CompTIA

Exam Questions CV0-003

CompTIA Cloud+ Certification Exam

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

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

Answer: D

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

NEW QUESTION 2
- (Topic 1)
A cloud administrator is reviewing the authentication and authorization mechanism implemented within the cloud environment. Upon review, the administrator discovers the sales group is part of the finance group, and the sales team members can access the financial application. Single sign-on is also implemented, which makes access much easier.
Which of the following access control rules should be changed?

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

Answer: D

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

NEW QUESTION 3
- (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 4
- (Topic 1)
A SAN that holds VM files is running out of storage space.
Which of the following will BEST increase the amount of effective storage on the SAN?

A. Enable encryption
B. Increase IOPS
C. Convert the SAN from RAID 50 to RAID 60
D. Configure deduplication

Answer: D

Explanation:

Deduplication is a type of data compression technique that eliminates redundant or duplicate data blocks or segments in a storage system or device. Configuring deduplication can help increase the amount of effective storage on a SAN that holds VM files and is running out of storage space, as it can reduce the storage space consumption and increase the storage space utilization by storing only unique data blocks or segments. Configuring deduplication can also improve performance and efficiency, as it can speed up data transfer and backup processes and save network bandwidth and power consumption. References: CompTIA Cloud+ Certification Exam Objectives, page 9, section 1.4

NEW QUESTION 5
- (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 6
- (Topic 1)
An organization is implementing a new requirement to facilitate users with faster downloads of corporate application content. At the same time, the organization is also expanding cloud regions.
Which of the following would be suitable to optimize the network for this requirement?

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

Answer: C

Explanation:

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

NEW QUESTION 7
- (Topic 1)
A cloud administrator is switching hosting companies and using the same script that was previously used to deploy VMs in the new cloud. The script is returning errors that the command was not found.
Which of the following is the MOST likely cause of the script failure?

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

Answer: C

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

NEW QUESTION 8
- (Topic 1)
A technician is working with an American company that is using cloud services to provide
video-based training for its customers. Recently, due to a surge in demand, customers in Europe are experiencing latency.
Which of the following services should the technician deploy to eliminate the latency issue?

A. Auto-scaling
B. Cloud bursting
C. A content delivery network
D. A new cloud provider

Answer: C

Explanation:
https://www.cloudflare.com/learning/cdn/what-is-a-cdn/

"A content delivery network (CDN) refers to a geographically distributed group of servers which work together to provide fast delivery of Internet content."

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

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

Answer: C

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

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

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

Answer: A

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

NEW QUESTION 10
- (Topic 1)
A systems administrator notices that a piece of networking equipment is about to reach its end of support.
Which of the following actions should the administrator recommend?

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

Answer: D

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

NEW QUESTION 15
- (Topic 1)
A global web-hosting company is concerned about the availability of its platform during an upcoming event. Web traffic is forecasted to increase substantially during the next week. The site contains mainly static content.
Which of the following solutions will assist with the increased workload?

A. DoH
B. WAF
C. IPS
D. CDN

Answer: D

Explanation:
A content delivery network (CDN) is a distributed network of servers that delivers web content to users based on their geographic location, origin server, and content delivery server. A CDN can assist with the increased workload caused by sudden continuous bursts of traffic, as it can reduce the load on the origin server by caching and serving static content from edge servers closer to the users. A CDN can also improve the performance and availability of web content delivery, as it can reduce latency, bandwidth consumption, and network congestion. References: CompTIA Cloud+ Certification Exam Objectives, page 12, section 2.2
Reference: https://www.globaldots.com/content-delivery-network-explained

NEW QUESTION 20
- (Topic 1)
A systems administrator needs to configure a set of policies to protect the data to comply with mandatory regulations.
Which of the following should the administrator implement to ensure DLP efficiently prevents the exposure of sensitive data in a cloud environment?

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

Answer: C

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

NEW QUESTION 24
- (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 26
- (Topic 1)
In an existing IaaS instance, it is required to deploy a single application that has different versions.
Which of the following should be recommended to meet this requirement?

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

Answer: A

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

NEW QUESTION 31
- (Topic 1)
A company needs to rehost its ERP system to complete a datacenter migration to the public cloud. The company has already migrated other systems and configured VPN connections.
Which of the following MOST likely needs to be analyzed before rehosting the ERP?

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

Answer: D

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

NEW QUESTION 36
- (Topic 1)
A cloud administrator is reviewing a new application implementation document. The administrator needs to make sure all the known bugs and fixes are applied, and unwanted
ports and services are disabled.
Which of the following techniques would BEST help the administrator assess these business requirements?

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

Answer: D

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

NEW QUESTION 37
- (Topic 1)
Which of the following is relevant to capacity planning in a SaaS environment?

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

Answer: D

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

NEW QUESTION 42
- (Topic 1)
A cloud architect wants to minimize the risk of having systems administrators in an IaaS compute instance perform application code changes. The development group should be the only group allowed to modify files in the directory.
Which of the following will accomplish the desired objective?

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

Answer: B

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

NEW QUESTION 43
- (Topic 1)
A company just successfully completed a DR test and is ready to shut down its DR site and resume normal operations.
Which of the following actions should the cloud administrator take FIRST?

A. Initiate a failover
B. Restore backups
C. Configure the network
D. Perform a failback

Answer: D

Explanation:
A failback is a process of restoring or returning a system or service to its original state or location after a failure or disaster recovery event. Performing a failback is the first action that a cloud administrator should take after successfully completing a DR test and being ready to shut down its DR site and resume normal operations, as it can ensure that all data and configurations are synchronized and consistent between the primary site and the DR site before switching back to the primary site. Performing a failback can also help minimize downtime or disruption, as it can verify that all systems or services
are functioning properly before resuming normal operations. References: CompTIA Cloud+ Certification Exam Objectives, page 10, section 1.5

NEW QUESTION 47
- (Topic 2)
A cloud administrator is managing an organization's infrastructure in a public cloud. All servers are currently located in a single virtual network with a single firewall

that all traffic must pass through. Per security requirements, production, QA, and development servers should not be able to communicate directly with each other. Which of the following should an administrator perform to comply with the security requirement?

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

Answer: A

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

NEW QUESTION 49
- (Topic 2)
A systems administrator is using a configuration management tool to perform maintenance tasks in a system. The tool is leveraging the target system's API to perform these maintenance tasks After a number of features and security updates are applied to the target system, the configuration management tool no longer works as expected. Which of the following is the MOST likely cause of the issue?

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

Answer: A

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

NEW QUESTION 53
- (Topic 2)
A systems administrator is deploying a new cloud application and needs to provision cloud services with minimal effort. The administrator wants to reduce the tasks required for maintenance, such as OS patching, VM and volume provisioning, and autoscaling configurations. Which of the following would be the BEST option to deploy the new application?

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

Answer: D

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

NEW QUESTION 56
- (Topic 2)
Which of the following should be considered for capacity planning?

A. Requirements, licensing, and trend analysis
B. Laws and regulations
C. Regions, clusters, and containers

D. Hypervisors and scalability

Answer: A

Explanation:
These are the factors that should be considered for capacity planning in a cloud environment. Capacity planning is a process of estimating and allocating the necessary resources and performance to meet the current and future demands of cloud applications or services. Capacity planning can help to optimize costs, efficiency, and reliability of cloud resources or services. The factors that should be considered for capacity planning are:
? Requirements: These are the specifications or expectations of the cloud applications or services, such as functionality, availability, scalability, security, etc. Requirements can help to determine the type, amount, and quality of resources or services needed to meet the objectives and goals of the cloud applications or services.
? Licensing: This is the agreement or contract that grants customers the right to use or access certain cloud resources or services for a specific period or fee. Licensing can affect the cost, availability, and compliance of cloud resources or services. Licensing can help to determine the budget, duration, and scope of using or accessing cloud resources or services.
? Trend analysis: This is the technique of analyzing historical and current data to identify patterns, changes, or fluctuations in demand or usage of cloud resources or services. Trend analysis can help to predict and anticipate future demand or usage of cloud resources or services, as well as identify any opportunities or challenges that may arise.

