

Exam Questions CV0-004

CompTIA Cloud+

<https://www.2passeasy.com/dumps/CV0-004/>



NEW QUESTION 1

An on-premises data center is located in an earthquake-prone location. The workload consists of real-time, online transaction processing. Which of the following data protection strategies should be used to back up on-premises data to the cloud while also being cost effective?

- A. Remote replication for failover
- B. A copy that is RAID 1 protected on spinning drives in an on-premises private cloud
- C. A full backup to on-site tape libraries in a private cloud
- D. Air-gapped protection to provide cyber resiliency

Answer: A

Explanation:

Remote replication for failover is the data protection strategy that should be used to back up on-premises data to the cloud for an earthquake-prone location. It provides real-time or near-real-time copying of data to a remote location, which can be quickly activated in case the primary site fails. References: Disaster recovery strategies, including remote replication for failover, are part of the cloud-based data protection methods covered in the CompTIA Cloud+ certification.

NEW QUESTION 2

A cloud engineer is running a latency-sensitive workload that must be resilient and highly available across multiple regions. Which of the following concepts best addresses these requirements?

- A. Cloning
- B. Clustering
- C. Hardware passthrough
- D. Stand-alone container

Answer: B

Explanation:

Clustering refers to the use of multiple servers/computers to form what appears to be a single system. This concept is key for achieving high availability and resilience, especially for latency-sensitive workloads. By distributing the workload across a cluster that spans multiple regions, the system can continue to operate even if one or more nodes fail, thus maintaining performance and availability. References: CompTIA Cloud+ Guide to Cloud Computing (ISBN: 978-1-64274-282-2)

NEW QUESTION 3

Which of the following is a difference between a SAN and a NAS?

- A. A SAN works only with fiber-based networks.
- B. A SAN works with any Ethernet-based network.
- C. A NAS uses a faster protocol than a SAN
- D. A NAS uses a slower protocol than a SAN.

Answer: D

Explanation:

A NAS (Network Attached Storage) typically uses file-level protocols such as NFS or SMB, which are generally considered slower and less efficient than the block-level protocols used by SANs (Storage Area Networks), such as iSCSI or Fibre Channel. SANs are designed for high performance and low latency, making them more suitable for applications requiring fast and efficient storage access.

NEW QUESTION 4

Which of the following will best reduce the cost of running workloads while maintaining the same performance? (Select two).

- A. Instance size
- B. Tagging
- C. Reserved resources model
- D. Spot instance model
- E. Pay-as-you-go model
- F. Dedicated host model

Answer: CD

Explanation:

The Reserved resources model offers cost savings for committed use over a long term, which can reduce costs while maintaining performance for predictable workloads. The Spot instance model allows users to take advantage of unused capacity at lower prices, offering significant cost savings, though with the possibility of instances being terminated when demand rises. Both models can be strategically used to optimize costs without compromising performance.

NEW QUESTION 5

An organization wants to ensure its data is protected in the event of a natural disaster. To support this effort, the company has rented a colocation space in another part of the country. Which of the following disaster recovery practices can be used to best protect the data?

- A. On-site
- B. Replication
- C. Retention
- D. Off-site

Answer: D

Explanation:

For an organization looking to protect its data in the event of a natural disaster, the best disaster recovery practice would be off-site replication. By renting a colocation space in another part of the country, the company can maintain copies of their data and critical systems in a geographically separate location, ensuring they are not affected by the same disaster. References: CompTIA Cloud+ Study Guide (Exam CV0-004) - Chapter on Disaster Recovery

NEW QUESTION 6

A systems administrator needs to configure a script that will monitor whether an application is healthy and stop the VM if an unsuccessful code is returned. Which of the following scripts should the systems administrator use to achieve this goal?

- A.

```
RESPONSE_CODE }string APP_URLbool RESPONSE_CODEstring VMhealth checker (APP_URL, VM) {if [ http_probe (APP_URL) == 200] { echo RESPONSE_CODE }else{ stop (VM) echo
```
- B.

```
else{ echostring APP_URLfloat RESPONSE_CODE string VMhealth_checker (APP_URL, VM) {if [ http_probe (APP_URL) == 200] { stop (RESPONSE_CODE)echo VM } stop (VM)RESPONSE CODE }
```
- C.

```
else{ echostring APP_URLint RESPONSE CODEstring VMhealth checker (APP_URL, VM) {if [ http_probe (APP_URL) == 200] { echo RESPONSE_CODE }stop (VM) RESPONSE_CODE }
```
- D.

```
else{ echostring APP_URLint RESPONSE_CODEstring VMhealth_checker (APP_URL, VM) { if [ http_probe (VM) == 200] { stop (VM)echo RESPONSE_CODE } RESPONSE CODE }
```

Answer: A

Explanation:

Script A is designed to monitor the health of an application by checking its response code. If the application returns a 200 (OK) status, it indicates that the application is healthy. Otherwise, the script will stop the VM to address the issue, which is a common approach to handle unhealthy application states in automated environments. This script effectively achieves the goal of monitoring application health and taking corrective action when an unsuccessful code is returned. References: CompTIA Cloud+ resources and general scripting practices for cloud environments

NEW QUESTION 7

A company experienced a data leak through its website. A security engineer, who is investigating the issue, runs a vulnerability scan against the website and receives the following output:

```
Nmap scan report for www.example.com (93.184.216.34)
Host is up (0.020s latency).
```

```
PORT STATE SERVICE
21/tcp open  ftp
443/tcp open  ssl/https
1119/tcp closed bnetgame
1935/tcp closed rtmp
```

Which of the following is the most likely cause of this leak?

- A. RTMP port open
- B. SQL injection
- C. Privilege escalation
- D. Insecure protocol

Answer: D

Explanation:

The data leak is most likely caused by the use of an insecure protocol. The vulnerability scan output shows that port 21/tcp for FTP (File Transfer Protocol) is open. FTP is known for transmitting data unencrypted, which could allow sensitive data to be intercepted during transfer. References: The security risks associated with the use of insecure or unencrypted protocols are covered under cloud security best practices in the CompTIA Cloud+ curriculum.

NEW QUESTION 8

A DevOps engineer is integrating multiple systems. Each system has its own API that exchanges data based on different application-level transactions. Which of the following delivery mechanisms would best support this integration?

- A. Enterprise service bus
- B. Socket
- C. RPC
- D. Queue

Answer: A

Explanation:

An Enterprise Service Bus (ESB) is designed to facilitate application integration by providing a centralized architecture for high-level, message-based, and event-driven communication between different systems. It is particularly well-suited for integrating multiple systems with their own APIs because it can handle various data formats and protocols, enabling different applications to communicate with each other seamlessly. References: CompTIA Cloud+ Certification Study Guide (Exam CV0-004) by Scott Wilson and Eric Vanderburg

NEW QUESTION 9

An DevOps engineer is receiving reports that users can no longer access the company's web application after hardening of a web server. The users are receiving the following error:

ERR_SSLJ/ERSION_OR_CIPHER_MISMATCH.

