrastructure and hardware from the company. The company only needs to focus on developing and deploying the application code and data. The PaaS provider takes care of the rest23.

A hybrid solution (B) is a cloud computing service that combines on-premises and cloud resources. It may offer some benefits such as flexibility and cost optimization, but it would not meet the company’s goal of requiring no infrastructure administration. The company would still need to manage and maintain the on-premises part of the solution4.

An IaaS solution ©, or infrastructure as a service, is a

NEW QUESTION 202

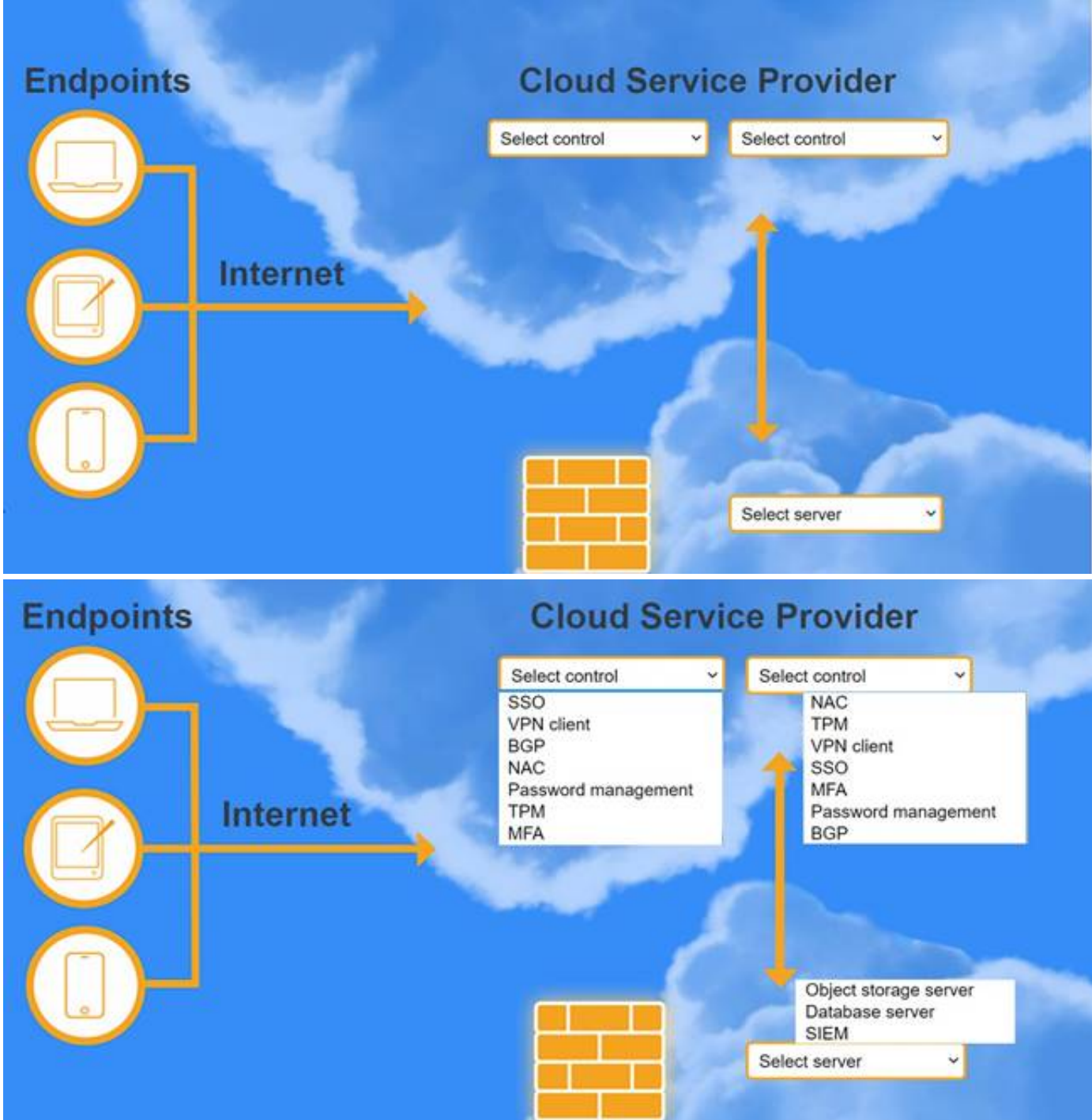
HOTSPOT - (Topic 4)

