Exam Questions CV0-003

CompTIA Cloud+ Certification Exam

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

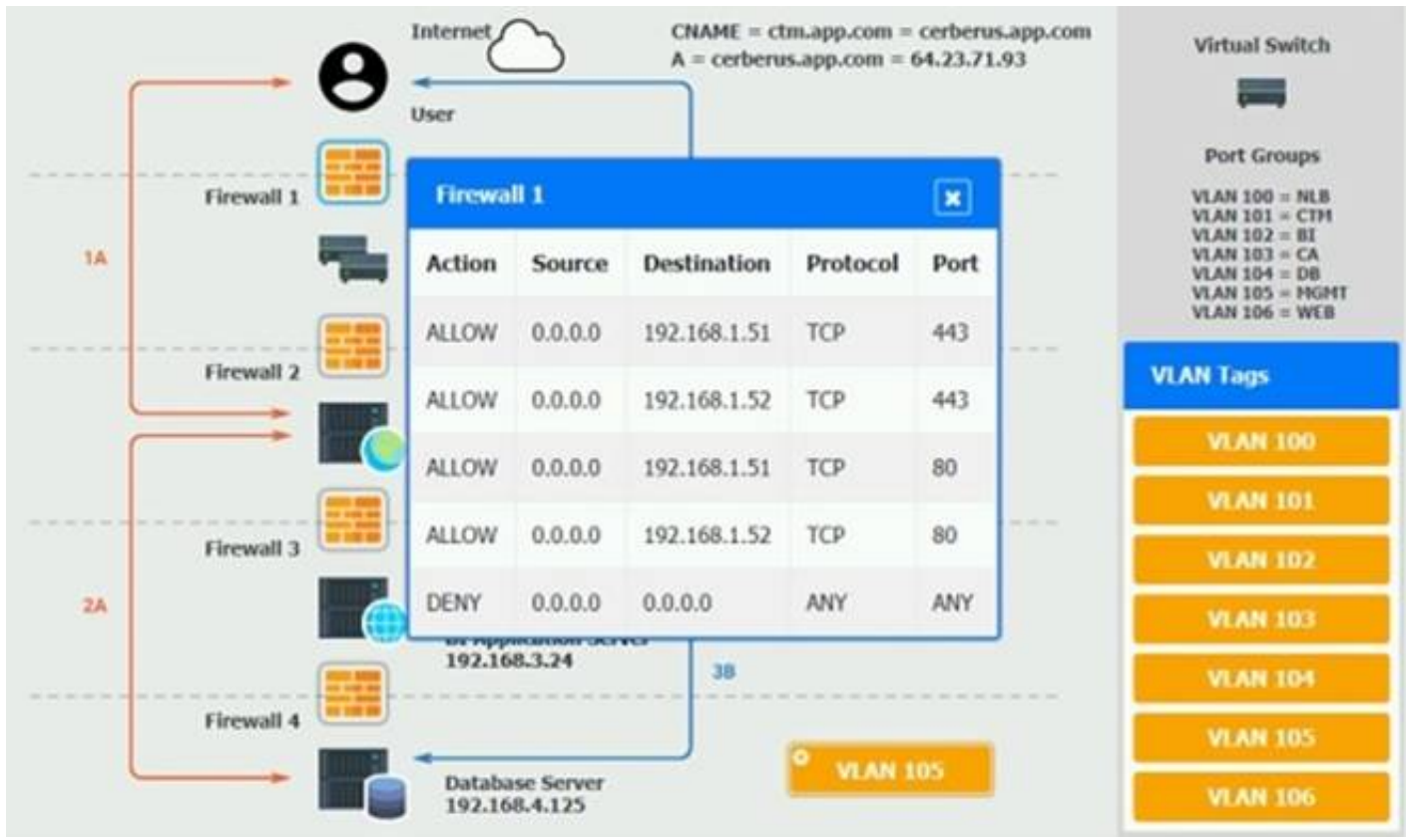
NEW QUESTION 1
- (Topic 1)
An organization is running a database application on a SATA disk, and a customer is experiencing slow performance most of the time.
Which of the following should be implemented to improve application performance?

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

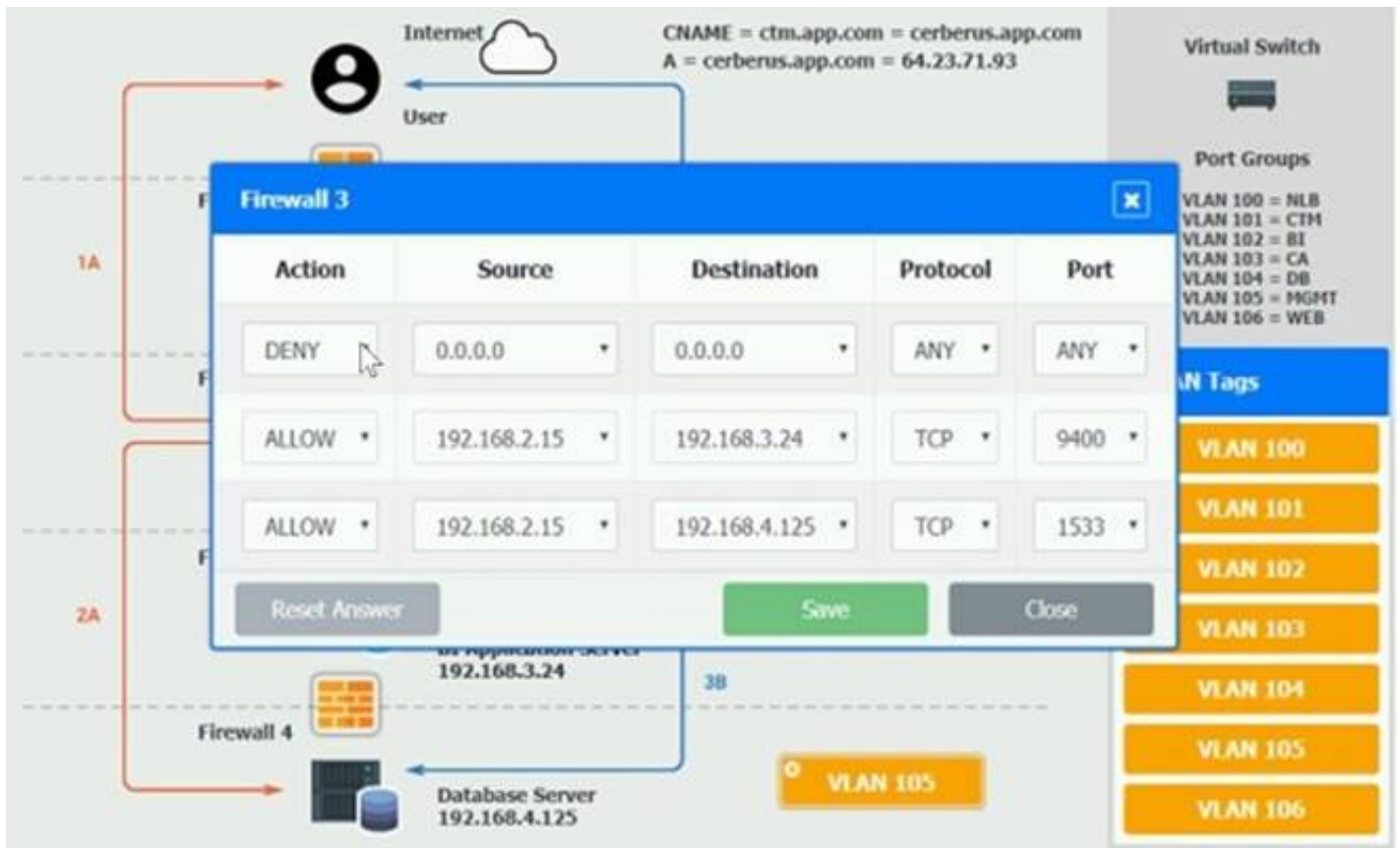
Answer: D

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

NEW QUESTION 2
SIMULATION - (Topic 1)
The QA team is testing a newly implemented clinical trial management (CTM) SaaS application that uses a business intelligence application for reporting. The UAT users were instructed to use HTTP and HTTPS.
Refer to the application dataflow:
1A – The end user accesses the application through a web browser to enter and view clinical data.
2A – The CTM application server reads/writes data to/from the database server.
1B – The end user accesses the application through a web browser to run reports on clinical data.
2B – The CTM application server makes a SOAP call on a non-privileged port to the BI application server.
3B – The BI application server gets the data from the database server and presents it to the CTM application server.
When UAT users try to access the application using https://ctm.app.com or http://ctm.app.com, they get a message stating: “Browser cannot display the webpage.” The QA team has raised a ticket to troubleshoot the issue.
INSTRUCTIONS
You are a cloud engineer who is tasked with reviewing the firewall rules as well as virtual network settings.
You should ensure the firewall rules are allowing only the traffic based on the dataflow. You have already verified the external DNS resolution and NAT are working.
Verify and appropriately configure the VLAN assignments and ACLs. Drag and drop the appropriate VLANs to each tier from the VLAN Tags table. Click on each Firewall to change ACLs as needed.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.