Which of the following actions should the engineer take to resolve the issue?

- A. Restart the web server.
- B. Configure TLS 1.2 or newer.
- C. Update the web server.
- D. Review logs on the WAF

Answer: B

Explanation:

To resolve the ERR_SSL_VERSION_OR_CIPHER_MISMATCH error after hardening a web server, the engineer should configure the server to use TLS 1.2 or newer. This error often occurs when the server or client supports an outdated version of SSL/TLS or incompatible cipher suites. Updating to a modern, secure version of TLS ensures compatibility and enhances security. References: The CompTIA Cloud+ certification includes governance, risk, compliance, and security for the cloud, emphasizing the importance of implementing up-to-date security protocols like TLS to protect data in transit and ensure secure communications in cloud environments.

NEW QUESTION 10

Which of the following are best practices when working with a source control system? (Select two).

- A. Merging code often
- B. Pushing code directly to production
- C. Performing code deployment
- D. Maintaining one branch for all features
- E. Committing code often
- F. Initiating a pull request

Answer: AE

Explanation:

Best practices when working with a source control system include merging code often to ensure that changes from different team members are integrated regularly, reducing integration issues. Committing code often is also recommended to save small changes frequently, which helps in tracking changes and resolving issues more effectively. References: Source control system best practices are part of the software development and deployment guidelines discussed in the CompTIA Cloud+ examination objectives.

NEW QUESTION 10

Which of the following requirements are core considerations when migrating a small business's on-premises applications to the cloud? (Select two).

- A. Availability
- B. Hybrid
- C. Testing
- D. Networking
- E. Compute
- F. Logs

Answer: AD

Explanation:

When migrating on-premises applications to the cloud for a small business, availability and networking are core considerations. Ensuring that applications are available and that the network is capable of handling the new cloud traffic are pivotal for a successful transition. References: The migration process and its core considerations, including availability and networking, are topics within the Business Principles of Cloud Environments in the CompTIA Cloud+ material.

NEW QUESTION 11

A cloud infrastructure administrator updated the IP tables to block incoming connections and outgoing responses to 104.225.110.203. Which of the following vulnerability management steps is this an example of?

- A. Scanning scope
- B. Remediation
- C. Identification
- D. Assessment

Answer: B

Explanation:

Updating the IP tables to block connections to a specific IP address as a response to vulnerabilities is an example of remediation. Remediation involves taking direct action to fix vulnerabilities, such as by applying patches, changing configurations, or, in this case, updating firewall rules to block potentially harmful traffic. References: CompTIA Cloud+ resources and vulnerability management processes

NEW QUESTION 16

Which of the following is the most cost-effective and efficient strategy when migrating to the cloud?

- A. Retire
- B. Replatform
- C. Retain
- D. Refactor

Answer: A

Explanation:

The most cost-effective and efficient strategy when migrating to the cloud can often be to 'retire' or turn off legacy systems that are no longer useful or necessary. This avoids spending resources on migrating and maintaining systems that do not provide value in a cloud environment. References: Cloud migration strategies, including retiring outdated systems, are part of the decision-making process for cloud adoption in the CompTIA Cloud+ certification material.

NEW QUESTION 21

A company is developing a new web application that requires a relational database management system with minimal operational overhead. Which of the following should the company choose?

- A. A database installed on a virtual machine
- B. A managed SQL database on the cloud
- C. A database migration service
- D. A hybrid database setup

Answer: B

Explanation:

For a new web application that requires a relational database management system with minimal operational overhead, the company should choose a managed SQL database on the cloud. Managed databases provide automated backups, patching, and other management tasks, reducing the administrative burden. References: The use of managed services, like managed databases, to minimize operational overhead is a strategic decision in cloud computing covered in CompTIA Cloud+.

NEW QUESTION 22

Which of the following is the most cost-effective way to store data that is infrequently accessed?

- A. Cold site
- B. Hot site
- C. Off-site
- D. Warm site

Answer: C

Explanation:

The most cost-effective way to store data that is infrequently accessed is typically an off-site storage service, often referred to as cold or archival storage. This type of storage is designed for data that is rarely accessed, providing lower storage costs. References: Data storage solutions and their cost implications, including off-site (cold or archival) storage for infrequently accessed data, are part of the cloud storage options discussed in CompTIA Cloud+.

NEW QUESTION 24

A company that has several branches worldwide needs to facilitate full access to a specific cloud resource to a branch in Spain. Other branches will have only read access. Which of the following is the best way to grant access to the branch in Spain?

- A. Set up MFA for the users working at the branch.
- B. Create a network security group with required permissions for users in Spain.
- C. Apply a rule on the WAF to allow only users in Spain access to the resource.
- D. Implement an IPS/IDS to detect unauthorized users.

Answer: B

Explanation:

The best way to grant full access to a specific cloud resource to a branch in Spain, while other branches have only read access, is to create a network security group with the required permissions. This group can be configured to allow full access to users within the branch's IP range while restricting others to read-only access. References: CompTIA Cloud+ Study Guide (Exam CV0-004) - Chapter on Security Configuration

NEW QUESTION 28

A cloud engineer wants to implement a disaster recovery strategy that:

- . Is cost-effective.
- . Reduces the amount of data loss in case of a disaster.
- . Enables recovery with the least amount of downtime.

Which of the following disaster recovery strategies best describes what the cloud engineer wants to achieve?

- A. Cold site
- B. Off site
- C. Warm site
- D. Hot site

Answer: D

Explanation:

A hot site is a disaster recovery strategy that is cost-effective, minimizes data loss, and allows for the fastest recovery time in case of a disaster. It is an exact replica of the original site of the organization, with full computer systems as well as near-complete backups of user data. Hot sites are operational 24/7 and can take over functionality from the primary site immediately or with minimal delay. References: CompTIA Cloud+ Study Guide (Exam CV0-004) - Chapter on Disaster Recovery

NEW QUESTION 29

A cloud engineer is provisioning a new application that requires access to the organization's public cloud resources. Which of the following is the best way for the

cloud engineer to authenticate the application?

- A. Access key
- B. API
- C. MFA token
- D. Username and Password

Answer: A

Explanation:

The best way to authenticate an application requiring access to an organization's public cloud resources is through the use of an access key. Access keys provide a secure means of authentication for applications and services without the need for interactive login credentials. This method is particularly useful for automated processes or applications that need to interact with cloud services programmatically, ensuring secure and efficient access control. References: CompTIA Cloud+ content emphasizes the importance of secure authentication mechanisms, such as access keys, in managing and securing access to cloud resources, aligning with best practices for cloud security and application deployment.

NEW QUESTION 30

SIMULATION

A company hosts various containerized applications for business uses. A client reports that one of its routine business applications fails to load the web-based login prompt hosted in the company cloud. Click on each device and resource. Review the configurations, logs, and characteristics of each node in the architecture to diagnose the issue. Then, make the necessary changes to the WAF configuration to remediate the issue.