A highly regulated business is required to work remotely, and the risk tolerance is very low. You are tasked with providing an identity solution to the company cloud that includes the following:

- ? secure connectivity that minimizes user login
- ? tracks user activity and monitors for anomalous activity
- ? requires secondary authentication

INSTRUCTIONS

Select controls and servers for the proper control points.

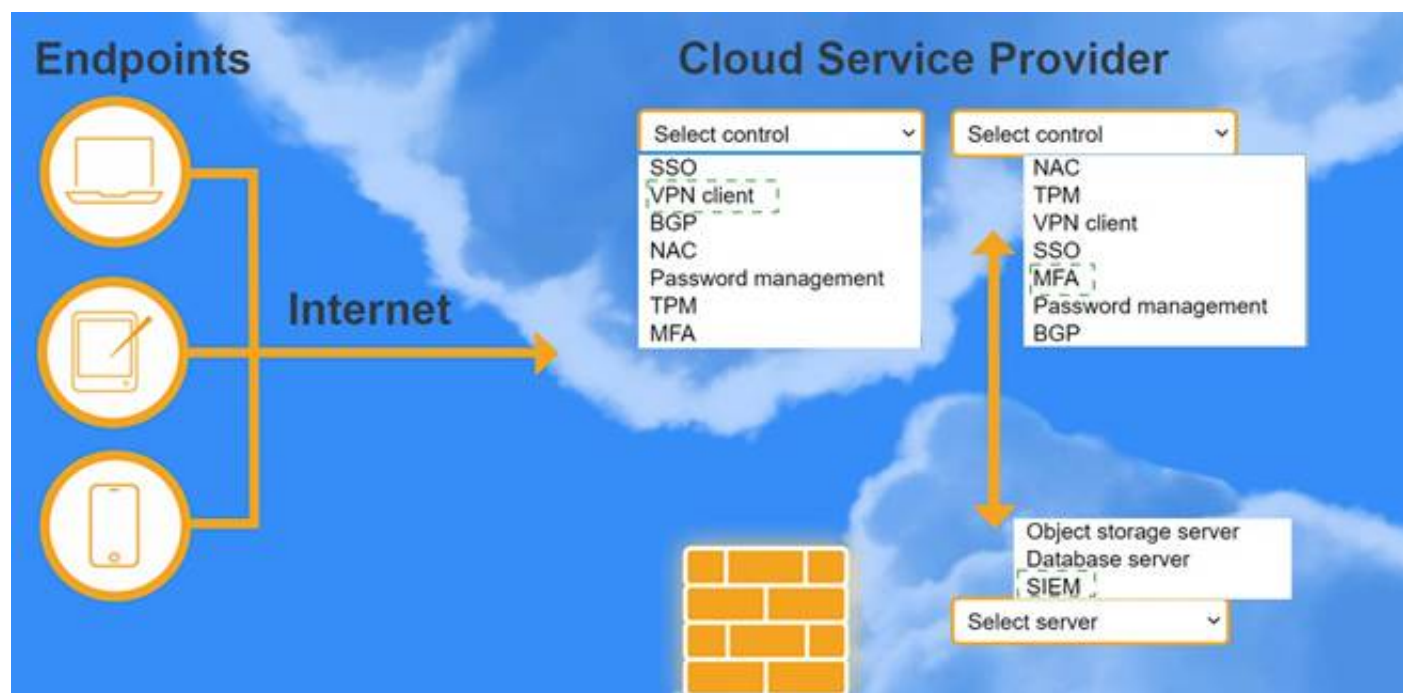


- A. Mastered
- B. Not Mastered

Answer: A

Explanation:





#### NEW QUESTION 206

- (Topic 4)

A cloud solutions architect has an environment that must only be accessed during work hours. Which of the following processes should be automated to BEST reduce cost?