Internet
CNAME = ctm.app.com = cerberus.app.com
A = cerberus.app.com = 64.23.71.93
User
Firewall 1
1A
Firewall 2
Firewall 3
2A
Firewall 4
Firewall 1
Action Source Destination Protocol Port
ALLOW 0.0.0.0 192.168.1.51 TCP 443
ALLOW 0.0.0.0 192.168.1.52 TCP 443
ALLOW 0.0.0.0 192.168.1.51 TCP 80
ALLOW 0.0.0.0 192.168.1.52 TCP 80
DENY 0.0.0.0 0.0.0.0 ANY ANY
192.168.3.24
3B
Database Server
192.168.4.125
VLAN 105
Virtual Switch
Port Groups
VLAN 100 = NLB
VLAN 101 = CTM
VLAN 102 = BI
VLAN 103 = CA
VLAN 104 = DB
VLAN 105 = MGMT
VLAN 106 = WEB
VLAN Tags
VLAN 100
VLAN 101
VLAN 102
VLAN 103
VLAN 104
VLAN 105
VLAN 106


Internet
CNAME = ctm.app.com = cerberus.app.com
A = cerberus.app.com = 64.23.71.93
Firewall 2
Action Source Destination Protocol Port
ALLOW 192.168.1.51 192.168.2.15 TCP 88
DENY 192.168.1.52 UDP
DENY TCP 443
DENY 0.0.0.0 ANY ANY
0.0.0.0
127.0.0.1
64.23.71.93
192.168.1.51
192.168.1.52
192.168.2.15
192.168.2.24
192.168.3.24
192.168.4.125
TCP
UDP
ANY
80
88
443
1533
9400
ANY
Reset Answer
Save
Close
Database Server
192.168.4.125
VLAN 105
Virtual Switch
Port Groups
VLAN 100 = NLB
VLAN 101 = CTM
VLAN 102 = BI
VLAN 103 = CA
VLAN 104 = DB
VLAN 105 = MGMT
VLAN 106 = WEB
VLAN 100
VLAN 101
VLAN 102
VLAN 103
VLAN 104
VLAN 105
VLAN 106


Internet
CNAME = ctm.app.com = cerberus.app.com
A = cerberus.app.com = 64.23.71.93
User
Firewall 3
Action Source Destination Protocol Port
DENY 0.0.0.0 0.0.0.0 ANY ANY
ALLOW 192.168.2.15 192.168.3.24 TCP 9400
ALLOW 192.168.2.15 192.168.4.125 TCP 1533
Reset Answer
Save
Close
192.168.3.24
3B
Firewall 4
Database Server
192.168.4.125
VLAN 105
Virtual Switch
Port Groups
VLAN 100 = NLB
VLAN 101 = CTM
VLAN 102 = BI
VLAN 103 = CA
VLAN 104 = DB
VLAN 105 = MGMT
VLAN 106 = WEB
VLAN 100
VLAN 101
VLAN 102
VLAN 103
VLAN 104
VLAN 105
VLAN 106

A. Mastered
B. Not Mastered

Answer: A

Explanation:
On firewall 3, change the DENY 0.0.0.0 entry to rule 3 not rule 1.

NEW QUESTION 3
- (Topic 1)
Which of the following strategies will mitigate the risk of a zero-day vulnerability MOST efficiently?

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

Answer: D

Explanation:
An incident response plan is a document or procedure that defines the roles, responsibilities, and actions to be taken in the event of a security incident or breach. Having a detailed incident response plan can help mitigate the risk of a zero-day vulnerability most efficiently, as it can provide a clear and consistent framework for identifying, containing, analyzing, and resolving any potential threats or exploits related to the unknown or unpatched vulnerability. Having a detailed incident response plan can also help minimize the impact and damage of a security incident or breach, as it can enable timely and effective recovery and restoration processes. References: CompTIA Cloud+ Certification Exam Objectives, page 14, section 2.7

NEW QUESTION 4
- (Topic 1)
A systems administrator disabled TLS 1.0 and 1.1, as well as RC4, 3DES, and AES-128 ciphers for TLS 1.2, on a web server. A client now reports being unable to access the web server, but the administrator verifies that the server is online, the web service is running, and other users can reach the server as well.
Which of the following should the administrator recommend the user do FIRST?

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

Answer: D

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

NEW QUESTION 5
- (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 6
- (Topic 1)
After analyzing a web server's logs, a systems administrator sees that users are connecting to the company's application through HTTP instead of HTTPS. The administrator then configures a redirect from HTTP to HTTPS on the web server, and the application responds with a connection time-out message.
Which of the following should the administrator verify NEXT?

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

Answer: B

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

NEW QUESTION 7
- (Topic 1)
The security team for a large corporation is investigating a data breach. The team members are all trying to do the same tasks but are interfering with each other's work. Which of the following did the team MOST likely forget to implement?

A. Incident type categories
B. A calling tree
C. Change management
D. Roles and responsibilities

Answer: D

Explanation:
Roles and responsibilities are definitions or descriptions of what each team member or stakeholder is expected to do or perform in a project or process. Roles and responsibilities can help clarify the scope, authority, and accountability of each team member or stakeholder and avoid any confusion or duplication of work. The security team most likely forgot to implement roles and responsibilities when investigating a data breach, as they are all trying to do the same tasks but are interfering with each other's work. Implementing roles and responsibilities can help improve efficiency and effectiveness, as it can ensure that each team member or stakeholder knows what tasks they need to do and how they need to coordinate with others. References: CompTIA Cloud+ Certification Exam Objectives, page 13, section 2.5

NEW QUESTION 8
- (Topic 1)
A systems administrator is deploying a GPU-accelerated VDI solution. Upon requests from several users, the administrator installs an older version of the OS on their virtual workstations. The majority of the VMs run the latest LTS version of the OS.
Which of the following types of drivers will MOST likely ensure compatibility will all virtual workstations?

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

Answer: D

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

NEW QUESTION 9
- (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 10
- (Topic 1)
A company wants to check its infrastructure and application for security issues regularly. Which of the following should the company implement?

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

Answer: C

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

NEW QUESTION 10
- (Topic 1)
A company has 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 13
- (Topic 1)
An organization will be deploying a web application in a public cloud with two web servers, two database servers, and a load balancer that is accessible over a single public IP.
Taking into account the gateway for this subnet and the potential to add two more web servers, which of the following will meet the minimum IP requirement?

A. 192.168.1.0/26
B. 192.168.1.0/27
C. 192.168.1.0/28
D. 192.168.1.0/29

Answer: C

Explanation:
A /28 subnet is a subnet that has a network prefix of 28 bits and a host prefix of 4 bits. A /28 subnet can support up to 16 hosts (14 usable hosts) and has a subnet mask of 255.255.255.240. Using a /28 subnet can meet the minimum IP requirement for deploying a web application in a public cloud with two web servers, two database servers, and a load balancer that is accessible over a single public IP, taking into account the gateway for this subnet and the potential to add two more web servers. Using a /28 subnet can provide enough host addresses for the current and future web servers, database servers, load balancer, and gateway, as well as allow for some growth or redundancy.
References: CompTIA Cloud+ Certification Exam Objectives, page 15, section 2.8

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

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

Answer: A

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

NEW QUESTION 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 22
- (Topic 1)
A company has a cloud infrastructure service, and the cloud architect needs to set up a DR site.
Which of the following should be configured in between the cloud environment and the DR site?