Web app 1			
SVC_Host	SVC_Name	SVC IP	SVC_Port
webapp1	FIN	10.22.10.11	443

Web app 2			
SVC_Host	SVC_Name	SVC IP	SVC_Port
webapp2	VIDEO	10.22.10.21	443

Web app 3			
SVC_Host	SVC_Name	SVC IP	SVC_Port
webapp3	API	10.22.10.31	443

Web app 4			
SVC_Host	SVC_Name	SVC IP	SVC_Port
webapp4	CHAT	10.22.10.41	443

WAF				
Edit config		WAF logs		
Rule ID	Description	Service	Action	Availability zone
1001	Brute force attempt	^https://webapp[.]compta[.]org/\$	Block	A
1002	Botnet	^https://webapp[.]compta[.]org/\$	Block	A
1003	API web server	^https://webapp3[.]compta[.]org/([0-9A-Za-z]([0-9A-Za-z_?]*))*\$	Allow	B
1004	Chat web traffic	^https://webapp4[.]compta[.]org/chat/request[.]php\$	Allow	B
1005	Finance application 1	^https://webapp1[.]compta[.]org/([0-9A-Za-z]([0-9A-Za-z_?]*))*\$	Allow	B
1006	Finance application 2	^https://webapp1[.]compta[.]org/login[.]html\$	Block	A
1007	Video application	^https://webapp2[.]compta[.]org/video/stream\$	Allow	A

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

From the image, it's noticeable that some finance application rules are set to "Block" traffic. If the client's issue is with a finance-related application not loading the login prompt, these rules could be the cause.

The rule with ID 1005, labeled "Finance application 1", is configured to allow access to "webapp1" for finance-related paths. However, rule 1006, labeled "Finance application 2", is set to block access to "webapp1" for login-related paths.

To remediate the issue based on the WAF configuration you have provided, you would want to:

? Ensure that the correct paths to the finance application are allowed through the WAF.

? Modify any rules that are incorrectly blocking access to the application.

If the client's problem is specifically with the login prompt, then rule 1006 seems the most likely culprit. Changing the action from "Block" to "Allow" for rule 1006 could potentially resolve the client's issue. The rule should be carefully reviewed and updated to ensure legitimate traffic is not being blocked while still protecting against unauthorized access.

NEW QUESTION 33

A company just learned that the data in its object storage was accessed by an unauthorized party. Which of the following should the company have done to make the data unusable?

- A. The company should have switched from object storage to file storage.
- B. The company should have hashed the data.
- C. The company should have changed the file access permissions.
- D. The company should have encrypted the data at rest.

Answer: D

Explanation:

Encrypting the data at rest is a crucial security measure to make the data unusable to unauthorized parties. If the object storage data was accessed by an unauthorized party, having the data encrypted would ensure that the data remains confidential and inaccessible without the proper encryption keys, thus mitigating the impact of the breach.

References: CompTIA Cloud+ resources and data security practices

NEW QUESTION 38

A CI/CD pipeline is used to deploy VMs to an IaaS environment. Which of the following can be used to harden the operating system once the VM is running?

- A. Docker
- B. Kubernetes
- C. Git
- D. Ansible

Answer: D

Explanation:

Ansible can be used to harden the operating system once the VM is running. It is an automation tool that can configure systems, deploy software, and orchestrate more advanced IT tasks such as continuous deployments or zero downtime rolling updates. References: Ansible and other configuration management tools are part of the cloud management strategies discussed in the CompTIA Cloud+ certification material.

NEW QUESTION 42

A cloud engineer is extending on-premises services to a public cloud. The following design requirements must be considered in the overall solution:

" The ability to remotely connect systems from both environments

- No IP address conflicts or overlap
- Cost-effectiveness

Which of the following cloud network concepts best meets these requirements?

- A. Dedicated connection
- B. VPN
- C. VLAN
- D. ACL

Answer: B

Explanation:

A Virtual Private Network (VPN) is the most cost-effective solution for extending on-premises services to a public cloud while ensuring secure remote connectivity. VPNs can be configured to avoid IP address conflicts and overlap by using IP address translation and tunneling techniques, making them suitable for connecting disparate environments without significant changes to the existing network infrastructure.

NEW QUESTION 43

A company has one cloud-based web server that is prone to downtime during maintenance. Which of the following should the cloud engineer add to ensure high availability?

- A. A redundant web server behind a load balancer
- B. A backup cloud web server
- C. A secondary network link to the web server
- D. An autoscaling feature on the web server

Answer: A

Explanation:

Adding a redundant web server behind a load balancer is the solution that will ensure high availability. If one server goes down for maintenance, the other can take over, ensuring that the web service remains available without interruption. References: High availability concepts, including the use of load balancers and redundant servers, are part of cloud infrastructure design as per CompTIA Cloud+.

NEW QUESTION 46

A cloud administrator wants to provision a host with two VMs. The VMs require the following:

	Host	VM1	VM2
NIC	1Gbps	1Gbps	1Gbps
CPU	4	1	1
RAM	8	2	2
Storage (thin provisioned)	2TB	1.5TB	1.2TB
Storage utilization		22.5%	50%
Daily network traffic		1.2TB	200GB

After configuring the servers, the administrator notices that during certain hours of the day, the performance heavily degrades. Which of the following is the best explanation?

- A. The host requires additional physical CPUs.
- B. A higher number of processes occur at those times.
- C. The RAM on each VM is insufficient.
- D. The storage is overutilized.

Answer: C

Explanation:

Given the provided table, the VMs have been allocated 2GB of RAM each, which may be insufficient for their workload, especially during peak hours which could lead to performance degradation. Insufficient RAM can cause the VMs to use swap space on disk, which is significantly slower and can lead to poor performance. References: CompTIA Cloud+ Certification Study Guide (Exam CV0-004) by Scott Wilson and Eric Vanderburg.

NEW QUESTION 48

A security engineer recently discovered a vulnerability in the operating system of the company VMs. The operations team reviews the issue and decides all VMs need to be updated from version 3.4.0 to 3.4.1. Which of the following best describes the type of update that will be applied?

- A. Consistent
- B. Major
- C. Minor
- D. Ephemeral

Answer: C

Explanation:

The update from version 3.4.0 to 3.4.1 is considered a minor update, typically involving small bug fixes or security patches that do not include major feature changes or improvements. References: CompTIA Cloud+ Study Guide (Exam CV0-004) - Chapter on Systems Management

NEW QUESTION 53

A customer is migrating applications to the cloud and wants to grant authorization based on the classification levels of each system. Which of the following should the customer implement to ensure authorisation to systems is granted when the user and system classification properties match? (Select two).

- A. Resource tagging
- B. Discretionary access control
- C. Multifactor authentication
- D. Role-based access control
- E. Token-based authentication
- F. Bastion host

Answer: BD

Explanation:

Discretionary Access Control (DAC) and Role-Based Access Control (RBAC) are effective methods for granting authorization based on system classification levels. DAC allows resource owners to grant access rights, making it flexible for environments with varying classification levels. RBAC assigns permissions based on roles within an organization, aligning access rights with the user's job functions and ensuring that users access only what is necessary for their role, which can be mapped to system classifications. References: CompTIA Cloud+ content covers various access control models, emphasizing the importance of implementing appropriate security measures that align with organizational policies and classification levels to ensure secure and authorized access to cloud systems.