NEW QUESTION 61
- (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 62
- (Topic 2)
A cloud administrator is building a new VM for machine-learning training. The developer requesting the VM has stated that the machine will need a full GPU dedicated to it.
Which of the following configuration options would BEST meet this requirement?

A. Virtual GPU
B. External GPU
C. Passthrough GPU
D. Shared GPU

Answer: C

Explanation:
Reference: https://blogs.vmware.com/apps/2018/09/using-gpus-with-virtual-machines-on- vsphere-part-2-vmdirectpath-i-o.html
Passthrough GPU is a configuration option that allows a VM to access a physical GPU directly without any virtualization layer or sharing mechanism. This provides the VM with full and exclusive access to the GPU resources and performance. Passthrough GPU is suitable for applications that require intensive graphics processing or machine learning training.

NEW QUESTION 66
- (Topic 2)
A database analyst reports it takes two hours to perform a scheduled job after onboarding 10,000 new users to the system. The analyst made no changes to the scheduled job before or after onboarding the users. The database is hosted in an IaaS instance on a cloud provider. Which of the following should the cloud administrator evaluate to troubleshoot the performance of the job?

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

Answer: A

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

NEW QUESTION 67
- (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 70
- (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 73
- (Topic 2)
A private IaaS administrator is receiving reports that all newly provisioned Linux VMs are running an earlier version of the OS than they should be. The administrator reviews the automation scripts to troubleshoot the issue and determines the scripts ran successfully. Which of the following is the MOST likely cause of the issue?

A. API version incompatibility
B. Misconfigured script account
C. Wrong template selection
D. Incorrect provisioning script indentation

Answer: C

Explanation:
The wrong template selection is the most likely cause of the issue of newly provisioned Linux VMs running an earlier version of OS than they should be in a private IaaS environment. A template is a preconfigured image or blueprint of a VM that contains an OS, applications, settings, etc., that can be used to create new VMs quickly and consistently. A template may have different versions or updates depending on when it was created or modified. If a template is selected incorrectly or not updated properly, it may result in creating VMs with an older or different version of OS than expected.

NEW QUESTION 75
- (Topic 2)
A company is currently running a website on site. However, because of a business requirement to reduce current RTO from 12 hours to one hour, and the RPO from one day to eight hours, the company is considering operating in a hybrid environment. The website uses mostly static files and a small relational database. Which of the following should the cloud architect implement to achieve the objective at the LOWEST cost possible?

A. Implement a load-balanced environment in the cloud that is equivalent to the current on- premises setup and use DNS to shift the load from on premises to cloud.
B. Implement backups to cloud storage and infrastructure as code to provision the environment automatically when the on-premises site is dow
C. Restore the data from the backups.
D. Implement a website replica in the cloud with auto-scaling using the smallest possible footprin
E. Use DNS to shift the load from on premises to the cloud.
F. Implement a CDN that caches all requests with a higher TTL and deploy the laaS instances manually in case of disaste
G. Upload the backup on demand to the cloud to restore on the new instances.

Answer: C

Explanation:
This is the best solution to achieve the objective of reducing current RTO (Recovery Time Objective) from 12 hours to one hour, and RPO (Recovery Point Objective) from one day to eight hours, at the lowest cost possible, for a website that uses mostly static files and a small relational database. RTO is a metric that measures how quickly a system or service can be restored after a disruption or disaster. RPO is a metric that measures how much data can be lost or how far back in time a recovery point can be without causing significant impact or damage. To reduce RTO and RPO, the administrator should implement a website replica in the cloud with auto-scaling using the smallest possible footprint. A website replica is a copy or backup of a website that can be used for recovery or failover purposes. Auto-scaling is a feature that allows cloud resources or systems to adjust their capacity and performance according to demand or workload. Using auto-scaling with the smallest possible footprint can minimize costs by using only the necessary resources and scaling up or down as needed. The administrator should also use DNS (Domain Name System) to shift the load from on premises to the cloud. DNS is a service that translates domain names into IP addresses and vice versa. Using DNS, the administrator can redirect traffic from the on-premises website to the cloud replica in case of a disruption or disaster, and vice versa when

recovery is complete.

NEW QUESTION 79
- (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 84
- (Topic 2)
A cloud administrator would like to deploy a cloud solution to its provider using automation techniques. Which of the following must be used? (Choose two.)

A. Auto-scaling
B. Tagging
C. Playbook
D. Templates
E. Containers
F. Serverless

Answer: CD

Explanation:
Playbook and templates are two things that must be used to deploy a cloud solution to its provider using automation techniques. A playbook is a file or script that defines a set of tasks or actions to be executed on one or more cloud resources or systems. A playbook can automate and standardize the deployment and configuration of cloud solutions using tools such as Ansible, Chef, Puppet, etc. A template is a preconfigured image or blueprint of a cloud resource or system that contains an OS, applications, settings, etc., that can be used to create new resources or systems quickly and consistently. A template can simplify and speed up the deployment of cloud solutions using tools such as AWS CloudFormation, Azure Resource Manager, Google Cloud Deployment Manager, etc.

NEW QUESTION 86
- (Topic 2)
A systems administrator 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 87
- (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 92
- (Topic 2)

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

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

Answer: C

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

NEW QUESTION 96
- (Topic 2)
A DevOps administrator is designing a new machine-learning platform. The application needs to be portable between public and private clouds and should be kept as small as possible. Which of the following approaches would BEST meet these requirements?

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

Answer: D

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

NEW QUESTION 97
- (Topic 2)
A technician is trying to delete six decommissioned VMs. Four VMs were deleted without issue. However, two of the VMs cannot be deleted due to an error. Which of the following would MOST likely enable the technician to delete the VMs?

A. Remove the snapshots
B. Remove the VMs' IP addresses
C. Remove the VMs from the resource group
D. Remove the lock from the two VMs

Answer: D

Explanation:
Removing the lock from the two VMs is what would most likely enable the technician to delete the VMs that cannot be deleted due to an error. A lock is a feature that prevents certain actions or operations from being performed on a resource or service, such as deleting, modifying, moving, etc. A lock can help to protect a resource or service from accidental or unwanted changes or removals. Removing the lock from the two VMs can enable the technician to delete them by allowing the delete action or operation to be performed on them.

NEW QUESTION 101
- (Topic 2)
A systems administrator wants to verify the word "qwerty" has not been used as a password on any of the administrative web consoles in a network. Which of the following will achieve this goal?

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

Answer: C

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

NEW QUESTION 102
- (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 107
- (Topic 2)
An organization suffered a critical failure of its primary datacenter and made the decision to switch to the DR site. After one week of using the DR site, the primary datacenter is now ready to resume operations.
Which of the following is the MOST efficient way to bring the block storage in the primary datacenter up to date with the DR site?