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

Answer: D

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

NEW QUESTION 25
- (Topic 1)
A cloud administrator is setting up a DR site on a different zone of the same CSP. The application servers are replicated using the VM replication, and the database replication is set up using log shipping. Upon testing the DR site, the application servers are unable to access the database servers. The administrator has verified the systems are running and are accessible from the CSP portal.

Which of the following should the administrator do to fix this issue?

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

Answer: C

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

NEW QUESTION 30
- (Topic 1)
A media company has made the decision to migrate a physical, internal file server to the cloud and use a web- based interface to access and manage the files. The users must be able to use their current corporate logins.
Which of the following is the MOST efficient way to achieve this goal?

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

Answer: B

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

NEW QUESTION 31
- (Topic 1)
A VDI administrator has received reports of poor application performance. Which of the following should the administrator troubleshoot FIRST?

A. The network environment
B. Container resources
C. Client devices
D. Server resources

Answer: A

Explanation:
The network environment is the set of network devices, connections, protocols, and configurations that enable communication and data transfer between different systems and applications. The network environment can affect the performance of a virtual desktop infrastructure (VDI) by influencing factors such as bandwidth, latency, jitter, packet loss, and congestion. Poor network performance can result in slow or unreliable application delivery, degraded user experience, and reduced productivity.
Therefore, troubleshooting the network environment should be the first step for a VDI administrator who receives reports of poor application performance.
References: CompTIA Cloud+ Certification Exam Objectives, page 17, section 3.4

NEW QUESTION 34
- (Topic 2)
A vendor is installing a new retail store management application for a customer. The application license ensures software costs are low when the application is not being used, but costs go up when use is higher.
Which of the following licensing models is MOST likely being used?

A. Socket-based
B. Core-based
C. Subscription
D. Volume-based

Answer: D

Explanation:
Volume-based licensing is a pricing model that charges the customers based on the amount of usage or consumption of a software product or service. The more the customers use the software, the higher the costs will be. This model is suitable for applications that have variable or seasonal demand patterns. Examples of volume-based licensing are AWS Lambda, Azure Functions, Google Cloud Run, etc.

NEW QUESTION 39
- (Topic 2)
A cloud administrator wants to have a central repository for all the logs in the company’s private cloud. Which of the following should be implemented to BEST meet this requirement?

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

Answer: D

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

NEW QUESTION 43
- (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 46
- (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 49
- (Topic 2)
A database analyst reports it takes two hours to perform a scheduled job after onboarding 10,000 new users to the system. The analyst made no changes to the scheduled job before or after onboarding the users. The database is hosted in an IaaS instance on a cloud provider. Which of the following should the cloud administrator evaluate to troubleshoot the performance of the job?

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

Answer: A

Explanation:
To troubleshoot the performance of a scheduled job that takes two hours to run after onboarding 10,000 new users to a cloud-based system, the administrator should evaluate the IaaS compute configurations, the capacity trend analysis reports, and the storage IOPS. These factors can affect the performance of a

database job in an IaaS instance on a cloud provider. The IaaS compute configurations include the CPU, memory, and network resources assigned to the instance. The capacity trend analysis reports show the historical and projected usage and demand of the resources. The storage IOPS (Input/Output Operations Per Second) measure the speed and performance of the disk storage. The administrator should check if these factors are sufficient, optimal, or need to be adjusted to improve the performance of the job.

NEW QUESTION 51
- (Topic 2)
All of a company's servers are currently hosted in one cloud MSP. The company created a new cloud environment with a different MSP. A cloud engineer is now tasked with preparing for server migrations and establishing connectivity between clouds. Which of the following should the engineer perform FIRST?

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

Answer: C

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

NEW QUESTION 53
- (Topic 2)
A systems administrator is configuring updates on a system. Which of the following update branches should the administrator choose to ensure the system receives updates that are maintained for at least four years?

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

Answer: A

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

NEW QUESTION 56
- (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 58
- (Topic 2)
Which of the following cloud services is fully managed?

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

Answer: E

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

NEW QUESTION 60

- (Topic 2)
A system administrator is migrating a bare-metal server to the cloud. Which of the following types of migration should the systems administrator perform to accomplish this task?

A. V2V
B. V2P
C. P2P
D. P2V

Answer: D

Explanation:
P2V (Physical to Virtual) is a type of migration that converts a physical server into a virtual machine (VM). P2V migration can help to move a bare-metal server to the cloud by creating an image of its disk and configuration and uploading it to a cloud platform that supports VM creation from custom images.

NEW QUESTION 62
- (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 65
- (Topic 2)
An organization is using multiple SaaS-based business applications, and the systems administrator is unable to monitor and control the use of these subscriptions. The administrator needs to implement a solution that will help the organization apply security policies and monitor each individual SaaS subscription. Which of the following should be deployed to achieve these requirements?

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

Answer: B

Explanation:
CASB (Cloud Access Security Broker) is what should be deployed to monitor and control the use of multiple SaaS-based business applications in a cloud environment. SaaS (Software as a Service) is a cloud service model that provides customers with access to software applications hosted on remote servers over a network or internet connection. SaaS can provide customers with convenience, flexibility, and scalability, but it may also introduce security risks such as data breaches, leaks, losses, etc., especially if customers have multiple SaaS subscriptions from different providers. CASB is a tool or service that acts as an intermediary between customers and SaaS providers. CASB can help to monitor and control the use of multiple SaaS subscriptions by providing features such as:
? Visibility: CASB can provide visibility into what SaaS applications are being used, by whom, when, where, how, etc., as well as identify any unauthorized or suspicious activities.
? Compliance: CASB can provide compliance with various laws, regulations, standards, policies, etc., that apply to SaaS applications and data, such as GDPR, HIPAA, PCI DSS, etc., as well as enforce them using rules or actions.
? Security: CASB can provide security for SaaS applications and data by detecting and preventing any threats or attacks, such as malware, phishing, ransomware, etc., as well as protecting them using encryption, authentication, authorization, etc.

NEW QUESTION 66
- (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 68
- (Topic 2)
A cloud administrator is responsible for managing a cloud-based content management solution. According to the security policy, any data that is hosted in the cloud must be protected against data exfiltration. Which of the following solutions should the administrator implement?

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

Answer: C

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

NEW QUESTION 73
- (Topic 2)
A systems administrator is performing upgrades to all the hypervisors in the environment. Which of the following components of the hypervisors should be upgraded? (Choose two.)

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

Answer: CF

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

NEW QUESTION 74
- (Topic 2)
A systems administrator is trying to establish an RDP session from a desktop to a server in the cloud. However, the connection appears to be refused even through the VM is responding to ICMP echo requests. Which of the following should the administrator check FIRST?

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

Answer: A

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

NEW QUESTION 78
- (Topic 2)
A resource pool in a cloud tenant has 90 GB of memory and 120 cores. The cloud administrator needs to maintain a 30% buffer for resources for optimal performance of the hypervisor. Which of the following would all ow for the maximum number of two-core machines with equal memory?

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

Answer: C

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

within the available limits.

NEW QUESTION 81
- (Topic 2)
A disaster situation has occurred, and the entire team needs to be informed about the situation. Which of the following documents will help the administrator find the details of the relevant team members for escalation?

A. Chain of custody
B. Root cause analysis
C. Playbook
D. Call tree

Answer: D

Explanation:
A call tree is what will help the administrator find the details of the relevant team members for escalation after a disaster situation has occurred and the entire team needs to be informed about the situation. A call tree is a document or diagram that shows the hierarchy or sequence of communication or notification among team members in case of an emergency or incident, such as a disaster situation. A call tree can help to find the details of the relevant team members for escalation by providing information such as:
? Name: This indicates who is involved in the communication or notification process, such as team members, managers, stakeholders, etc.
? Role: This indicates what is their function or responsibility in the communication or notification process, such as initiator, receiver, sender, etc.
? Contact: This indicates how they can be reached or contacted in the communication or notification process, such as phone number, email address, etc.