NEW QUESTION 54

Department supervisors have requested a report that will help them understand the utilization of cloud resources, make decisions about budgeting for the following year, and reduce costs. Which of the following are the most important requisite steps to create the report? (Select two).

- A. Set the desired retention of resource logs.
- B. Configure application tracing.
- C. Integrate email alerts with ticketing software.
- D. Enable resource tagging.
- E. Configure the collection of performance/utilization logs.
- F. Configure metric threshold alerts.

Answer: DE

Explanation:

To create a report that helps understand the utilization of cloud resources, make budget decisions, and reduce costs, the most important steps are to enable resource tagging and configure the collection of performance/utilization logs. Resource tagging helps in categorizing and tracking costs by associating tags with resources, while performance/utilization logs are essential for analyzing resource usage over time. References: CompTIA Cloud+ Study Guide (Exam CV0-004) - Chapter on Cloud Management

NEW QUESTION 57

An IT security team wants to ensure that the correct parties are informed when a specific user account is signed in. Which of the following would most likely allow an administrator to address this concern?

- A. Creating an alert based on user sign-in criteria
- B. Aggregating user sign-in logs from all systems
- C. Enabling the collection of user sign-in logs
- D. Configuring the retention of all sign-in logs

Answer: A

Explanation:

To ensure that the correct parties are informed when a specific user account is signed in, the best action is to create an alert based on user sign-in criteria. This alert can notify administrators or security personnel when the specified event occurs. References: Security monitoring and alerting are critical components of managing cloud environments securely, as discussed in the CompTIA Cloud+ certification.

NEW QUESTION 61

A software engineer is integrating an application to the cloud that is web socket based. Which of the following applications is the engineer most likely deploying?

- A. Image-sharing
- B. Data visualization
- C. Chat
- D. File transfer

Answer: C

Explanation:

A chat application is most likely to be deployed when integrating a web socket-based application to the cloud. Web sockets provide full-duplex communication channels over a single, long-lived connection, which is ideal for real-time applications like chat services that require persistent connections between the client and server for instant data exchange. References: CompTIA Cloud+ materials cover cloud networking concepts, emphasizing the importance of choosing the right technologies, like web sockets, for specific application requirements to ensure efficient and responsive cloud-based services.

NEW QUESTION 65

An administrator received a report that company data has been compromised. The compromise occurred on a holiday, and no one in the organization was working. While reviewing the logs from the holiday, the administrator noted the following details:

Account	Access	Details
Cloud administrator	Granted	Log-in granted
Software developer	Granted	Log-in granted
Software developer	Denied	Denied access to human resources folder
Security engineer	Granted	Log-in granted
Security engineer	Denied	Denied access to personnel files
Human resources manager	Granted	Log-in granted
Human resources manager	Granted	Access granted to human resources folder

The most appropriate action for the cloud security analyst to recommend is using CIS- hardened images. These images are pre-configured by the Center for

Internet Security to provide security benchmark standards that help in mitigating vulnerabilities in publicly available container images. References: CompTIA Cloud+ Study Guide (Exam CV0-004) - Chapter on Cloud Security Posture
Which of the following accounts should the administrator disable to prevent a further breach?

- A. Cloud administrator
- B. Human resources manager
- C. Security engineer
- D. Software developer

Answer: D

Explanation:

Based on the provided log details, the account of the Software Developer was used to gain unauthorized access. This account should be disabled to prevent further breaches, especially considering no one from the organization was working during the holiday, suggesting a compromised account. References: CompTIA Cloud+ Study Guide (Exam CV0-004) - Chapter on Cloud Security

NEW QUESTION 70

A developer at a small startup company deployed some code for a new feature to its public repository. A few days later, a data breach occurred. A security team investigated the incident and found that the database was hacked. Which of the following is the most likely cause of this breach?

- A. Database core dump
- B. Hard-coded credentials
- C. Compromised deployment agent
- D. Unpatched web servers

Answer: B

Explanation:

Hard-coded credentials within code, especially when deployed in a public repository, are a common security vulnerability. If credentials such as passwords or API keys are embedded in the code, anyone with access to the repository can potentially use them to gain unauthorized access to databases or other sensitive resources. This is a likely cause of the data breach in the scenario described. References: CompTIA Security+ Guide to Network Security Fundamentals by Mark Ciampa.

NEW QUESTION 73

An organization's security policy states that software applications should not exchange sensitive data in cleartext. The security analyst is concerned about a software application that uses Base64 to encode credit card data. Which of the following would be the best algorithm to replace Base64?

- A. 3DES
- B. AES
- C. RC4
- D. SHA-3

Answer: B

Explanation:

AES (Advanced Encryption Standard) is the best algorithm to replace Base64 for secure data exchange. Base64 is an encoding method that is not secure by itself, as it's easily reversible. AES, on the other hand, is a widely used encryption standard that ensures data is protected and is not readable without the correct encryption key. References: Encryption standards and practices, including the use of AES for securing data, are essential knowledge in cloud security covered in CompTIA Cloud+.

NEW QUESTION 77

Which of the following storage resources provides higher availability and speed for currently used files?

- A. Warm/HDD
- B. Cold/SSD
- C. Hot/SSD
- D. Archive/HDD

Answer: C

Explanation:

Hot storage using Solid State Drives (SSD) is designed for data that needs to be accessed frequently and quickly. SSDs provide faster access times compared to HDDs, making them suitable for high-availability and speed-critical files, such as those currently in use or requiring rapid access. References: CompTIA Cloud+ resources and storage tiering concepts

NEW QUESTION 81

A SaaS provider introduced new software functionality for customers as part of quarterly production enhancements. After an update is implemented, users cannot locate certain transactions from an inbound integration. During the investigation, the application owner finds the following error in the logs:

Error: REST API - Deprecated call is no longer supported in this release.

Which of the following is the best action for the application owner to take to resolve the issue?

- A. Update the custom integration to use a supported function.
- B. Include the custom integration in the quarterly testing scope.
- C. Ask the users to monitor the quarterly updates.
- D. Revert the application to the last stable quarterly release.

Answer: A

Explanation:

The error message indicates that the SaaS provider has deprecated a function that was previously called by the custom integration. The best action for the application owner to take is to update the custom integration to use a function that is supported in the current release. This is a direct solution to the problem and ensures the custom integration conforms to the updated SaaS provider's API. References: Based on the error message provided and standard practices for dealing with deprecated API calls in a SaaS environment.

NEW QUESTION 83

A cloud administrator needs to collect process-level, memory-usage tracking for the virtual machines that are part of an autoscaling group. Which of the following is the best way to accomplish the goal by using cloud-native monitoring services?