A. Set up replication.
B. Copy the data across both sites.
C. Restore incremental backups.
D. Restore full backups.

Answer: A

Explanation:
Reference: https://www.ibm.com/docs/en/cloud-pak-system-w3550/2.3.3?topic=system- administering-block-storage-replication
Setting up replication is the most efficient way to bring the block storage in the primary datacenter up to date with the DR site after a critical failure. Replication is a process of copying data from one location to another in real-time or near real-time. Replication can be synchronous or asynchronous, depending on the latency and bandwidth requirements. Replication can ensure data consistency and availability across multiple sites and facilitate faster recovery.

NEW QUESTION 108
- (Topic 2)
A development team recently completed testing changes to a company's web-based CMS in the sandbox environment. The cloud administrator deployed these CMS application changes to the staging environment as part of the next phase in the release life cycle. The deployment was successful, but after deploying the CMS application, the web page displays an error message stating the application is unavailable. After reviewing the application logs, the administrator sees an error message that the CMS is unable to connect to the database. Which of the following is the BEST action for the cloud administrator to perform to resolve the issue?

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

Answer: D

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

NEW QUESTION 112
- (Topic 2)
A company had a system compromise, and the engineering team resolved the issue after 12 hours. Which of the following information will MOST likely be requested by the Chief Information Officer (CIO) to understand the issue and its resolution?

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

Answer: A

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

etc.

NEW QUESTION 115
- (Topic 2)
Users of a public website that is hosted on a cloud platform are receiving a message indicating the connection is not secure when landing on the website. The administrator has found that only a single protocol is opened to the service and accessed through the URL https://www.comptiasite.com. Which of the following would MOST likely resolve the issue?

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

Answer: A

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

NEW QUESTION 118
- (Topic 2)
A systems administrator is about to deploy a new VM to a cloud environment. Which of the following will the administrator MOST likely use to select an address for the VM?

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

Answer: D

Explanation:
IPAM (IP Address Management) is what the administrator will most likely use to select an address for the new VM that is about to be deployed to a cloud environment. IPAM is a tool or service that allows customers to plan, track, and manage the IP addresses and DNS names of their cloud resources or systems. IPAM can help to select an address for the new VM by providing information such as available IP addresses, IP address ranges, subnets, domains, etc., as well as ensuring that the address is unique and valid.

NEW QUESTION 123
- (Topic 1)
A web server has been deployed in a public IaaS provider and has been assigned the public IP address of 72.135.10.100. Users are now reporting that when they browse to the website, they receive a message indicating the service is unavailable. The cloud administrator logs into the server, runs a netstat command, and notices the following relevant output:

```
TCP  17.3.130.3:0 72.135.10.100:5500 TIME_WAIT
TCP  17.3.130.3:0 72.135.10.100:5501 TIME_WAIT
TCP  17.3.130.3:0 72.135.10.100:5502 TIME_WAIT
TCP  17.3.130.3:0 72.135.10.100:5503 TIME_WAIT
TCP  17.3.130.3:0 72.135.10.100:5504 TIME_WAIT
```

Which of the following actions should the cloud administrator take to resolve the issue?

A. Assign a new IP address of 192.168.100.10 to the web server
B. Modify the firewall on 72.135.10.100 to allow only UDP
C. Configure the WAF to filter requests from 17.3.130.3
D. Update the gateway on the web server to use 72.135.10.1

Answer: D

Explanation:
Updating the gateway on the web server to use 72.135.10.1 is the best action to take to resolve the issue of the web server being unavailable after being deployed in a public IaaS provider and assigned the public IP address of 72.135.10.100. Updating the gateway can ensure that the web server can communicate with the Internet and other networks by using the correct router or device that connects the web server's network to other networks. Updating the gateway can also improve performance and reliability, as it can avoid any routing errors or conflicts that may prevent the web server from responding to remote login requests.
References: CompTIA Cloud+ Certification Exam Objectives, page 15, section 2.8

NEW QUESTION 124
- (Topic 1)
An organization purchased new servers with GPUs for render farms. The servers have limited CPU resources.
Which of the following GPU configurations will be the MOST optimal for virtualizing this environment?

A. Dedicated
B. Shared
C. Passthrough

D. vGPU

Answer: C

Explanation:
Passthrough is a type of GPU configuration that allows a VM to directly access a physical GPU on the host system without any virtualization layer or sharing mechanism. Passthrough can provide optimal performance and compatibility for GPU- intensive applications, such as rendering or gaming, as it eliminates any overhead or contention caused by virtualization or sharing. Passthrough is also suitable for servers with limited CPU resources, as it reduces the CPU load and offloads the graphics processing to the GPU. Passthrough is the most optimal GPU configuration for virtualizing a new server with GPUs for render farms.
References: CompTIA Cloud+ Certification Exam Objectives, page 11, section 1.6

NEW QUESTION 127
- (Topic 1)
A developer is no longer able to access a public cloud API deployment, which was working ten minutes prior.
Which of the following is MOST likely the cause?

A. API provider rate limiting
B. Invalid API token
C. Depleted network bandwidth
D. Invalid API request

Answer: A

Explanation:
API provider rate limiting 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 provider rate limiting can cause a failure to access a public cloud API deployment, as it can reject or block any requests that exceed the limit. API provider rate limiting can be used by cloud providers to control the usage and traffic of their customers and prevent overloading or abuse of their resources. API provider rate limiting is the most likely cause for the developer being unable to access a public cloud API deployment that was working ten minutes prior.
References: CompTIA Cloud+ Certification Exam Objectives, page 13, section 2.5

NEW QUESTION 132
- (Topic 1)
A cloud architect is designing the VPCs for a new hybrid cloud deployment. The business requires the following:
? High availability
? Horizontal auto-scaling
? 60 nodes peak capacity per region
? Five reserved network IP addresses per subnet
? /24 range
Which of the following would BEST meet the above requirements?

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

Answer: C

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

NEW QUESTION 136
- (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 140

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

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

Answer: D

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

NEW QUESTION 143
- (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 144
- (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 146
- (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 151
- (Topic 1)

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

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

Answer: B

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

NEW QUESTION 152
- (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 154
- (Topic 1)
A systems administrator for an e-commerce company will be migrating the company's main
website to a cloud provider. The principal requirement is that the website must be highly available.
Which of the following will BEST address this requirement?

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

Answer: B

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

NEW QUESTION 156
- (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 159
- (Topic 4)
A cloud administrator must ensure all servers are in compliance with the company's security policy Which of the following should the administrator check FIRST?

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

Answer: C

Explanation:
Hardened baselines are a set of security best practices that reduce the vulnerability of a system to exploits by reducing its attack surface1. They are also known as security configurations or benchmarks, and they provide a standard level of system hardening for an organization23.
Checking the hardened baselines of the servers is the first step that a cloud administrator should take to ensure compliance with the company's security policy. This is because hardened baselines can help to:
Identify and eliminate common vulnerabilities and exposures (CVEs) that attackers can exploit1.
Remove unnecessary or unused services, accounts, software, and ports that can increase the attack surface23.
Apply appropriate settings and controls for encryption, authentication, authorization, firewall, and logging23.
Streamline audits and testing by reducing complexity and providing a reliable benchmark23.

NEW QUESTION 160
- (Topic 4)
A web consultancy group currently works in an isolated development environment. The group uses this environment for the creation of the final solution, but also for showcasing it to customers, before commissioning the sites in production. Recently, customers of newly commissioned sites have reported they are not receiving the final product shown by the group, and the website is performing in unexpected ways. Which of the following additional environments should the group adopt and include in its process?

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

Answer: C

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

NEW QUESTION 162
- (Topic 4)
A systems administrator is reviewing the logs from a company's IDS and notices a large amount of outgoing traffic from a particular server. The administrator then runs a scan on the server, which detects malware that cannot be removed. Which of the following should the administrator do first?