NEW QUESTION 86
- (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 89
- (Topic 2)
A systems administrator is analyzing a report of slow performance in a cloud application. This application is working behind a network load balancer with two VMs, and each VM has its own digital certificate configured. Currently, each VM is consuming 85% CPU on average. Due to cost restrictions, the administrator cannot scale vertically or horizontally in the environment. Which of the following actions should the administrator take to decrease the CPU utilization? (Choose two.)

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

Answer: BC

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

NEW QUESTION 91
- (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 94
- (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 95
- (Topic 1)
Company A has acquired Company B and is in the process of integrating their cloud resources. Company B needs access to Company A's cloud resources while retaining its IAM solution.
Which of the following should be implemented?

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

Answer: C

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

NEW QUESTION 98
- (Topic 1)
A systems administrator is informed that a database server containing PHI and PII is unencrypted. The environment does not support VM encryption, nor does it have a key management system. The server needs to be able to be rebooted for patching without manual intervention.
Which of the following will BEST resolve this issue?

A. Ensure all database queries are encrypted
B. Create an IPSec tunnel between the database server and its clients
C. Enable protocol encryption between the storage and the hypervisor
D. Enable volume encryption on the storage
E. Enable OS encryption

Answer: D

Explanation:
Volume encryption is a type of encryption that protects data at the storage level by encrypting an entire disk or partition. Volume encryption can provide strong security for data at rest, as it prevents unauthorized access to the data even if the storage device is lost, stolen, or compromised. Volume encryption can also support automatic booting without manual intervention, as it can use a pre-boot authentication mechanism that does not require user input. Enabling volume encryption on the storage is the best way to resolve the issue of having an unencrypted database server containing PHI and PII, as it can protect the sensitive data without relying on VM encryption or a key management
system. References: CompTIA Cloud+ Certification Exam Objectives, page 14, section 2.7

NEW QUESTION 100
- (Topic 1)
A company is utilizing a private cloud solution that is hosted within its datacenter. The company wants to launch a new business application, which requires the resources below:

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

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

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

Answer: B

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

NEW QUESTION 105
- (Topic 1)
A storage array that is used exclusively for datastores is being decommissioned, and a new array has been installed. Now the private cloud administrator needs to migrate the data.
Which of the following migration methods would be the BEST to use?

A. Conduct a V2V migration
B. Perform a storage live migration
C. Rsync the data between arrays
D. Use a storage vendor migration appliance

Answer: B

Explanation:
A storage live migration is a process of moving or transferring data or files from one storage system or device to another without interrupting or affecting the availability or performance of the VMs or applications that use them. Performing a storage live migration can help migrate the data from a SAN that is being decommissioned to a new array, as it can ensure that there is no downtime or disruption for the VMs or applications that rely on the data or files stored on the SAN. Performing a storage live migration can also help maintain consistency and integrity, as it can synchronize and verify the data or files between the source and destination storage systems or devices.
References: CompTIA Cloud+ Certification Exam Objectives, page 10, section 1.5

NEW QUESTION 109
- (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 113
- (Topic 1)
A systems administrator is reviewing two CPU models for a cloud deployment. Both CPUs have the same number of cores/threads and run at the same clock speed.
Which of the following will BEST identify the CPU with more computational power?

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

Answer: D

Explanation:

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

NEW QUESTION 114
- (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 119
- (Topic 1)
A cloud administrator recently noticed that a number of files stored at a SaaS provider's file-sharing service were deleted. As part of the root cause analysis, the administrator noticed the parent folder permissions were modified last week. The administrator then used a test user account and determined the permissions on the files allowed everyone to have write access.
Which of the following is the best step for the administrator to take NEXT?

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

Answer: D

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

NEW QUESTION 123
- (Topic 1)
An organization's web server farm, which is hosted in the cloud with DNS load balancing, is experiencing a spike in network traffic. This has caused an outage of the organization's web server infrastructure.
Which of the following should be implemented to prevent this in the future as a mitigation method?

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

Answer: D

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

NEW QUESTION 124
- (Topic 1)
An OS administrator is reporting slow storage throughput on a few VMs in a private IaaS cloud. Performance graphs on the host show no increase in CPU or memory. However, performance graphs on the storage show a decrease of throughput in both IOPS and MBps but not much increase in latency. There is no increase in workload, and latency is stable on the NFS storage arrays that are used by those VMs.
Which of the following should be verified NEXT?

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

Answer: D

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

NEW QUESTION 129
- (Topic 1)
A marketing team is using a SaaS-based service to send emails to large groups of potential customers. The internally managed CRM system is configured to generate a list of target customers automatically on a weekly basis, and then use that list to send emails to each customer as part of a marketing campaign. Last week, the first email campaign sent emails successfully to 3,000 potential customers. This week, the email campaign attempted to send out 50,000 emails, but only 10,000 were sent.
Which of the following is the MOST likely reason for not sending all the emails?

A. API request limit
B. Incorrect billing account
C. Misconfigured auto-scaling
D. Bandwidth limitation

Answer: A

Explanation:
An API request limit is a restriction on the number of requests that can be made to a web service or application programming interface (API) within a certain time period. API request limits are often used by SaaS-based services to control the usage and traffic of their customers and prevent overloading or abuse of their resources. An API request limit can cause a failure to send all the emails if the marketing team exceeds the number of requests allowed by the SaaS-based service in a week. The service may reject or block any requests that go beyond the limit, resulting in fewer emails being sent than expected. References: CompTIA Cloud+ Certification Exam Objectives, page 13, section 2.5
Reference: https://developers.google.com/analytics/devguides/config/mgmt/v3/limits- quotas

NEW QUESTION 133
- (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 138
- (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 139
- (Topic 4)
A security analyst is investigating a recurring alert. The alert is reporting an insecure firewall configuration state after every cloud application deployment. The process of identifying the issue, requesting a fix, and waiting for the developers to manually patch the environment is being repeated multiple times. In an effort to identify the root issue, the following logs were collected:
Deploying template app prod. •yaml Instance DB successfully created DB keys successfully stored on vault
Instance WebApp successfully created Access rules successfully applied Access—keys successfully created
Which of the following options will provide a permanent fix for the issue?

A. Validate the Iac code used during the deployment.

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

Answer: A

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

NEW QUESTION 142
- (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 PATH12. 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 144
- (Topic 4)
A systems administrator is deploying a new version of a website. The website is deployed in the cloud using a VM cluster. The administrator must then deploy the new version into one VM first. After a period of time, if there are no issues detected, a second VM will be updated. This process must continue until all the VMS are updated. Which of the following upgrade methods is being implemented?

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

Answer: C

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

NEW QUESTION 148
- (Topic 4)
A systems administrator audits a cloud application and discovers one of the key regulatory requirements has not been addressed. The requirement states that if a physical breach occurs and hard drives are stolen, the contents of the drives should not be readable. Which of the following should be used to address the requirement?

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

Answer: B

Explanation:
Encryption is the process of transforming data into an unreadable format using a secret key or algorithm. Encryption can be used to protect data at rest or in transit from unauthorized access or theft. If a physical breach occurs and hard drives are stolen, encryption can prevent the contents of the drives from being readable by anyone who does not have the decryption key or algorithm.
References: [CompTIA Cloud+ Study Guide], page 236.

NEW QUESTION 153
- (Topic 4)
A cloud administrator is having difficulty correlating logs for multiple servers. Upon inspection, the administrator finds that the time-zone settings are mismatched throughout the deployment. Which of the following solutions can help maintain time synchronization between all the resources?