- A. Configuring page file/swap metrics
- B. Deploying the cloud-monitoring agent software
- C. Scheduling a script to collect the data
- D. Enabling memory monitoring in the VM configuration

Answer: B

Explanation:

To collect process-level, memory-usage tracking for virtual machines, deploying cloud- monitoring agent software is the best approach. The agent can gather detailed system metrics and send them to the cloud-native monitoring services for analysis and visualization. References: CompTIA Cloud+ Study Guide (Exam CV0-004) - Chapter on Cloud Monitoring

NEW QUESTION 87

A video surveillance system records road incidents and stores the videos locally before uploading them to the cloud and deleting them from local storage. Which of the following best describes the nature of the local storage?

- A. Persistent
- B. Ephemeral
- C. Differential
- D. Incremental

Answer: B

Explanation:

The nature of the local storage in a video surveillance system that records road incidents and stores the videos locally before uploading them to the cloud and deleting them from local storage is ephemeral. Ephemeral storage is temporary and is designed to provide short-term storage for information that changes frequently or is not meant to be persistent. References: CompTIA Cloud+ Study Guide (Exam CV0-004) - Chapter on Cloud Storage Options

NEW QUESTION 91

A cloud security analyst is concerned about security vulnerabilities in publicly available container images. Which of the following is the most appropriate action for the analyst to recommend?

- A. Using CIS-hardened images
- B. Using watermarked images
- C. Using digitally signed images
- D. Using images that have an application firewall

Answer: A

NEW QUESTION 94

A software engineer needs to transfer data over the internet using programmatic access while also being able to query the data. Which of the following will best help the engineer to complete this task?

- A. SQL
- B. Web sockets
- C. RPC
- D. GraphQL

Answer: D

Explanation:

GraphQL is the best option for transferring data over the internet with programmatic access and querying capabilities. It is a query language for APIs and a runtime for executing those queries with existing data, providing a more efficient, powerful, and flexible alternative to the REST API. References: Data transfer and querying methods are part of the technical knowledge associated with cloud computing, as included in CompTIA Cloud+.

NEW QUESTION 95

A government agency in the public sector is considering a migration from on premises to the cloud. Which of the following are the most important considerations for this cloud migration? (Select two).

- A. Compliance
- B. IaaS v
- C. SaaS
- D. Firewall capabilities
- E. Regulatory
- F. Implementation timeline
- G. Service availability

Answer: AD

Explanation:

For a government agency considering cloud migration, compliance and regulatory considerations are of utmost importance. The agency must ensure that the migration aligns with legal requirements, industry standards, and government regulations specific to the public sector. References: Compliance and regulatory considerations are crucial factors in the cloud migration process for government entities, as emphasized in the CompTIA Cloud+ certification.

NEW QUESTION 96

A company uses containers stored in Docker Hub to deploy workloads (or its IaaS infrastructure). The development team releases changes to the containers several times per hour. Which of the following should a cloud engineer do to prevent the proprietary code from being exposed to third parties?

- A. Use IaC to deploy the IaaS infrastructure.
- B. Convert the containers to VMs.
- C. Deploy the containers over SSH.
- D. Use private repositories for the containers.

Answer: D

Explanation:

To prevent proprietary code from being exposed to third parties, a cloud engineer should use private repositories for the containers. Private repositories ensure that access to container images is restricted and controlled, unlike public repositories where images are accessible to anyone. References: The concept of using private repositories for protecting proprietary code is part of cloud security best practices, which is covered under the Governance, Risk, Compliance, and Security domain of the CompTIA Cloud+ certification.

NEW QUESTION 101

A cloud engineer is designing a high-performance computing cluster for proprietary software. The software requires low network latency and high throughput between cluster nodes.

Which of the following would have the greatest impact on latency and throughput when designing the HPC infrastructure?

- A. Node placement
- B. Node size
- C. Node NIC
- D. Node OS

Answer: A

Explanation:

Node placement is critical in high-performance computing (HPC) clusters where low network latency and high throughput are required. Proper placement of nodes within the network infrastructure, including proximity to each other and to key network components, can significantly reduce latency and increase throughput. Ensuring that nodes are physically close and well-connected can facilitate faster data transfer rates between them. References: CompTIA Cloud+ Certification Study Guide (Exam CV0-004) by Scott Wilson and Eric Vanderburg

NEW QUESTION 106

The performance of an e-commerce website decreases dramatically during random periods. The IT team is evaluating available resources to mitigate the situation. Which of the following is the best approach to effectively manage this scenario?

- A. Migrating to a dedicated host
- B. Purchasing additional servers
- C. Scheduling resource allocation
- D. Configuring automatic elasticity

Answer: D

Explanation:

Configuring automatic elasticity is the best approach to manage an e-commerce website that experiences random performance drops due to variable traffic. Automatic elasticity enables the cloud resources to scale up or down automatically based on the current load, ensuring consistent performance even during unexpected traffic surges. References: The concept of automatic elasticity is part of the cloud management and technical operations content in the CompTIA Cloud+ curriculum.

NEW QUESTION 108

A company wants to combine solutions in a central and scalable environment to achieve the following goals:

- Control
- Visibility
- Automation
- Cost efficiency

Which of the following best describes what the company should implement?

- A. Batch processing
- B. Workload orchestration
- C. Containerization
- D. Application modernization

Answer: B

Explanation:

Workload orchestration is the best description of what the company should implement to achieve control, visibility, automation, and cost efficiency. It involves using orchestration tools to manage workloads in cloud environments, ensuring resources are used efficiently and operations are automated. References: Workload orchestration is a part of cloud management strategies discussed under the Management and Technical Operations domain in the CompTIA Cloud+ objectives.

NEW QUESTION 110

Which of the following industry standards mentions that credit card data must not be exchanged or stored in cleartext?

- A. CSA
- B. GDPR
- C. SOC2
- D. PCI-DSS

Answer: D

Explanation:

The Payment Card Industry Data Security Standard (PCI-DSS) is the industry standard that mandates that credit card data must not be stored or transmitted in cleartext. It includes requirements for encryption, access control, and other security measures to protect cardholder data. References: Official PCI Security Standards Council Site.

NEW QUESTION 113

An engineer made a change to an application and needs to select a deployment strategy that meets the following requirements:

- Is simple and fast
- Can be performed on two identical platforms

Which of the following strategies should the engineer use?

- A. Blue-green
- B. Canary
- C. Rolling
- D. in-place

Answer: A

Explanation:

The blue-green deployment strategy is ideal for scenarios where simplicity and speed are crucial. It involves two identical production environments: one (blue) hosts the current application version, while the other (green) is used to deploy the new version. Once testing is completed on the green environment and it's ready to go live, traffic is switched from blue to green, ensuring a quick and efficient rollout with minimal downtime. This method allows for immediate rollback if issues arise, by simply redirecting the traffic back to the blue environment. References: CompTIA Cloud+ material emphasizes the importance of understanding various cloud deployment strategies, including blue-green, and their application in real-world scenarios to ensure efficient and reliable software deployment in cloud environments.