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

Answer: B

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

NEW QUESTION 163
- (Topic 4)
A cloud engineer is migrating a customer's web servers from a hypervisor platform to a CSP environment. The engineer needs to decouple the infrastructure and components during the migration to reduce the single points of failure. Which of the following storage options should the cloud engineer migrate the content to in order to improve availability?

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

Answer: C

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

NEW QUESTION 165
- (Topic 4)
A cloud administrator needs to deploy a security virtual appliance in a private cloud environment, but this appliance will not be part of the standard catalog of items for other users to request. Which of the following is the BEST way to accomplish this task?

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

Answer: C

Explanation:
The correct answer is C. Import the virtual appliance into the environment and deploy it as a VM.
A virtual appliance is a pre-packaged and pre-configured software solution that runs on a virtual machine (VM). A virtual appliance typically consists of an operating system, an application, and any required dependencies, and is designed to provide a specific function or service. A virtual appliance can be distributed as a single file or a set of files that can be imported into a virtualization platform, such as VMware, Hyper-V, or KVM .
A cloud administrator can deploy a security virtual appliance in a private cloud environment by importing the virtual appliance into the environment and deploying it as a VM. This is the best way to accomplish this task because it preserves the original configuration and functionality of the virtual appliance, and does not require any additional installation or customization. The cloud administrator can also control the access and visibility of the virtual appliance, and prevent other users from requesting it from the standard catalog of items .
Creating an empty VM, importing the hard disk of the virtual appliance, and configuring the CPU and memory is not the best way to accomplish this task because it involves more steps and complexity than importing the virtual appliance as a whole. It also introduces the risk of losing or corrupting some data or settings during the import process, or misconfiguring the CPU and memory for the virtual appliance.
Acquiring the build scripts from the vendor and recreating the appliance using the baseline templates is not the best way to accomplish this task because it involves more time and effort than importing the virtual appliance directly. It also depends on whether the vendor provides the build scripts or not, and whether they are compatible with the baseline templates or not.
Converting the virtual appliance to a template and deploying a new VM using the template is not the best way to accomplish this task because it adds an unnecessary step of creating a template from the virtual appliance. It also does not prevent other users from accessing or requesting the template from the catalog of items.

NEW QUESTION 170
- (Topic 4)
A systems administrator needs to connect the companys network to a public cloud services provider. Which of the following will BEST ensure encryption in transit for data transfers?

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

Answer: B

Explanation:
The answer is A. SAML. SAML (Security Assertion Markup Language) is a standard for exchanging authentication and authorization data between different parties, such as a user and a service provider. In a federated cluster, SAML can be used to enable single sign-on (SSO) for users across multiple clusters or cloud providers. SAML relies on the exchange of XML-based assertions that contain information about the user's identity, attributes, and entitlements. If the users' API access tokens have become invalid, it could be because the SAML assertions have expired, been revoked, or corrupted. The administrator should check the SAML configuration and logs to determine the cause of this issue.
Some possible sources of information about SAML and federated clusters are:
? Authenticating | Kubernetes: This page provides an overview of authenticating users in Kubernetes, including using SAML for federated identity.
? Authenticating to the Kubernetes API server - Google Cloud: This page explains how to authenticate to the Kubernetes API server on Google Cloud, including using SAML for federated identity with Google Cloud Identity Platform.
? Error 403 User not authorized when trying to access Azure Databricks API through Active Directory - Stack Overflow: This page discusses a similar issue of users getting an error when trying to access Azure Databricks API using SAML and Active Directory.

NEW QUESTION 173
- (Topic 4)
A systems administrator deployed a new web application in a public cloud and would like to test it, but the company's network firewall is only allowing outside connections to the cloud provider network using TCP port 22. While waiting for the network administrator to open the required ports, which of the following actions should the systems administrator take to test the new application? (Select two).

A. Create an IPSec tunnel.
B. Create a VPN tunnel.
C. Open a browser using the default gateway IP address.
D. Open a browser using the localhost IP address.
E. Create a GRE tunnel.
F. Create a SSH tunnel.

Answer: BF

Explanation:
To test the new web application in the public cloud, the systems administrator should create a replica database, synchronize the data, and switch to the new instance, and create a SSH tunnel. Creating a replica database can help minimize the downtime and ensure data consistency during the migration. Synchronizing the data can help keep the replica database up to date with the original database. Switching to the new instance can help activate the new web application in the public cloud. Creating a SSH tunnel can help bypass the network firewall and access the web application using TCP port 22. SSH is a secure protocol that can create encrypted tunnels between the local and remote hosts. By creating a SSH tunnel, the systems administrator can forward the web application traffic through the tunnel and test it using a web browser. 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 cloud engineer is deploying a server in a cloud platform. The engineer reviews a security scan report. Which of the following recommended services should be disabled? (Select TWO).

A. Telnet
B. FTP
C. Remote login
D. DNS
E. DHCP
F. LDAP

Answer: AB

Explanation:
Telnet and FTP are two services that should be disabled on a cloud server because they are insecure and vulnerable to attacks. Telnet and FTP use plain text to transmit data over the network, which means that anyone who can intercept the traffic can read or modify the data, including usernames, passwords, commands, files, etc. This can lead to data breaches, unauthorized access, or malicious actions on the server1.
Instead of Telnet and FTP, more secure alternatives should be used, such as SSH (Secure Shell) and SFTP (Secure File Transfer Protocol). SSH and SFTP use encryption to protect the data in transit and provide authentication and integrity checks for the communication. SSH and SFTP can prevent eavesdropping, tampering, or spoofing of the data and ensure the confidentiality and privacy of the server2.
The other options are not services that should be disabled on a cloud server:
? Option C: Remote login. Remote login is a service that allows users to access a remote server from another location using a network connection. Remote login can be useful for managing, configuring, or troubleshooting a cloud server without having to physically access it. Remote login can be secured by using encryption, authentication, authorization, and logging mechanisms3.
? Option D: DNS (Domain Name System). DNS is a service that translates human- friendly domain names into IP addresses that can be used to communicate over the Internet. DNS is essential for resolving the names of the cloud resources and services that are hosted on the cloud platform. DNS can be secured by using DNSSEC (DNS Security Extensions), which add digital signatures to DNS records to verify their authenticity and integrity.
? Option E: DHCP (Dynamic Host Configuration Protocol). DHCP is a service that assigns IP addresses and other network configuration parameters to devices on a network. DHCP can simplify the management of IP addresses and avoid conflicts or errors in the network. DHCP can be secured by using DHCP snooping, which filters out unauthorized DHCP messages and prevents rogue DHCP servers from assigning IP addresses.
? Option F: LDAP (Lightweight Directory Access Protocol). LDAP is a service that stores and organizes information about users, devices, and resources on a network. LDAP can provide identity management and access control for the cloud environment. LDAP can be secured by using LDAPS (LDAP over SSL/TLS), which encrypts the LDAP traffic and provides authentication and integrity checks.

NEW QUESTION 178
- (Topic 4)
A cloud administrator needs to verify domain ownership with a third party. The third party has provided a secret that must be added to the DNS server. Which of the following DNS records does the administrator need to update to include the secret?

A. NS
B. TXT
C. AAAA
D. SOA

Answer: B

Explanation:
TXT is a type of DNS record that can store arbitrary text data, such as a secret, a verification code, or a configuration parameter. TXT records are often used to verify domain ownership with a third party, such as a certificate authority, an email service provider, or a cloud service provider. The third party can check the TXT record of the domain and compare it with the secret they provided to confirm the identity and authority of the domain owner .