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

Answer: C

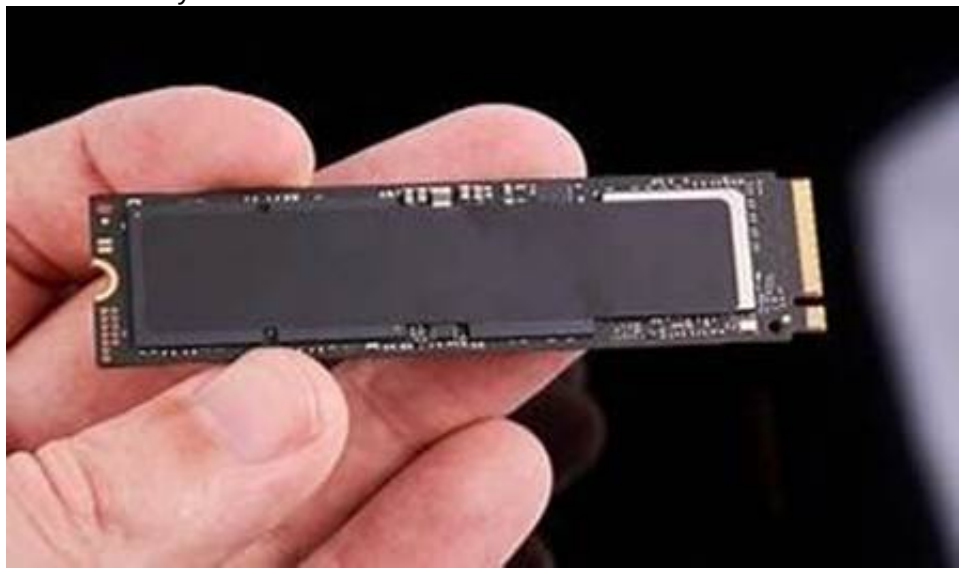
Explanation:
The correct answer is C. NTP.
NTP stands for Network Time Protocol, which is a standard protocol for synchronizing the clocks of computers over a network. NTP uses a hierarchical, client-server architecture, where a client requests the current time from a server, and the server responds with a timestamp. The client then adjusts its own clock to match the server's time, taking into account the network delay and clock drift. NTP can achieve sub-millisecond accuracy over local area networks and a few milliseconds over the internet12.
NTP can help maintain time synchronization between all the resources in a distributed cloud environment, as it allows each resource to get the accurate time from a reliable source. This can help with correlating logs, auditing, security, and other time-sensitive operations. NTP can also handle different time zones, as it uses Coordinated Universal Time (UTC) as the reference time, and each resource can convert UTC to its local time zone12.
DNS stands for Domain Name System, which is a protocol for resolving domain names into IP addresses. DNS does not provide any functionality for time synchronization3.
IPAM stands for IP Address Management, which is a method for planning, tracking, and managing the IP address space used in a network. IPAM does not provide any functionality for time synchronization.
SNMP stands for Simple Network Management Protocol, which is a protocol for collecting and organizing information about managed devices on a network. SNMP can be used to monitor the performance, availability, configuration, and security of network devices, but it does not provide any functionality for time synchronization.

NEW QUESTION 158
- (Topic 4)
A technician deployed a VM with NL-SAS storage to host a critical application. Two weeks later, users have begun to report high application latency. Which of the following is the best action to correct the latency issue?

A. Increase the capacity of the data storage.
B. Migrate the data to SAS storage.
C. Increase the CPU of the VM.
D. Migrate the data to flash storage.

Answer: D

Explanation:
Flash memory



Explore
One possible answer is:
D. Migrate the data to flash storage.
Flash storage is a type of solid-state storage technology that uses flash memory chips to store data. Flash storage has several advantages over NL-SAS storage, which is a hybrid of SATA and SAS technologies that uses spinning disks to store data. Flash storage can provide much faster performance, lower latency, higher reliability, and lower power consumption than NL-SAS storage12. Therefore, migrating the data to flash storage can help correct the latency issue for the critical application. However, flash storage may also be more expensive and have lower capacity than NL-SAS storage, so these factors should also be considered before making the migration decision12.

NEW QUESTION 161
- (Topic 4)
When designing a three-node. load-balanced application, a systems administrator must ensure each node runs on a different physical server for HA purposes.

Which of the following does the systems administrator need to configure?

A. Round-robin methods
B. Live migration
C. Anti-affinity rule
D. Priority queues

Answer: C

Explanation:
The correct answer is C. Anti-affinity rule.
An anti-affinity rule is a configuration option that prevents two or more virtual machines (VMs) from running on the same physical host. This can improve the availability and fault tolerance of the VMs, as it reduces the risk of losing multiple VMs due to a single host failure. An anti-affinity rule can also improve the performance and load balancing of the VMs, as it distributes the workload across different hosts and avoids resource contention . A round-robin method is a load balancing algorithm that distributes incoming requests to a pool of servers in a circular order. A round-robin method does not consider the availability, capacity, or location of the servers, and may assign requests to servers that are overloaded, offline, or far away. A round-robin method does not ensure that each node runs on a different physical server.
A live migration is a process that allows moving a running VM from one physical host to another without interrupting its operation. A live migration can improve the availability and performance of the VMs, as it enables dynamic load balancing, maintenance, and disaster recovery. However, a live migration does not prevent two or more VMs from running on the same physical host in the first place.
A priority queue is a data structure that stores elements based on their priority values. A priority queue allows inserting and removing elements in order of their priority, such that the element with the highest priority is always at the front of the queue. A priority queue can be used to implement scheduling algorithms for processes or tasks, but it does not affect where they run on physical servers.

NEW QUESTION 162
- (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 165
- (Topic 4)
A company is comparing an application environment to be hosted on site versus a SaaS model of the same application. Which of the following SaaS-based licensing models should the administrator consider?

A. Per core
B. Per socket
C. Per instance
D. Per user

Answer: D

Explanation:
Per user is a common SaaS-based licensing model that charges customers based on the number of users who access the software. This model is suitable for applications that have a clear and consistent user base, such as CRM, ERP, or collaboration tools. Per user licensing allows customers to scale up or down their usage as their needs change, and only pay for what they use. Per user licensing also simplifies the billing and management of the software, as customers do not need to worry about the underlying infrastructure, hardware, or software updates. References: CompTIA Cloud+ CV0-003 Study Guide, Chapter 1: Cloud Concepts and Models, page 19; SaaS Licensing.

NEW QUESTION 167
- (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: AC

Explanation:
A Platform-as-a-Service (PaaS) is a cloud computing model that provides customers a complete cloud platform—hardware, software, and infrastructure—for developing, running, and managing applications without the cost, complexity, and inflexibility that often comes with building and maintaining that platform on-premises1.
To develop a new website using a PaaS, the development team needs to deploy new virtual machines (VMs) on the cloud platform. VMs are software emulations

of physical computers that can run different operating systems and applications. By deploying new VMs, the development team can create a scalable and flexible environment for their website project, without having to invest in or manage physical hardware2.
To enable remote access to the workstations using their corporate email addresses, the development team needs to integrate identity services on the cloud platform. Identity services are services that provide authentication, authorization, and identity management for users and devices accessing cloud resources. By integrating identity services, the development team can use their corporate email addresses as single sign-on (SSO) credentials to access their workstations from any device and location, while ensuring security and compliance3.
The other options are not the best solutions for these requirements:
? Configuring email account replication is not necessary for remote access to the workstations. Email account replication is a process of synchronizing email accounts across different servers or locations. It can provide backup and redundancy for email services, but it does not provide authentication or identity management for remote access4.
? Implementing a Virtual Desktop Infrastructure (VDI) solution is not a PaaS solution.
VDI is a technology that allows users to access virtual desktops hosted on a centralized server. VDI can provide remote access to desktop environments, but it requires additional hardware, software, and management costs that are not included in a PaaS model5.
? Migrating local VHD workstations is not a PaaS solution. VHD stands for Virtual Hard Disk, which is a file format that represents a virtual hard disk drive. Migrating local VHD workstations means moving the virtual hard disk files from local storage to cloud storage. This can provide backup and portability for the workstations, but it does not provide a complete cloud platform for developing and running applications6.
? Creating a new directory service is not necessary for remote access to the workstations. A directory service is a service that stores and organizes information about users, devices, and resources on a network. Creating a new directory service means setting up a new database and schema for storing this information. This can provide identity management and access control for the network, but it does not provide authentication or SSO for remote access.