NEW QUESTION 118

A security analyst reviews the daily logs and notices the following suspicious activity:

Host	NA/US/John Smith
IP	10.150.71.151
Activity	A powershell process executed compressed, encoded command line content.

The analyst investigates the firewall logs and identifies the following:

Operating system	Kali Linux
CPU	x64
Filesystem	ext4
User	John Smith
Category	Compromised - Unauthorized Access
Domain	NA/US
IP	201.101.25.121 (External)
Port	4444
Connection type	Inbound Connection

Which of the following steps should the security analyst take next to resolve this issue? (Select two).

- A. Submit an IT support ticket and request Kali Linux be uninstalled from John Smith's computer
- B. Block all inbound connections on port 4444 and block the IP address 201.101.25.121.
- C. Contact John Smith and request the Ethernet cable attached to the desktop be unplugged
- D. Check the running processes to confirm if a backdoor connection has been established.
- E. Upgrade the Windows x64 operating system on John Smith's computer to the latest version.
- F. Block all outbound connections from the IP address 10.150.71.151.

Answer: BD

Explanation:

Given the suspicious activity and Kali Linux's association with penetration testing and hacking tools, the security analyst should block all inbound connections on port 4444, as it is commonly used for malicious purposes, and block the IP address that's potentially the source of the intrusion. Additionally, checking the running processes on John Smith's computer is crucial to determine if a backdoor or unauthorized connection has been established. References: Incident response and threat mitigation steps such as these are part of the security protocols discussed in the CompTIA Cloud+ certification.

NEW QUESTION 123

A cloud administrator needs to distribute workloads across remote data centers for redundancy reasons. Which of the following deployment strategies would eliminate downtime, accelerate deployment, and remain cost efficient?

- A. In-place
- B. Rolling
- C. Blue-green
- D. Canary

Answer: C

Explanation:

Blue-green deployment is the strategy that can eliminate downtime, accelerate deployment, and remain cost-efficient. It involves running two identical production environments, only one of which is live at any given time (blue or green). When it's time to deploy, the new version is released to the inactive environment (green), which is then thoroughly tested. Once ready, the traffic is switched over, making the green environment live. References: Deployment strategies and their impact on operations are a significant topic within the CompTIA Cloud+ examination objectives.

NEW QUESTION 125

Which of the following AI/ML technologies consumes text input to discern tone?

- A. Text recognition

- B. Computer vision
- C. Visual recognition
- D. Sentiment analysis

Answer: D

Explanation:

Sentiment analysis is an AI/ML technology that processes text to determine the tone. It helps in understanding the sentiments behind the words by analyzing the text input, which can be positive, negative, or neutral. References: CompTIA Cloud+ Study Guide (Exam CV0-004) - Chapter on Cloud Technologies and Applications

NEW QUESTION 126

SIMULATION

The QA team is testing a newly implemented clinical trial management (CTM) SaaS application that uses a business intelligence application for reporting. The UAT users were

instructed to use HTTP and HTTPS. Refer to the application dataflow:

- 1A– The end user accesses the application through a web browser to enter and view clinical data.
- 2A– The CTM application server reads/writes data to/from the database server.
- 1B– The end user accesses the application through a web browser to run reports on clinical data.
- 2B– The CTM application server makes a SOAP call on a non-privileged port to the BI application server.
- 3B– The BI application server gets the data from the database server and presents it to the CTM application server.

When UAT users try to access the application using https://ctm.app.com or http://ctm.app.com, they get a message stating: ??Browser cannot display the webpage.?? The QA team has raised a ticket to troubleshoot the issue.