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

**Answer: C**

#### Explanation:

One of the main benefits of cloud computing is that you only pay for the resources that you use. However, this also means that you need to manage your cloud resources efficiently and avoid paying for idle or unused resources<sup>1</sup>.

Shutting down the environment after work hours is a process that can be automated to best reduce cost in a cloud environment that must only be accessed during work hours. This process involves stopping or terminating the cloud resources, such as virtual machines, databases, load balancers, etc., that are not needed outside of the work hours. This can significantly reduce the cloud bill by avoiding charges for compute, storage, network, and other services that are not in use<sup>2</sup>.

The other options are not the best processes to automate to reduce cost in this scenario:

? Option A: Scaling of the environment after work hours. Scaling is a process that involves adjusting the number or size of cloud resources to match the demand or workload. Scaling can be done manually or automatically using triggers or policies. Scaling can help optimize the performance and availability of a cloud environment, but it does not necessarily reduce the cost. Scaling down the environment after work hours may reduce some costs, but it may still incur charges for the remaining resources. Scaling up the environment before work hours may increase the cost and also introduce delays or errors in provisioning new resources<sup>3</sup>.

? Option B: Implementing access control after work hours. Access control is a process that involves defining and enforcing rules and policies for who can access what resources in a cloud environment. Access control can help improve the security and compliance of a cloud environment, but it does not directly affect the cost. Implementing access control after work hours may prevent unauthorized access to the environment, but it does not stop or terminate the resources that are still running and consuming cloud services<sup>4</sup>.

? Option D: Blocking external access to the environment after work hours. Blocking external access is a process that involves restricting or denying network traffic from outside sources to a cloud environment. Blocking external access can help protect the environment from potential attacks or breaches, but it does not impact the cost. Blocking external access after work hours may prevent unwanted requests or connections to the environment, but it does not shut down or release the resources that are still active and generating cloud charges.

#### NEW QUESTION 207

- (Topic 4)

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

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

**Answer: C**

#### Explanation:

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

#### NEW QUESTION 211

- (Topic 4)

A business is looking at extending the platform for an internally developed application using microservices from various cloud vendors. The cloud architect is

responsible for reviewing the proposed solution design, which covers critical requirements for the business to fulfill its requirements. Which of the following is the most likely requirement the cloud architect needs to fulfill?

- A. Software
- B. Budgetary
- C. Security
- D. Integration

**Answer:** D

**Explanation:**

Integration is the process of connecting and coordinating different components or systems to work together as a whole. In this scenario, the business is looking at extending the platform for an internally developed application using microservices from various cloud vendors. This means that the cloud architect needs to ensure that the microservices can communicate and interact with each other across different cloud platforms, as well as with the existing application. Integration is a critical requirement for the business to fulfill its requirements, as it affects the functionality, performance, and reliability of the application. Software, budgetary, and security are also important requirements, but they are not the most likely ones that the cloud architect needs to fulfill in this scenario. Software refers to the programs and applications that run on the cloud platforms. Budgetary refers to the costs and expenses associated with the cloud services and solutions. Security refers to the protection of the data and resources in the cloud environment from unauthorized access or attacks. References: CompTIA Cloud+ CV0-003 Certification Study Guide, Chapter 22, Microservices and Cloud Integration, page 3531.

**NEW QUESTION 212**

- (Topic 4)

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

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 217**

- (Topic 4)

A systems administrator has a redundant backup system in place. Which of the following should the systems administrator perform to maintain efficient operation and comply with the global standard in the corporate backup policies?

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

**Answer:** C

**NEW QUESTION 221**

- (Topic 4)

A cloud administrator deployed new hosts in a private cloud. After a few months elapsed, some of the hypervisor features did not seem to be working. Which of the following was MOST likely causing the issue?

- A. Incorrect permissions
- B. Missing license
- C. Incorrect tags
- D. Oversubscription

**Answer:** B

**Explanation:**

The correct answer is B. Missing license.