NEW QUESTION 168
- (Topic 4)
A systems administrator is troubleshooting issues with audio lag during phone conferences. When looking at the core switch, the administrator notices its buffers are consistently full, and packets are being dropped due to the large number being sent and received. There is no room in the budget for new hardware, but it is critical that the audio lag be fixed immediately. Which of the following will most likely resolve the issue?

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

Answer: B

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

NEW QUESTION 169
- (Topic 4)
A company is using a hybrid cloud environment. The private cloud is hosting the business applications, and the cloud services are being used to replicate for availability purposes.
The cloud services are also being used to accommodate the additional resource requirements to provide continued services. Which of the following scalability models is the company utilizing?

A. Vertical scaling
B. Autoscaling
C. Cloud bursting
D. Horizontal scaling

Answer: C

Explanation:
Cloud bursting is a scalability model that allows a company to use a hybrid cloud environment to handle peak or unpredictable workloads. Cloud bursting involves using the private cloud to host the core or critical applications, and using the public cloud to provide additional or temporary resources when the demand exceeds the capacity of the private cloud .
Cloud bursting can help a company to:
Improve the availability and reliability of the applications by replicating them across multiple cloud platforms and locations .
Optimize the performance and efficiency of the applications by dynamically allocating and releasing resources based on the workload and traffic .
Reduce the cost and complexity of the IT infrastructure by leveraging the pay-as-you-go and on-demand models of the public cloud .

NEW QUESTION 171
- (Topic 4)
A cloud administrator needs to reduce storage costs. Which of the following would best help the administrator reach that goal?

A. Enabling compression
B. Implementing deduplication
C. Using containers
D. Rightsizing the VMs

Answer: B

Explanation:
Deduplication is a process by which redundant data is eliminated, thus reducing the size of the dataset. Deduplication with cloud storage reduces the storage requirements, along with the amount of data to be transferred over the network, resulting in faster and more efficient data protection operations1. Deduplication can help to shrink the data footprint, lower the storage costs, and improve the performance of backup and recovery processes2. Deduplication can be applied at different levels, such as file-level, block-level, or byte-level, depending on the granularity and efficiency of the technique3. Deduplication can also be performed at different locations, such as source, target, or cloud, depending on the architecture and design of the storage system3. By implementing deduplication, a cloud

administrator can achieve significant data savings and optimize the cloud storage costs4. References: Data deduplication techniques for efficient cloud storage management: a systematic review; How Data Deduplication Reduces Cloud Data Costs; How Data Deduplication Can Save Cloud Storage Costs?; Data Deduplication Overview; What is Data Deduplication and How Can it Help Reduce Cloud Costs?.

NEW QUESTION 172
- (Topic 4)
A cloud engineer needs to perform a database migration. The database has a restricted SLA and cannot be offline for more than ten minutes per month. The database stores 800GB of data, and the network bandwidth to the CSP is 100MBps Which of the following is the best option to perform the migration?

A. Copy the database to an external device and ship the device to the CSP.
B. Create a replica database, synchronize the data, and switch to the new instance.
C. Utilize a third-party tool to back up and restore the data to the new database.
D. Use the database import/export method and copy the exported file.

Answer: B

Explanation:
The best option to perform the database migration is to create a replica database, synchronize the data, and switch to the new instance. This option can help meet the restricted SLA and avoid offline time for the database. Creating a replica database can help copy the data from the source to the destination without interrupting the database operations. Synchronizing the data can help ensure that the replica database is updated with any changes that occur in the source database during the migration process. Switching to the new instance can help complete the migration and activate the new database in the cloud. This option can also help avoid the network bandwidth limitation and the large size of the data. References: CompTIA Cloud+ CV0-003 Certification Study Guide, Chapter 7, Objective 7.1: Given a scenario, migrate applications and data to the cloud.

NEW QUESTION 176
- (Topic 4)
A systems administrator notices the host filesystem is running out of storage space. Which of the following will best reduce the storage space on the system?

A. Deduplication
B. Compression
C. Adaptive optimization
D. Thin provisioning

Answer: A

Explanation:
Deduplication is a technique that reduces the storage space by eliminating duplicate data blocks and replacing them with pointers to the original data. Deduplication can help free up the host filesystem by removing redundant data and increasing the storage efficiency. Deduplication can be performed at the source or the target, and it can be applied at the file or block level. References: [CompTIA Cloud+ CV0-003 Certification Study Guide], Chapter 4, Objective 4.3: Given a scenario, troubleshoot common storage issues.

NEW QUESTION 177
- (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 Storage123. 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 permissions456.
? 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 178
- (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 179
- (Topic 4)
A cloud administrator is reviewing the current private cloud and public laaS environment, and is building an optimization plan. Portability is of great concern for the administrator so resources can be easily moved from one environment to another.
Which of the following should the administrator implement?

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

Answer: C

Explanation:
Containers are packages of software that contain all of the necessary elements to run in any environment. Containers virtualize the operating system and run anywhere, from a private data center to the public cloud or even on a developer's personal laptop. Containers provide an isolated environment for running applications, sharing the host OS kernel but isolating processes, file systems, and network resources. Containers package applications and their dependencies together, ensuring they run consistently across different environments, from development to production. Containers are lightweight, resource-efficient, fast, and immutable, making them ideal for portability and scalability. By using containers, a cloud administrator can easily move resources from one environment to another without changing the code or configuration of the applications. References: CompTIA Cloud+ CV0-003 Study Guide, Chapter 2: Deploying a Cloud Environment, page 75-76; What are containers?; Portability in the Cloud: Cloud Native and Containers.

NEW QUESTION 182
- (Topic 4)
A company has a web application that is accessed around the world. An administrator has been notified of performance issues regarding the application. Which of the following will BEST improve performance?

A. IPAM
B. SDN
C. CDN
D. VPN

Answer: C

Explanation:
The correct answer is C. CDN.
A CDN, or content delivery network, is a group of servers spread out over a region or around the world that work together to speed up content delivery on the web. The servers in a CDN temporarily store (or cache) webpage content like images, HTML, JavaScript, and video. They send the cached content to users who load the webpage1.
A CDN can improve the performance of a web application that is accessed around the
world by:
Decreasing the distance between where content is stored and where it needs to go. A CDN can serve content from the server that is closest to the user, reducing network latency and bandwidth consumption.
Reducing file sizes to increase load speed. A CDN can employ techniques such as compression, minification, and image optimization to reduce the amount of data that needs to be transferred.
Optimizing server infrastructure to respond to user requests more quickly. A CDN can use hardware and software enhancements such as solid-state hard drives, load balancing, and caching algorithms to improve the efficiency and reliability of the servers12.
IPAM, or IP address management, is a method for planning, tracking, and managing the IP address space used in a network. IPAM does not directly affect the performance of a web application.
SDN, or software-defined networking, is a technology that allows network administrators to dynamically configure and control network resources using software applications. SDN can improve the flexibility and scalability of a network, but it does not necessarily improve the performance of a web application.
VPN, or virtual private network, is a technology that creates a secure and encrypted connection between a device and a network over the internet. VPN can enhance the privacy and security of a web application, but it does not improve its performance. In fact, VPN may introduce some overhead and latency due to encryption and decryption processes3.

NEW QUESTION 185
- (Topic 4)
Following the deployment of a new VM, a cloud engineer notices the backup platform has not added the machine to the appropriate job. The backup platform uses a text-based variable for job configuration. This variable is based on the RPO requirements for the workload. Which of the following did the cloud engineer forget to configure when deploying the virtual machine?
? Tags

A. RPO
B. RTO
C. Server name
D. Template

Answer: A

Explanation:
Tags are key-value pairs that can be applied to cloud resources to organize, categorize, and filter them. Tags can also be used to assign resources to backup jobs based on their RPO requirements. The cloud engineer forgot to configure the appropriate tag for the new VM that matches the text-based variable of the backup platform. Therefore, the backup platform did not add the VM to the correct job. References: Tags and labels |
Cloud Storage | Google Cloud, CompTIA Cloud+ Certification Exam Objectives, Domain 4.0: Operations and Support, Objective 4.3: Given a scenario, apply the appropriate methods for cost control in a cloud environment.