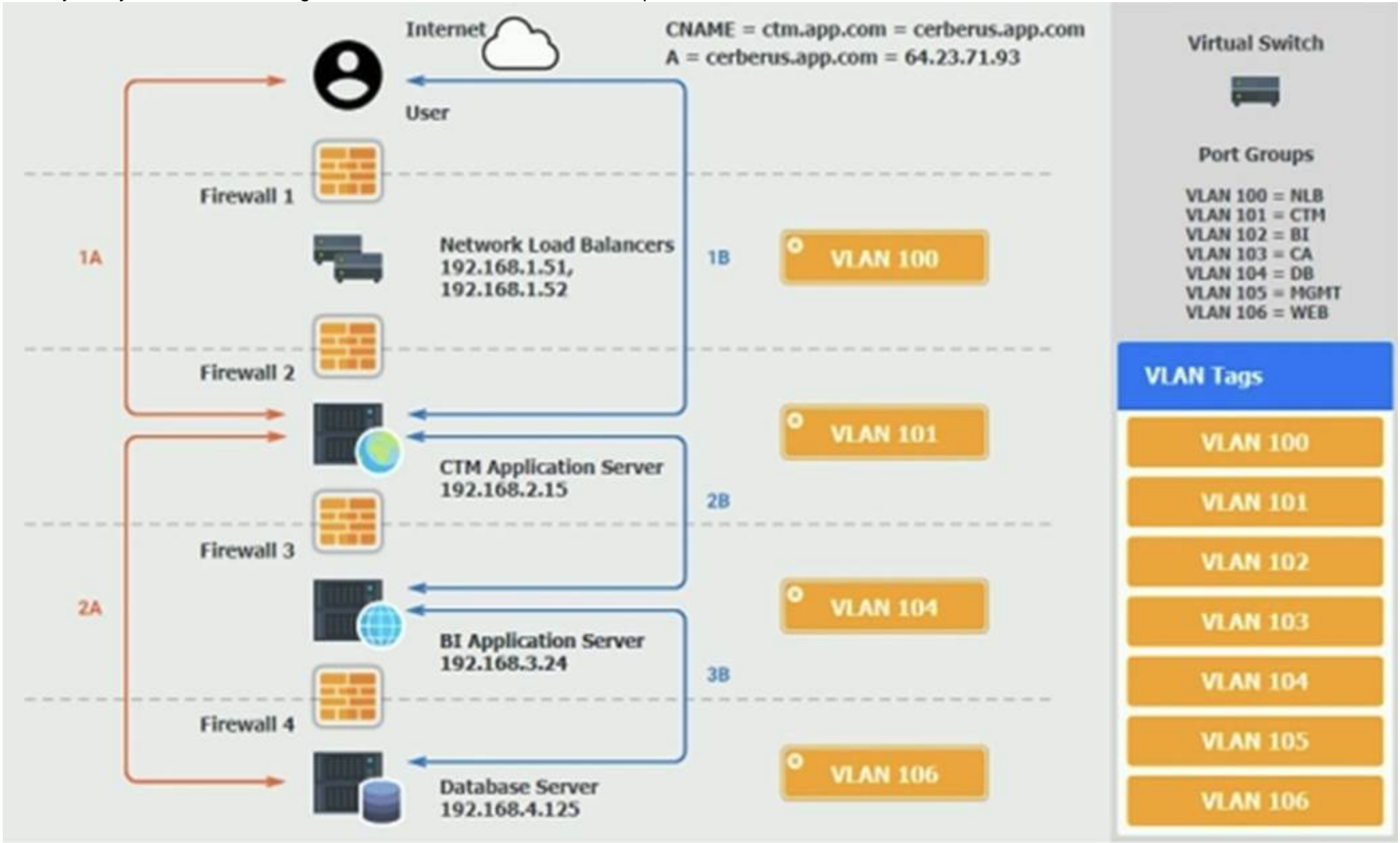
INSTRUCTIONS

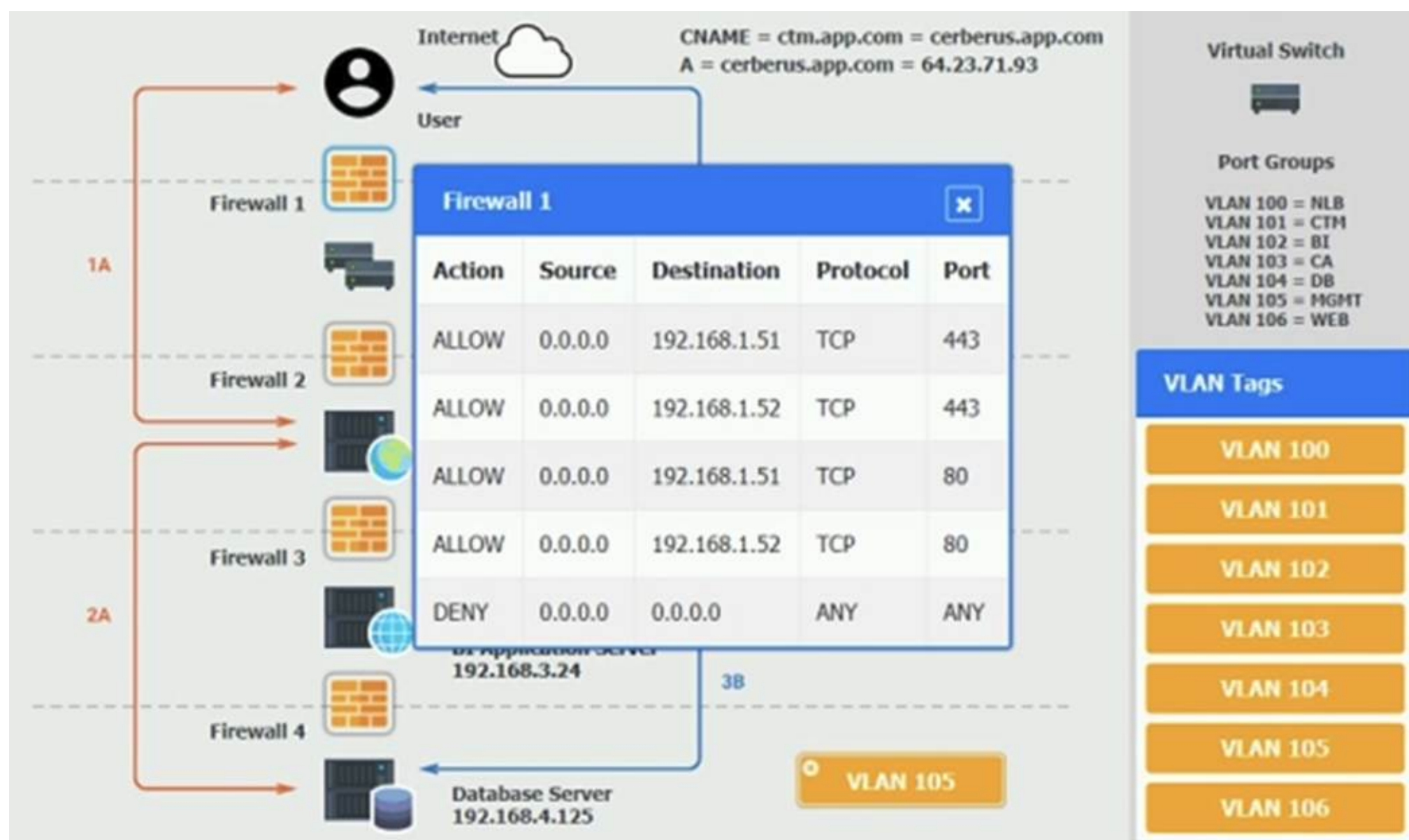
You are a cloud engineer who is tasked with reviewing the firewall rules as well as virtual network settings.

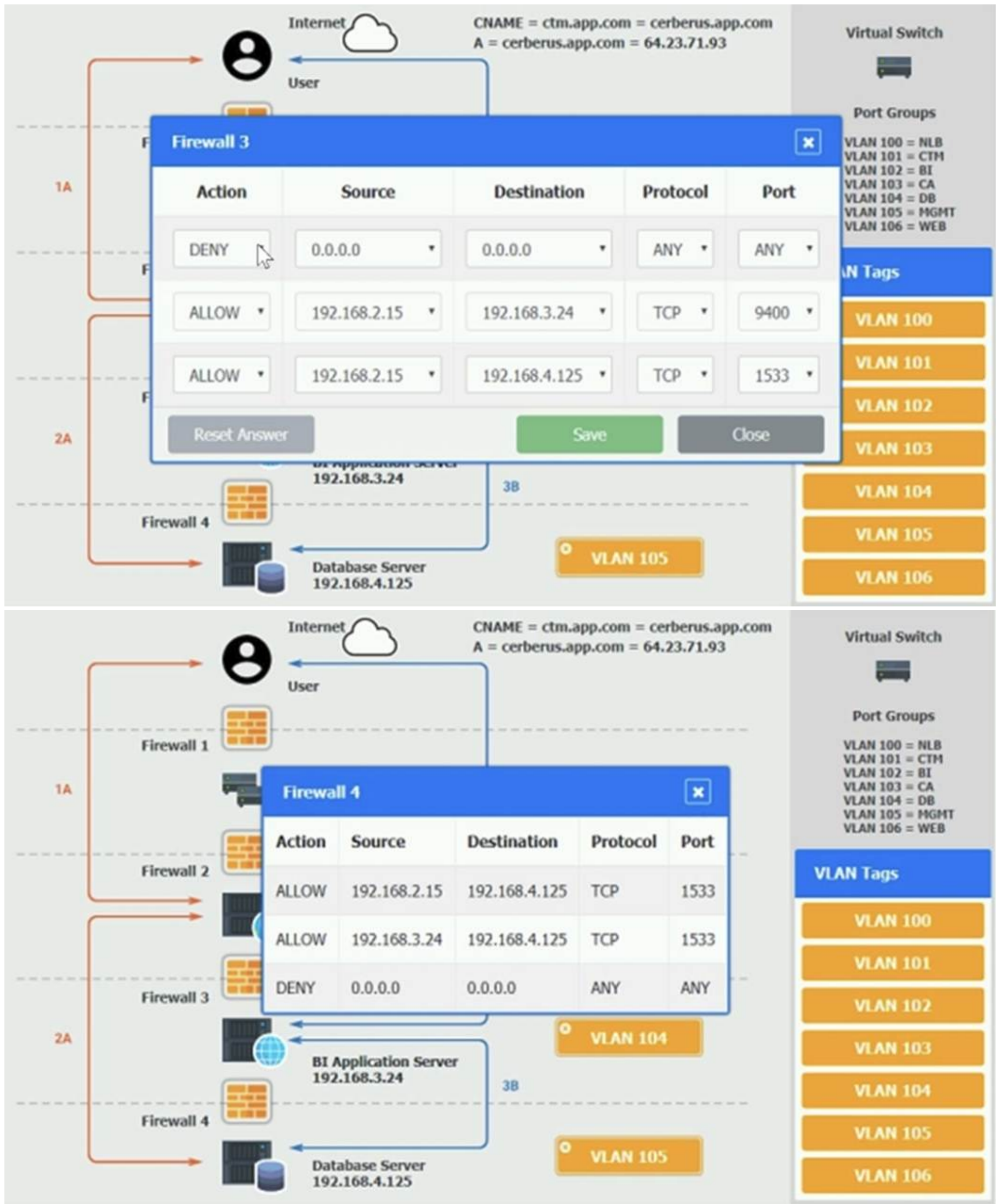
You should ensure the firewall rules are allowing only the traffic based on the dataflow. You have already verified the external DNS resolution and NAT are working.