Some hypervisor features may require a valid license to work properly. If the license is missing, expired, or invalid, the hypervisor may not be able to use those features or may operate in a reduced functionality mode. For example, some features of Hyper-V, such as live migration, replication, and failover clustering, require a license for Windows Server or Windows 10 Enterprise<sup>1</sup>. Similarly, some features of VMware ESXi, such as vMotion, Storage vMotion, and Fault Tolerance, require a license for VMware vSphere<sup>2</sup>. Therefore, if a cloud administrator deployed new hosts in a private cloud and found that some of the hypervisor features did not seem to be working after a few months elapsed, the most likely cause was a missing license. The administrator should check the license status of the hypervisor and renew or activate the license if needed.

Incorrect permissions are not a likely cause of the issue, as they would affect the access to the hypervisor or its resources, not the functionality of the hypervisor itself. Incorrect tags are also not a likely cause of the issue, as they are used for identification and classification of resources, not for enabling or disabling features. Oversubscription is not a likely cause of the issue either, as it would affect the performance or availability of the resources, not the functionality of the hypervisor itself.

**NEW QUESTION 222**

- (Topic 4)

A new development team requires workstations hosted in a PaaS to develop a new website. Members of the team also require remote access to the workstations using their corporate email addresses. Which of the following solutions will best meet these requirements? (Select two).



- A. Deploy new virtual machines.
- B. Configure email account replication.
- C. Integrate identity services.
- D. Implement a VDI solution.
- E. Migrate local VHD workstations.
- F. Create a new directory service.

**Answer:** CD

**Explanation:**

To meet the requirements of the development team, the cloud administrator should integrate identity services and implement a VDI solution. Identity services are used to authenticate and authorize users and devices to access cloud resources. By integrating identity services, the cloud administrator can enable the development team to use their corporate email addresses to log in to the PaaS workstations. A VDI solution is a virtualization technology that allows users to access remote desktops hosted on a cloud platform. By implementing a VDI solution, the cloud administrator can provide the development team with workstations that have the necessary tools and configurations for web development. References: [CompTIA Cloud+ CV0-003 Certification Study Guide], Chapter 2, Objective 2.1: Given a scenario, deploy cloud services and solutions.

**NEW QUESTION 224**

- (Topic 4)

A cloud administrator has received a physical disk that was analyzed by the incident response team. Which of the following documents should the cloud administrator update?

- A. Chain of custody
- B. Incident taxonomy
- C. Risk register
- D. Incident playbook

**Answer:** A

**Explanation:**

A. Chain of custody

A chain of custody is a document that records the sequence of custody, control, transfer, analysis, and disposition of physical or electronic evidence. A chain of custody is important to ensure the integrity and admissibility of evidence in legal cases. A cloud administrator who receives a physical disk that was analyzed by the incident response team should update the chain of custody to document when, how, and by whom the disk was handled, and what actions were performed on it<sup>12</sup>.

An incident taxonomy is a classification system that provides additional information about an incident, such as the nature, impact, intent, root cause, and data exposed. An incident taxonomy is useful for identifying trends and patterns, but it does not track the movement or manipulation of evidence<sup>3</sup>.

A risk register is a document that identifies, records, and assesses potential risks in a project or an organization. A risk register helps to prioritize and mitigate risks, and to develop contingency plans. A risk register is not directly related to the analysis of a physical disk by the incident response team<sup>4</sup>.

An incident playbook is a document that provides a series of prescriptive steps and guidance for responding and resolving incidents. An incident playbook helps to simplify and standardize the response process, and to reduce human error. An incident playbook does not record the details or outcomes of the response actions<sup>5</sup>.

**NEW QUESTION 226**

- (Topic 4)

An organization is conducting a performance test of a public application. The following actions have already been completed:

- The baseline performance has been established.
- A load test has passed.
- A benchmark report has been generated.

Which of the following needs to be done to conclude the performance test?