NEW QUESTION 180
- (Topic 4)
An integration application that communicates between different application and database servers is currently hosted on a physical machine. A P2V migration needs to be done to reduce the hardware footprint. Which of the following should be considered to maintain the same level of network throughput and latency in the virtual server?

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

Answer: C

Explanation:
SR-IOV stands for Single Root I/O Virtualization, which is a technology that allows a physical network adapter to be partitioned into multiple virtual functions (VFs) that can be directly assigned to virtual machines (VMs). This way, the network traffic bypasses the software layer of the hypervisor and the virtual switch, and goes directly from the VM to the physical adapter. This reduces the CPU overhead, the network latency, and the packet loss, and improves the network throughput and

scalability. SR-IOV can achieve near-native performance for network-intensive applications, such as an integration application that communicates between different application and database servers. By enabling SR-IOV capability on the physical server and the virtual server, the P2V migration can maintain the same level of network throughput and latency as the original physical machine. References: High performance network virtualization with SR-IOV; Supercharge Your Network Throughput via Single Root I/O Virtualization (SR-IOV); Overview of Single Root I/O Virtualization (SR-IOV).

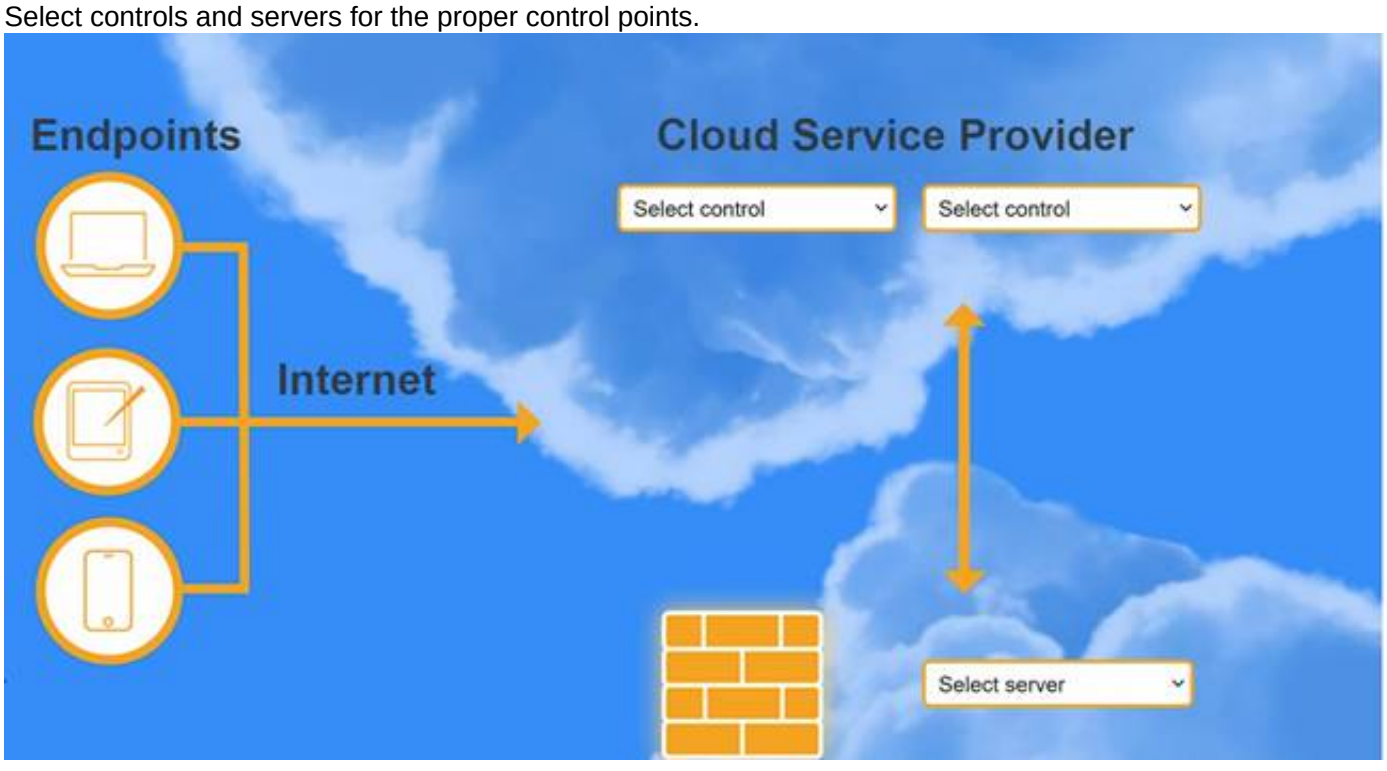
NEW QUESTION 184
- (Topic 4)
A company has a web application running in an on-premises environment that needs to be migrated to the cloud. The company wants to implement a solution that maximizes scalability, availability, and security, while requiring no infrastructure administration. Which of the following services would be BEST to meet this goal?

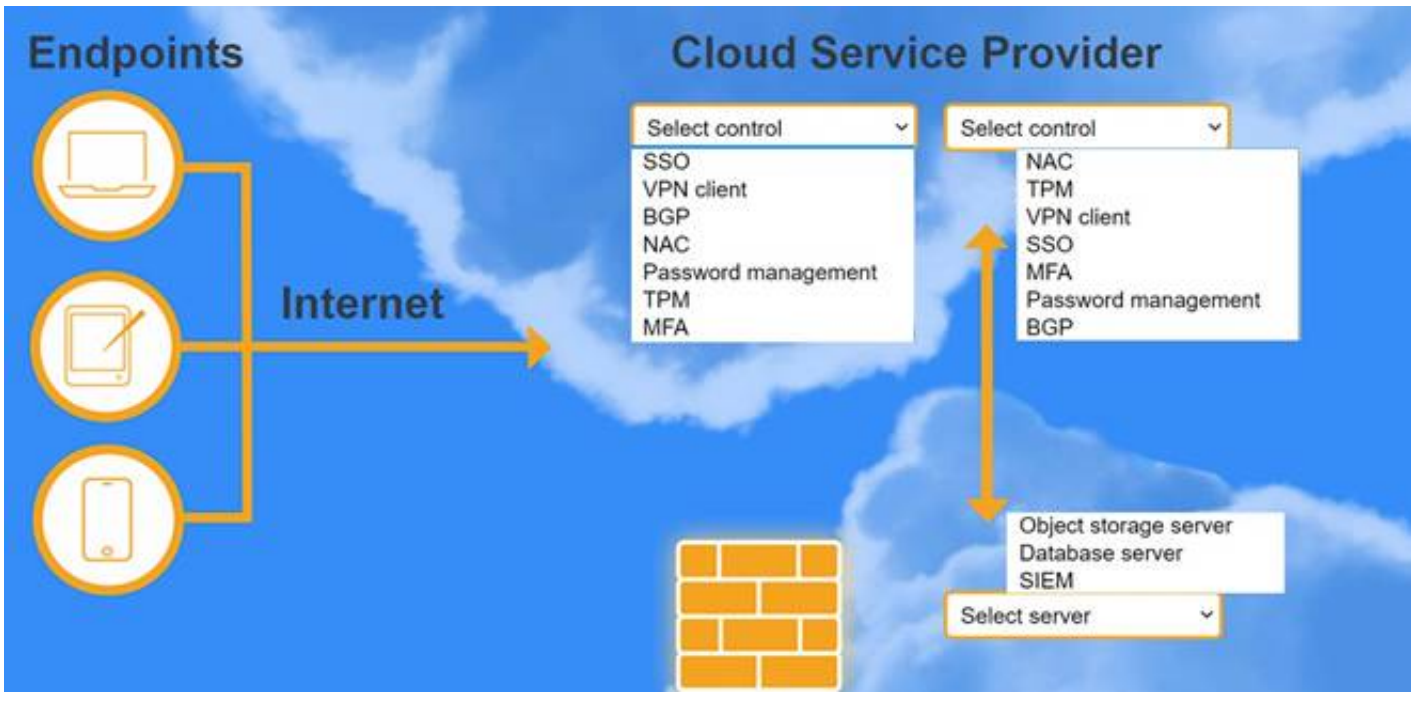
A. A PaaS solution
B. A hybrid solution
C. An laaS solution
D. A SaaS solution