Verify and appropriately configure the VLAN assignments and ACLs. Drag and drop the appropriate VLANs to each tier from the VLAN Tags table. Click on each Firewall to change ACLs as needed.

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







A. Mastered
B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 129

Users have been reporting that a remotely hosted application is not accessible following a recent migration. However, the cloud administrator is able to access the

application from the same site as the users. Which of the following should the administrator update?

- A. Cipher suite
- B. Network ACL
- C. Routing table
- D. Permissions

Answer: C

Explanation:

Since the cloud administrator can access the application from the same site but users cannot, it suggests a possible issue with the network routing. The routing table may need to be updated to ensure that traffic from the users' location is correctly directed to the new location of the remotely hosted application after the migration. References: CompTIA Network+ Certification Study Guide by Glen E. Clarke.

NEW QUESTION 132

A cloud administrator is building a company-standard VM image, which will be based on a public image. Which of the following should the administrator implement to secure the image?

- A. ACLs
- B. Least privilege
- C. Hardening
- D. Vulnerability scanning

Answer: C

Explanation:

Hardening a VM image involves implementing security measures to reduce vulnerabilities and protect against threats. This process includes removing unnecessary software, services, and permissions, ensuring that the remaining software is updated with the latest security patches, and configuring settings to enhance security. Starting with a public image, the administrator should apply hardening techniques to ensure the custom company-standard VM image is secure and resilient against attacks.

NEW QUESTION 134

A cloud engineer is designing a cloud-native, three-tier application. The engineer must adhere to the following security best practices:

- Minimal services should run on all layers of the stack.
- The solution should be vendor agnostic.
- Virtualization could be used over physical hardware.

Which of the following concepts should the engineer use to design the system to best meet these requirements?

- A. Virtual machine
- B. Micro services
- C. Fan-out
- D. Cloud-provided managed services

Answer: B

Explanation:

Microservices architecture is the most suitable design principle that aligns with the security best practices mentioned. It involves developing a suite of small services, each running in its own process and communicating with lightweight mechanisms, often an HTTP resource API. This architecture minimizes the services running on each layer, allows for vendor-agnostic solutions, and is well-suited for virtualization over physical hardware. References: Microservices as an architectural approach is discussed in the context of cloud-native applications within the CompTIA Cloud+ material.

NEW QUESTION 135

Which of the following communication methods between on-premises and cloud environments would ensure minimal-to-low latency and overhead?

- A. Site-to-site VPN
- B. Peer-to-peer VPN
- C. Direct connection
- D. peering

Answer: C

Explanation:

A direct connection between on-premises and cloud environments involves a dedicated, private connection that does not traverse the public internet. This setup ensures minimal-to-low latency and overhead, providing more consistent network performance and reliability compared to other methods like VPNs or public internet connections, making it suitable for high-volume or latency-sensitive applications.

NEW QUESTION 137

Two CVEs are discovered on servers in the company's public cloud virtual network. The CVEs are listed as having an attack vector value of network and CVSS score of 9.0. Which of the following actions would be the best way to mitigate the vulnerabilities?

- A. Patching the operating systems
- B. Upgrading the operating systems to the latest beta
- C. Encrypting the operating system disks
- D. Disabling unnecessary open ports

Answer: A

Explanation:

For vulnerabilities with a high CVSS score and a network attack vector, the most effective and direct mitigation action is to patch the operating systems. Patching addresses the specific vulnerabilities that have been identified and helps to secure the servers against the known exploits that could take advantage of these CVEs. References: CompTIA Cloud+ Guide to Cloud Computing (ISBN: 978-1-64274-282-2)

NEW QUESTION 141

A company serves customers globally from its website hosted in North America. A cloud engineer recently deployed new instances of the website in the Europe region. Which of the following is the most likely reason?

- A. To simplify workflow
- B. To enhance security
- C. To reduce latency
- D. To decrease cost

Answer: C

Explanation:

The most likely reason for deploying new instances of a website in the Europe region, in addition to the ones hosted in North America, is to reduce latency for users located in Europe. By having the website's resources closer to the end-users, the data has a shorter distance to travel, resulting in faster load times and better performance. References: CompTIA Cloud+ Study Guide (Exam CV0-004) by Todd Montgomery and Stephen Olson

NEW QUESTION 144

Which of the following cloud deployment models is the best way to replicate a workload non-disruptively between on-premises servers and a public cloud?

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

Answer: D

Explanation:

A hybrid cloud deployment model is the best way to replicate workloads non-disruptively between on-premises servers and a public cloud. This model integrates on-premises infrastructure, or private clouds with public clouds, allowing data and applications to be shared between them. References: CompTIA Cloud+ Study Guide (Exam CV0-004) - Chapter on Cloud Deployment Models

NEW QUESTION 147

Once a change has been made to templates, which of the following commands should a cloud architect use next to deploy an IaaS platform?

- A. git pull
- B. git fetch
- C. git commit
- D. git push

Answer: D

Explanation:

After making changes to templates, a cloud architect should use the git push command to deploy an IaaS platform. This command is used to upload the local repository content to a remote repository, making the new or changed templates available for the next deployment. References: Version control practices and commands, such as using git for IaaS template management, are covered under the best practices for cloud deployments in the CompTIA Cloud+ certification.

NEW QUESTION 152

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual CV0-004 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the CV0-004 Product From:

<https://www.2passeasy.com/dumps/CV0-004/>

Money Back Guarantee

CV0-004 Practice Exam Features:

- * CV0-004 Questions and Answers Updated Frequently
- * CV0-004 Practice Questions Verified by Expert Senior Certified Staff
- * CV0-004 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * CV0-004 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year