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

**Answer:** A

**Explanation:**

To conclude the performance test of a public application, the organization needs to verify the application works well under an unexpected volume of requests. This is also known as a stress test, which is a type of performance test that evaluates the behavior and stability of the application under extreme conditions<sup>1</sup>. A stress test can help identify potential bottlenecks, errors, or failures that may occur when the application is subjected to a sudden surge or spike in demand<sup>2</sup>. A stress test can also help determine the maximum capacity and scalability of the application<sup>3</sup>.

References: CompTIA Cloud+ CV0-003 Exam Objectives, Objective 2.2: Given a scenario, deploy and test a cloud solution ; Performance Testing | Cloud Computing | CompTIA<sup>1</sup> ; Stress Testing - Software Testing Fundamentals<sup>2</sup> ; What is Stress Testing? Definition, Types, Tools & Examples<sup>3</sup>

**NEW QUESTION 229**

- (Topic 4)

A cloud administrator created four VLANs to autoscale the container environment. Two of the VLANs are on premises, while two VLANs are on a public cloud provider with a direct link between them. Firewalls are between the links with an additional subnet for communication, which is 192.168.5.0/24.

The on-premises gateways are:

- \* 192.168.1.1/24
- \* 192.168.2.1/24

The cloud gateways are:

- \* 192.168.3.1/24
- \* 192.168.4.1/24

The orchestrator is unable to communicate with the cloud subnets. Which Of the following should the administrator do to resolve the issue?

- A. Allow firewall traffic to 192.168.5.0/24.
- B. Set both firewall interfaces to 192.168.5.1/24.
- C. Add interface 192.168.3.1/24 on the local firewall.

D. Add interface 192.168.1.1/24 on the cloud firewall.

**Answer:** A

**Explanation:**

To allow communication between the on-premises and cloud subnets, the firewall traffic should be allowed to pass through the additional subnet for communication, which is 192.168.5.0/24. This subnet acts as a bridge between the two networks and should have firewall rules that permit traffic from and to both sides.

References: [CompTIA Cloud+ Study Guide], page 181.

**NEW QUESTION 231**

- (Topic 4)

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

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 233**

- (Topic 4)

An IT professional is selecting the appropriate cloud storage solution for an application that has the following requirements:

- The owner of the objects should be the object writer.
- The storage system must enforce TLS encryption.

Which of the following should the IT professional configure?

- A. A bucket
- B. A CIFS endpoint
- C. A SAN
- D. An NFS mount

**Answer:** A

**Explanation:**

A bucket is a cloud storage solution that allows users to store and access objects, such as files, images, videos, etc. A bucket is typically associated with object storage services, such as Amazon S3, Google Cloud Storage, or Microsoft Azure Blob Storage<sup>123</sup>. A bucket has the following characteristics that match the requirements of the application:

? The owner of the objects is the object writer. This means that the user who uploads or writes an object to the bucket becomes the owner of that object and can control its access permissions<sup>456</sup>.

? The storage system enforces TLS encryption. This means that the data in transit between the client and the bucket is encrypted using the Transport Layer Security (TLS) protocol, which provides security and privacy for the communication . A CIFS endpoint, a SAN, and an NFS mount are not cloud storage solutions, but rather network protocols or architectures that enable access to storage devices

**NEW QUESTION 236**

- (Topic 4)

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

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 240**

- (Topic 4)

An integration application that communicates between different application and database servers is currently hosted on a physical machine. A P2V migration needs to be done to reduce the hardware footprint. Which of the following should be considered to maintain the same level of network throughput and latency in the virtual server?

- A. Upgrading the physical server NICs to support IOGbps
- B. Adding more vCPU
- C. Enabling SR-IOV capability
- D. Increasing the VM swap/paging size

**Answer:** C

**Explanation:**

SR-IOV stands for Single Root Input/Output Virtualization, which is a technology that allows a physical device, such as a network interface card (NIC), to be shared by multiple virtual machines (VMs) without sacrificing performance or latency. By enabling SR-IOV capability, the integration application can communicate directly with the physical NIC, bypassing the hypervisor and the virtual switch, and reducing the network overhead and latency .

**NEW QUESTION 242**

.....

## 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