NEW QUESTION 186
- (Topic 4)
A cloud administrator used a deployment script to recreate a number of servers hosted in a public-cloud provider_ However, after the script completes, the administrator receives the following error when attempting to connect to one of the servers Via SSH from the administrators workstation: CHANGED. Which of the following IS the MOST likely cause of the issue?

A. The DNS records need to be updated
B. The cloud provider assigned a new IP address to the server.
C. The fingerprint on the server's RSA key is different
D. The administrator has not copied the public key to the server.

Answer: C

Explanation:
This error indicates that the SSH client has detected a change in the server's RSA key, which is used to authenticate the server and establish a secure connection. The SSH client stores the fingerprints of the servers it has previously connected to in a file called known_hosts, which is usually located in the ~/.ssh directory. When the SSH client tries to connect to a server, it compares the fingerprint of the server's RSA key with the one stored in the known_hosts file. If they match, the connection proceeds. If they do not match, the SSH client warns the user of a possible man-in-the-middle attack or a host key change, and aborts the connection.
The most likely cause of this error is that the deployment script has recreated the server with a new RSA key, which does not match the one stored in the known_hosts file. This can happen when a server is reinstalled, cloned, or migrated. To resolve this error, the administrator needs to remove or update the old fingerprint from the known_hosts file, and accept the new fingerprint when connecting to the server again. Alternatively, the administrator can use a tool or service that can synchronize or manage the RSA keys
across multiple servers, such as AWS Key Management Service (AWS KMS) 1, Azure Key Vault 2, or HashiCorp Vault 3.

NEW QUESTION 189
- (Topic 4)
A DevOps team needs to provide a solution that offers isolation, portability, and scalability Which of the following would BEST meet these requirements?

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

Answer: B

Explanation:
Containers are a solution that offers isolation, portability, and scalability for software development and deployment. Containers are lightweight and self-contained units of software that package up the application code and all its dependencies, such as libraries, frameworks, and configuration files. Containers run on a container platform, such as Docker or Kubernetes, that provides the runtime environment and orchestration for the containers.
Containers offer isolation, as they run independently from each other and from the underlying host system. Each container has its own namespace, filesystem, network, and resources, and does not interfere with other containers or processes. Containers also offer portability, as they can run on any system that supports the container platform, regardless of the hardware or operating system differences. Containers can be easily moved, copied, or deployed across different environments, such as development, testing, or production. Containers also offer scalability, as they can be dynamically created, destroyed, or replicated to meet the changing demand for the application. Containers can also leverage the distributed computing power of clusters, which are groups of servers that work together to provide high availability and performance .

NEW QUESTION 193
- (Topic 4)
A company has applications that need to remain available in the event of the data center being unavailable. The company's cloud architect needs to find a solution to maintain business continuity. Which of following should the company implement?

A. A DR solution for the application between different data centers
B. An off-site backup solution with a third-party vendor
C. laC techniques to recreate the system at a new provider
D. An HA solution for the application inside the data center

Answer: A

Explanation:
A disaster recovery (DR) solution is a set of policies, procedures, and tools that enable an organization to restore or continue its critical functions in the event of a natural or human-induced disaster. A DR solution for the application between different data centers means that the application is replicated or backed up to another location that is geographically separated from the primary data center. This way, if the primary data center becomes unavailable due to a power outage, fire, flood, cyberattack, or any other cause, the application can be switched over to the secondary data center and resume its operations with minimal downtime and data loss. This solution ensures business continuity and high availability for the application and its users. References: CompTIA Cloud+ CV0- 003 Study Guide, Chapter 5: Maintaining a Cloud Environment, page 221-222; Disaster recovery planning guide.

NEW QUESTION 197
- (Topic 4)
A systems administrator needs to implement a way for users to verify software integrity. Which of the following tools would BEST meet the administrator's needs?

A. TLS 1.3
B. CRC32
C. AES-256
D. SHA-512

Answer: D

Explanation:

SHA-512 is a tool that can generate a cryptographic hash value for any given data. A cryptographic hash value is a fixed-length string of bits that uniquely and irreversibly represents the data. SHA-512 is one of the variants of the Secure Hash Algorithm 2 (SHA-2) family, which is a widely used and standardized hash function .
SHA-512 can help users to verify software integrity by comparing the hash values of the software before and after downloading, installing, or transferring. If the hash values match, it means that the software has not been altered, corrupted, or tampered with. If the hash values differ, it means that the software may have been compromised, infected, or damaged .

NEW QUESTION 200
- (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 the concept of ensuring that certain virtual machines or workloads do not run on the same physical host. This can improve the availability and performance of the system, as well as prevent a single point of failure. In this scenario, the systems administrator needs to ensure the database nodes do not exist on the same physical host, so anti-affinity would best meet this requirement. Oversubscription is the concept of allocating more resources to virtual machines than the physical host actually has, which can improve the utilization and efficiency of the system, but it does not guarantee the separation of the database nodes. A firewall is a device or software that controls the network traffic between different zones or segments, which can improve the security and isolation of the system, but it does not affect the placement of the database nodes. A separate cluster is a group of hosts that share common resources and policies, which can improve the scalability and manageability of the system, but it does not ensure the database nodes do not exist on the same physical host within the cluster. References: CompTIA Cloud+ CV0-003 Certification Study Guide, Chapter 1, Cloud Architecture and Design, page 131.

NEW QUESTION 205
- (Topic 4)
A systems administrator wants to be notified every time an application's configuration files are updated. Which of the following should the administrator implement to achieve the objective?

A. ZFS
B. FIM
C. MAC
D. DLP

Answer: B

Explanation:
FIM stands for File Integrity Monitoring, and it is a security technique that monitors and detects changes in files and directories. FIM can help the systems administrator to be notified every time an application’s configuration files are updated by generating alerts or reports when the files are modified, added, deleted, or accessed. FIM can also help verify the integrity and authenticity of the files by comparing their hashes or signatures with a baseline or a trusted source. FIM can be implemented using software
tools or agents that run on the host or the network. References: CompTIA Cloud+ CV0-003 Certification Study Guide, Chapter 9, Objective 9.1: Given a scenario, apply security controls and techniques.

NEW QUESTION 208
- (Topic 4)
A cloud administrator is looking at the company's cloud services bill for the previous month. The administrator notices on the billing dashboard that certain resources are not being billed to any particular department. Which of the following actions will help correct this billing issue?

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

Answer: D

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

NEW QUESTION 213
- (Topic 4)
A systems administrator notices several VMS are constantly ballooning, while the memory usage of several other VMS is significantly lower than their resource allocation. Which of the following will MOST likely solve the issue?

A. Rightsizing
B. Bandwidth increase
C. Cluster placement
D. Storage tiers

Answer: A

Explanation:
The best answer is A. Rightsizing.
Rightsizing is the process of restructuring a company so it can make a profit more efficiently and meet updated business objectives1. Organizations will usually rightsize their business by reducing their workforce, reorganizing upper management, cutting costs, and changing job roles2.
Rightsizing can help solve the issue of VMs constantly ballooning, while the memory usage of several other VMs is significantly lower than their resource allocation. Ballooning is a memory reclamation technique used when ESXi host runs out of memory. It involves a balloon driver that consumes unused memory within the VM's address space and makes it available for other uses by the host machine3. However, ballooning can also degrade the performance of the VMs and cause swapping or paging4.
By rightsizing the VMs, the systems administrator can adjust the memory allocation according to the actual demand and usage of each VM. This can prevent overprovisioning or underprovisioning of memory resources and improve the efficiency and profitability of the company. Rightsizing can also help avoid redundancies, streamline workflows, and make better hiring decisions1.

NEW QUESTION 218
- (Topic 4)
A cloud security engineer needs to design an IDS/IPS solution for a web application in a single virtual private network. The engineer is considering implementing IPS protection for traffic coming from the internet. Which of the following should the engineer consider to meet this requirement?