Answer: A

Explanation:
A PaaS solution, or platform as a service, is a cloud computing service that provides a complete, ready-to-use, cloud-hosted platform for developing, running, maintaining and managing applications1. A PaaS solution would meet the company's goal of maximizing scalability, availability, and security, while requiring no infrastructure administration, because:
Scalability: A PaaS solution can automatically scale up or down the resources needed to run the application based on the demand and traffic. The company does not need to worry about provisioning or managing servers, storage, network, or load balancers23.
Availability: A PaaS solution can ensure high availability and reliability of the application by replicating it across multiple regions and zones. The company does not need to worry about backup, recovery, or failover23.
Security: A PaaS solution can provide built-in security features such as encryption, authentication, authorization, and firewall. The company does not need to worry about installing or updating security patches or software23.
No infrastructure administration: A PaaS solution can abstract away the underlying infrastructure and hardware from the company. The company only needs to focus on developing and deploying the application code and data. The PaaS provider takes care of the rest23.
A hybrid solution (B) is a cloud computing service that combines on-premises and cloud resources. It may offer some benefits such as flexibility and cost optimization, but it would not meet the company's goal of requiring no infrastructure administration. The company would still need to manage and maintain the on-premises part of the solution4.
An IaaS solution ©, or infrastructure as a service, is a

NEW QUESTION 189
HOTSPOT - (Topic 4)
A highly regulated business is required to work remotely, and the risk tolerance is very low. You are tasked with providing an identity solution to the company cloud that includes the following:
? secure connectivity that minimizes user login
? tracks user activity and monitors for anomalous activity
? requires secondary authentication
INSTRUCTIONS
Select controls and servers for the proper control points.

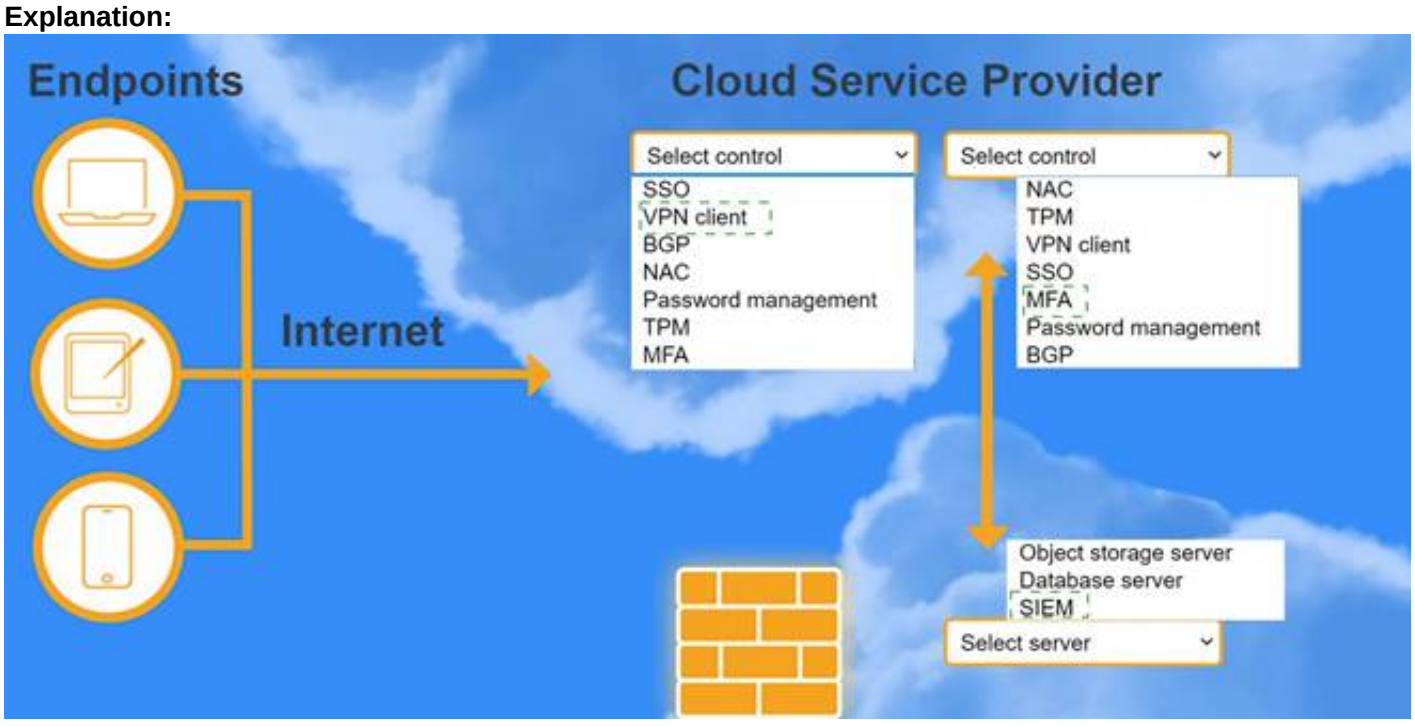




A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 191
- (Topic 4)
A systems administrator is planning to migrate to a cloud solution with volume-based licensing. Which of the following is most important when considering licensing costs?

A. The number of cores
B. The number of threads
C. The number of machines
D. The number of sockets

Answer: C

Explanation:
Volume-based licensing is a model where the cost of the software is based on the number of licenses purchased1. This model is commonly used for software that is installed on a specific number of devices, such as antivirus software or office productivity suites1. Therefore, the number of machines is the most important factor when considering licensing costs in this model.
References: CompTIA Cloud+ CV0-003 Exam Objectives, Objective 1.2: Given a scenario, compare and contrast various cloud service models ; Cloud+ Exam CV0-003: CompTIA Cloud+ Licensing Models1

NEW QUESTION 193
- (Topic 4)
A systems administrator is configuring a cloud solution for a vulnerability assessment to test the company's resources that are hosted in a public cloud. The solution must test the company's resources from an external user's perspective. Which of the following should the systems administrator configure?

A. An agent-based scan
B. A network-based scan
C. A port scan
D. A credentialed scan

Answer: B

Explanation:
A network-based scan is a type of vulnerability assessment that tests the security of a system or a network from an external user's perspective, without requiring any software or credentials on the target. A network-based scan can identify vulnerabilities such as open ports, misconfigured firewalls, outdated software, or exposed services .

NEW QUESTION 195
- (Topic 4)
A systems administrator has a redundant backup system in place. Which of the following should the systems administrator perform to maintain efficient operation and comply with the global standard in the corporate backup policies?

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

Answer: C

NEW QUESTION 200
- (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 201
- (Topic 4)
An organization is deploying development, quality assurance, and production environments with equal numbers of IP addresses to the cloud. The IP address range provided is 10.168.0.0/24, and it needs to be terminated on a firewall. Which of the following IP subnets and firewall IPS should be used for one of the environments?

A. 10.168.0.0/26 and 10.168.0.63
B. 10.168.0.64/26 and 10.168.0.64
C. 10.168.0.128/26 and 10.168.0.190
D. 10.168.0.128/26 and 10.168.0.194
E. 10.168.0.192/26 and 10.168.0.191

Answer: A

Explanation:
The IP address range 10.168.0.0/24 can be divided into four equal subnets of 64 addresses each by using a /26 mask. The subnets are 10.168.0.0/26, 10.168.0.64/26, 10.168.0.128/26, and 10.168.0.192/26. The last address in each subnet is the broadcast address, and the second-last address can be used as the gateway address for that subnet. Therefore, one of the possible subnets and firewall IPs for one of the environments is 10.168.0.0/26 and 10.168.0.63.
References: [CompTIA Cloud+ Study Guide], page 178.

NEW QUESTION 206
- (Topic 4)
An organization provides integration services for finance companies that use web services. A new company that sends and receives more than 100,000

transactions per second has
been integrated using the web service. The other integrated companies are now reporting slowness with regard to the integration service. Which of the following is the cause of the issue?

A. Incorrect configuration in the authentication process
B. Incorrect configuration in the message queue length
C. Incorrect configuration in user access permissions
D. Incorrect configuration in the SAN storage pool

Answer: B

Explanation:
The correct answer is B. Incorrect configuration in the message queue length.
A message queue is a data structure that stores messages or requests that are sent and received by web services. A message queue allows asynchronous communication between web services, as it decouples the sender and the receiver, and enables them to process messages at different rates. A message queue also provides reliability, scalability, and load balancing for web services, as it ensures that messages are not lost, duplicated, or corrupted, and that they are distributed evenly among the available servers .
However, a message queue also has a limit on how many messages it can store at a time. This limit is determined by the configuration of the message queue length, which is the maximum number of messages that can be in the queue before it becomes full. If the message queue length is too short, the queue may fill up quickly and reject new messages, causing errors or delays in communication. If the message queue length is too long, the queue may consume too much memory or disk space, affecting the performance or availability of the web service .
Therefore, if an organization provides integration services for finance companies that use web services, and a new company that sends and receives more than 100,000 transactions per second has been integrated using the web service, the most likely cause of the issue is an incorrect configuration in the message queue length. The new company may have generated a large volume of messages that exceeded the capacity of the message queue, resulting in slowness for the other integrated companies. The organization should adjust the message queue length to accommodate the increased traffic and optimize the resource utilization of the web service.

NEW QUESTION 208
- (Topic 4)
A new development team requires workstations hosted in a PaaS to develop a new website. Members of the team also require remote access to the workstations using their corporate email addresses. Which of the following solutions will best meet these requirements? (Select two).

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

Answer: CD

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

NEW QUESTION 211
- (Topic 4)
A cloud administrator has received a physical disk that was analyzed by the incident response team. Which of the following documents should the cloud administrator update?

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

Answer: A

Explanation:
A. Chain of custody
A chain of custody is a document that records the sequence of custody, control, transfer, analysis, and disposition of physical or electronic evidence. A chain of custody is important to ensure the integrity and admissibility of evidence in legal cases. A cloud administrator who receives a physical disk that was analyzed by the incident response team should update the chain of custody to document when, how, and by whom the disk was handled, and what actions were performed on it12.
An incident taxonomy is a classification system that provides additional information about an incident, such as the nature, impact, intent, root cause, and data exposed. An incident taxonomy is useful for identifying trends and patterns, but it does not track the movement or manipulation of evidence3.
A risk register is a document that identifies, records, and assesses potential risks in a project or an organization. A risk register helps to prioritize and mitigate risks, and to develop contingency plans. A risk register is not directly related to the analysis of a physical disk by the incident response team4.
An incident playbook is a document that provides a series of prescriptive steps and guidance for responding and resolving incidents. An incident playbook helps to simplify and standardize the response process, and to reduce human error. An incident playbook does not record the details or outcomes of the response actions5.

NEW QUESTION 213
- (Topic 4)
Different healthcare organizations have agreed to collaborate and build a cloud infrastructure that should minimize compliance costs and provide a high degree of security and privacy, as per regulatory requirements. This is an example of a:

A. private cloud.

B. community cloud.
C. hybrid cloud.
D. public cloud.

Answer: B

Explanation:
The correct answer is B. Community cloud.
A community cloud is a cloud deployment model that involves a shared infrastructure among several organizations that have common interests, goals, or requirements. A community cloud can provide a high degree of security, privacy, and compliance, as well as cost savings and efficiency, for the participating organizations. A community cloud can be managed by one or more of the organizations, or by a third-party service provider .
A private cloud is a cloud deployment model that involves a dedicated infrastructure for a single organization. A private cloud can provide a high degree of control, customization, and security for the organization, but it may also incur higher costs and complexity. A private cloud can be managed by the organization itself, or by a third-party service provider.
A hybrid cloud is a cloud deployment model that involves a combination of two or more different cloud models, such as private, public, or community clouds. A hybrid cloud can provide the benefits of both models, such as scalability, flexibility, and cost-effectiveness, as well as address the challenges of each model, such as security, compliance, and performance. A hybrid cloud can be managed by the organization itself, or by one or more service providers .
A public cloud is a cloud deployment model that involves a shared infrastructure for multiple organizations or individuals. A public cloud can provide a high degree of scalability, accessibility, and affordability for the users, but it may also pose some risks in terms of security, privacy, and compliance. A public cloud is managed by a third-party service provider .

NEW QUESTION 215
- (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 216
- (Topic 4)
A cloud administrator created four VLANs to autoscale the container environment. Two of the VLANs are on premises, while two VLANs are on a public cloud provider with a direct link between them. Firewalls are between the links with an additional subnet for communication, which is 192.168.5.0/24.
The on-premises gateways are:
* 192.168.1.1/24
* 192.168.2.1/24
The cloud gateways are:
* 192.168.3.1/24
* 192.168.4.1/24
The orchestrator is unable to communicate with the cloud subnets. Which Of the following should the administrator do to resolve the issue?

A. Allow firewall traffic to 192.168.5.0/24.
B. Set both firewall interfaces to 192.168.5.1/24.
C. Add interface 192.168.3.1/24 on the local firewall.
D. Add interface 192.168.1.1/24 on the cloud firewall.

Answer: A

Explanation:
To allow communication between the on-premises and cloud subnets, the firewall traffic should be allowed to pass through the additional subnet for communication, which is 192.168.5.0/24. This subnet acts as a bridge between the two networks and should have firewall rules that permit traffic from and to both sides.
References: [CompTIA Cloud+ Study Guide], page 181.

NEW QUESTION 218
- (Topic 4)
A company plans to publish a new application and must conform with security standards. Which of the following types of testing are most important for the systems administrator to run to assure the security and compliance of the application before publishing? (Select two).

A. Regression testing
B. Vulnerability testing
C. Usability testing
D. Functional testing
E. Penetration testing
F. Load testing

Answer: BE

Explanation:
Vulnerability testing and penetration testing are two types of security testing that can help to identify and mitigate potential risks in an application before publishing. Vulnerability testing is the process of scanning the application for known weaknesses or flaws that could be exploited by attackers. Penetration testing is the process of simulating real-world attacks on the application to test its defenses and find vulnerabilities that may not be detected by automated scans. Both types of testing can help to assure the security and compliance of the application by revealing and resolving any issues that could compromise the confidentiality, integrity, or availability of the application or its
data. References: CompTIA Cloud+ CV0-003 Study Guide, Chapter 5: Maintaining a Cloud Environment, page 221.