A. Configuring a web proxy server
B. Implementing load balancing using SSI- in front of web applications
C. Implementing IDS/IPS agents on each instance running in that virtual private network
D. Implementing dynamic routing

Answer: C

Explanation:
An Intrusion Detection System (IDS) is a software or hardware system that monitors network traffic for malicious activity and alerts the administrator of any potential threats.
An Intrusion Prevention System (IPS) is a software or hardware system that not only detects but also blocks or mitigates the malicious activity. Both IDS and IPS are essential for securing a web application in a cloud environment1.
A web proxy server is a server that acts as an intermediary between the client and the web server. It can provide caching, filtering, and authentication services, but it does not offer IDS/IPS functionality. Therefore, option A is incorrect.
Load balancing using SSI (Server Side Includes) is a technique that distributes the workload among multiple web servers by inserting dynamic content into web pages. It can improve the performance and availability of a web application, but it does not provide IDS/IPS protection. Therefore, option B is incorrect.
Implementing IDS/IPS agents on each instance running in that virtual private network is a valid solution for providing IPS protection for traffic coming from the internet. The agents can monitor and inspect the network traffic on each instance and block or report any suspicious activity to a central management console. This can prevent attacks from reaching the web application or spreading to other instances in the same network. Therefore, option C is correct.
Implementing dynamic routing is a technique that allows routers to select the best path for forwarding packets based on network conditions. It can enhance the reliability and efficiency of a network, but it does not offer IDS/IPS functionality. Therefore, option D is incorrect.

NEW QUESTION 223
- (Topic 4)
A systems administrator has been notified of possible illegal activities taking place on the network and has been directed to ensure any relevant emails are preserved for court use.
Which of the following is this MOST likely an example of?

A. Email archiving
B. Version control
C. Legal hold
D. File integrity monitoring

Answer: C

Explanation:
The correct answer is C. Legal hold.
A legal hold is a process that organizations use to preserve relevant electronic information when they anticipate litigation or have an active e-discovery request. A legal hold requires that certain email messages be retained and unaltered until they are no longer required for court use. Legal hold requirements apply both to the content of messages as well as the metadata which can provide proof of delivery and other critical non-repudiation information12.
Email archiving is a process that organizations use to store email messages for long-term retention, compliance, and backup purposes. Email archiving does not necessarily imply that the email messages are preserved for legal purposes, although some email archiving solutions may offer legal hold capabilities1.
Version control is a process that software developers use to manage changes to source code and other files in a project. Version control allows developers to track, compare, and revert changes, as well as collaborate with other developers. Version control does not apply to email messages or legal hold.
File integrity monitoring is a process that security professionals use to detect unauthorized or malicious changes to files and directories on a system. File integrity monitoring helps to protect the system from malware, data breaches, and configuration errors. File integrity monitoring does not apply to email messages or legal hold.

NEW QUESTION 225
- (Topic 4)
An environment has a dual-stack infrastructure in an active-active configuration in two separate data centers. Which of the following best describes replication between the two sites?

A. Data is moved constantly from the hot site to the warm site.
B. Data is replicated every 15 minutes from one site to the other.
C. Data is moved from one site to the other once per day.

D. Data is synchronized in real time across the sites.
E. Data is moved twice a day from Site A to Site B, and then from Site B to Site A.

Answer: D

Explanation:
A dual-stack infrastructure is a network that supports both IPv4 and IPv6 protocols. An active-active configuration is a high-availability cluster that distributes workloads across two or more nodes that are running the same service simultaneously. Replication between the two sites means that data is copied from one site to another to ensure consistency and redundancy. Data synchronization is the process of ensuring that data is identical across multiple locations. Therefore, data synchronization in real time means that data is replicated as soon as it changes on either site, without any delay or lag. References: Active-Active vs. Active-Passive High-Availability Clustering, Dual-stack IPv6 architectures for AWS and hybrid networks – Part 2, Understanding Dual Stacking of IPv4 and IPv6 Unicast Addresses

NEW QUESTION 230
- (Topic 4)
A systems administrator is implementing a new file storage service that has been deployed in the company's private cloud instance. The key requirement is fast read/write times for the targeted users, and the budget for this project is not a concern. Which of the following storage types should the administrator deploy?

A. Spinning disks
B. NVMe
C. SSD
D. Hybrid

Answer: B

Explanation:
The best storage type to deploy for the new file storage service is NVMe. NVMe stands for Non-Volatile Memory Express, and it is a protocol that allows faster access to data stored on solid state drives (SSDs). NVMe can deliver high performance, low latency, and parallelism for the file storage service. NVMe can also support fast read/write times for the targeted users, which is the key requirement for the project. Since the budget for the project is not a concern, NVMe can be a suitable choice for the file storage service. References: CompTIA Cloud+ CV0-003 Certification Study Guide, Chapter 4, Objective 4.1: Given a scenario, implement cloud storage solutions.

NEW QUESTION 235
- (Topic 4)
A cloud administrator has deployed a website and needs to improve the site security to meet requirements. The website architecture is designed to have a DBaaS in the back end and autoscaling instances in the front end using a load balancer to distribute the request.
Which of the following will the cloud administrator most likely use?

A. An API gateway
B. An IPS/IDS
C. A reverse proxy
D. A WAF

Answer: D

Explanation:
A web application firewall (WAF) is a security solution that monitors and filters the traffic between a web application and the Internet. A WAF can help improve the site security by blocking malicious requests, preventing SQL injection attacks, mitigating cross-site scripting (XSS) attacks, and enforcing security policies. A WAF can be deployed as a cloud service or as a device in front of the load balancer. A WAF is more suitable than an API gateway, an IPS/IDS, or a reverse proxy for the website architecture described in the question. References: [CompTIA Cloud+ CV0-003 Certification Study Guide], Chapter 9, Objective 9.1: Given a scenario, apply security controls and techniques.

NEW QUESTION 236
- (Topic 4)
During a security incident on an IaaS platform, which of the following actions will a systems administrator most likely take as part of the containment procedure?

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

Answer: B

Explanation:
Adding a deny rule to the network ACL is a common containment procedure for a security
incident on an IaaS platform, as it can isolate the affected instance from the rest of the network and prevent further compromise or data exfiltration. Connecting to an instance for triage, mirroring the traffic to perform a traffic capture, and performing a memory acquisition are more likely to be part of the analysis or evidence collection procedures, not the containment procedure.
References: CompTIA Cloud+ CV0-003 Exam Objectives, Objective 4.2: Given a scenario, apply security configurations and compliance controls ; Cloud Security Mitigation | Cloud Computing | CompTIA1

NEW QUESTION 240
- (Topic 3)
A cloud administrator would like to maintain file integrity checks through hashing on a cloud object store. Which of the following is MOST suitable from a performance perspective?

A. SHA-256
B. SHA-512
C. MD5

D. AES

Answer: C

Explanation:
The most suitable hashing algorithm from a performance perspective to maintain file integrity checks on a cloud object store is MD5 (Message Digest 5). MD5 is a hashing algorithm that generates a 128-bit hash value for any given input data. MD5 is faster and more efficient than other hashing algorithms, such as SHA-256 or SHA-512, which generate longer hash values and require more computational resources. MD5 can be used to verify the integrity of files by comparing their hash values before and after transmission or storage. Reference: CompTIA Cloud+ Certification Exam Objectives, Domain 2.0 Security, Objective 2.5 Given a scenario, apply data security techniques in the cloud.

NEW QUESTION 243
- (Topic 3)
A cloud engineer is performing updates to an application and needs to gracefully stop any new transactions from processing before the updates can be applied. Which of the following steps should the engineer take?

A. Enable maintenance mode from the application dashboard
B. Wait until after business hours to conduct the change when the system is not in use
C. Run a kill command on the system to stop the application services
D. Use a load balancer to redirect traffic to other systems serving the application

Answer: A

Explanation:
The best way to gracefully stop any new transactions from processing before applying updates to an application is to enable maintenance mode from the application dashboard. Maintenance mode is a feature that allows temporarily disabling the access or functionality of an application or service while performing maintenance tasks, such as updates, patches, or backups. It also displays a message or notification to the users or clients informing them about the maintenance and the expected downtime. This method will prevent any new transactions from being initiated or interrupted while the updates are being applied. Reference: [CompTIA Cloud+ Certification Exam Objectives], Domain 3.0 Maintenance, Objective 3.1 Given a scenario, apply appropriate changes to meet performance, security and user requirements.

NEW QUESTION 247
.....

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