NEW QUESTION 221
- (Topic 4)
A cloud engineer recently set up a container image repository. The engineer wants to ensure that downloaded images are not modified in transit. Which of the following is the best method to achieve this goal?

A. SHA-256
B. IPSec
C. AES-256
D. MD5
E. serpent-256

Answer: A

Explanation:
SHA-256 is the best method to ensure that downloaded images are not modified in transit. SHA-256 is a type of cryptographic hash function that can generate a unique and fixed- length digest for any input data. The digest can be used to verify the integrity and
authenticity of the data, as any modification or tampering of the data would result in a different digest. SHA-256 is more secure and reliable than MD5, which is an older and weaker hash function that has been proven to be vulnerable to collisions and attacks12. AES-256 and serpent-256 are types of encryption algorithms, not hash functions, and they are used to protect the confidentiality of the data, not the integrity. IPSec is a network security protocol that can use encryption and hashing to secure data in transit, but it is not a method by itself

NEW QUESTION 223
- (Topic 4)
A systems administrator has verified that a physical switchport that is connected to a virtualization host is using all available bandwidth. Which of the following would best address this issue?

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

Answer: B

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

NEW QUESTION 228
- (Topic 4)
A cloud administrator is troubleshooting an issue regarding users at one location who are reporting that their API access tokens have become invalid. The users are issued tokens based on their credentials in a federated cluster. Which of the following should the administrator check to determine the cause of this issue?

A. SAML
B. DNS
C. SSL
D. NTP

Answer: A

Explanation:
The answer is A. SAML. SAML (Security Assertion Markup Language) is a standard for exchanging authentication and authorization data between different parties, such as a user and a service provider. In a federated cluster, SAML can be used to enable single sign-on (SSO) for users across multiple clusters or cloud providers. SAML relies on the exchange of XML-based assertions that contain information about the user's identity, attributes, and entitlements. If the users' API access tokens have become invalid, it could be because the SAML assertions have expired, been revoked, or corrupted. The administrator should check the SAML configuration and logs to determine the cause of this issue.
Some possible sources of information about SAML and federated clusters are:
? Authenticating | Kubernetes: This page provides an overview of authenticating users in Kubernetes, including using SAML for federated identity.
? Authenticating to the Kubernetes API server - Google Cloud: This page explains how to authenticate to the Kubernetes API server on Google Cloud, including using SAML for federated identity with Google Cloud Identity Platform.
? Error 403 User not authorized when trying to access Azure Databricks API through Active Directory - Stack Overflow: This page discusses a similar issue of users getting an error when trying to access Azure Databricks API using SAML and Active Directory.

NEW QUESTION 230
- (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 235
- (Topic 4)
A cloud administrator is supporting an application that has several reliability issues. The administrator needs visibility into the performance characteristics of the application. Which of the following will MOST likely be used in a reporting dashboard?

A. Data from files containing error messages from the application
B. Results from the last performance and workload testing
C. Detail log data from syslog files of the application
D. Metrics and time-series data measuring key performance indicators

Answer: D

Explanation:
The best answer is D. Metrics and time-series data measuring key performance indicators.
Metrics and time-series data are numerical values that represent the state and behavior of a system over time. They can measure key performance indicators (KPIs) such as availability, latency, throughput, error rate, and resource utilization. Metrics and time-series data can help a cloud administrator to monitor, analyze, and troubleshoot the performance characteristics of an application .
Metrics and time-series data are most likely to be used in a reporting dashboard, because they can provide a clear and concise overview of the application's performance. A reporting dashboard is a graphical user interface that displays the most important information about a system or a process in a single view. A reporting dashboard can help a cloud administrator to:
Visualize the trends and patterns of the metrics and time-series data using charts, graphs, tables, or gauges .
Compare the actual performance of the application with the expected or desired performance based on the defined service level objectives (SLOs) or service level agreements (SLAs) .
Identify and diagnose any performance issues or anomalies that may affect the reliability of the application .
Communicate and report the performance status and results to the stakeholders or customers.
The other options are not as likely to be used in a reporting dashboard, because they are either too detailed, too outdated, or too irrelevant for measuring the performance characteristics of the application. For example:
Data from files containing error messages from the application (A) may help to identify and debug some specific errors or exceptions that occur in the application. However, they are not sufficient to measure the overall performance or reliability of the application. They are also too verbose and unstructured to be displayed in a reporting dashboard.
Results from the last performance and workload testing (B) may help to evaluate and optimize the performance of the application under different scenarios and conditions. However, they are not representative of the current or real-time performance of the application in production. They are also too static and outdated to be displayed in a reporting dashboard.
Detail log data from syslog files of the application © may help to record and track the events and activities that happen in the application. However, they are not designed to measure the key performance indicators or metrics of the application. They are also too complex and voluminous to be displayed in a reporting dashboard.

NEW QUESTION 236
- (Topic 4)
A cloud engineer is troubleshooting RSA key-based authentication from a local computer to a cloud-based server, which is running SSH service on a default port. The following file permissions are set on the authorized keys file:
-rw-rw-rw-1 ubuntu ubuntu 391 Mar S 01:36 authorized _ keys
Which Of the following security practices are the required actions the engineer Should take to gain access to the server? (Select TWO).

A. Fix the file permissions with execute permissions to the owner of the file.
B. Open port 21 access for the computer's public IP address.
C. Fix the file permissions with read-only access to the owner Of the file.
D. Open port 22 access for the computer's public IP address.
E. Open port 21 access for 0.0.0.0/0 CIDR.
F. open port 22 access for 0.0.0.0/0 CIDR.

Answer: CD

Explanation:
The correct answer is C and D.
* C. Fix the file permissions with read-only access to the owner of the file.
* D. Open port 22 access for the computer's public IP address.
The authorized_keys file on the server should have read-only access for the owner of the file, and no access for anyone else. This ensures that only the owner can read the public keys that are authorized to log in, and no one can modify or delete them. The file permissions can be fixed with the command chmod 400 ~/.ssh/authorized_keys on the server. This is a recommended security practice for SSH key-based authentication123. The computer that wants to log in to the server using SSH key-based authentication needs to have access to port 22 on the server, which is the default port for SSH service. This can be done by opening port 22 access for the computer's public IP address on the server's firewall or security group settings. This allows the computer to initiate an SSH connection to the server and authenticate with its private key. Opening port 21, which is used for FTP service, is not relevant or secure for SSH key-based authentication1.

NEW QUESTION 241
FILL IN THE BLANK - (Topic 4)
?MISSING?

A.

Answer: D

Explanation:
This means that data is divided into blocks and written across multiple disks, and two additional disks are used to store parity information that can be used to reconstruct data in case of disk failure. RAID 6 can withstand the failure of up to two disks without losing any data or performance. RAID 6 also maximizes the storage capacity of its drives, as it only uses two disks for parity out of the total number of disks in the array. For example, if the array has 10 disks, RAID 6 will use 8 disks for data and 2 disks for parity, resulting in a storage capacity of 8/10 or 80% of the total disk space. RAID 6 is suitable for private cloud environments that require high availability, fault tolerance, and large storage
capacity. References: CompTIA Cloud+ CV0-003 Study Guide, Chapter 3: Storage Technologies, Section 3.2: RAID Levels, Page 125

NEW QUESTION 244
- (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 248
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

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