CV0-003 Q&As

CompTIA Cloud+ Certification

Pass CompTIA CV0-003 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.leads4pass.com/cv0-003.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CompTIA Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

A security team is conducting an audit of the security group configurations for the Linux servers that are hosted in a public IaaS The team identifies the following rule as a potential issue:

Protocol	Port	Source	Description
TCP	22	0.0.0.0/0	Allow SSH access

A cloud administrator, who is working remotely, logs in to the cloud management console and modifies the rule to set the source to "My IP." Shortly after deploying the rule, an internal developer receives the following error message when attempting to log in to the server using SSH: Network error: Connection timed out. However, the administrator is able to connect successfully to the same server using SSH. Which of the following is the BEST option for both the developer and the administrator to access the server from their locations?

A. Modify the outbound rule to allow the company\\'s external IP address as a source

B. Add an inbound rule to use the IP address for the company\\'s main office as a source

C. Modify the inbound rule to allow the company\\'s external IP address as a source

D. Delete the inbound rule to allow the company\\'s external IP address as a source

Correct Answer: A

QUESTION 2

A cloud administrator needs to establish a secure connection between two different locations. Which of the following is the BEST option to implement the secure connection?

A. HTTPS

B. IPSec

C. TLS

D. SSH

Correct Answer: B

The best option to implement a secure connection between two different locations is IPSec (Internet Protocol Security). IPSec is a protocol suite that provides security for IP-based communications over networks. IPSec can encrypt and authenticate the data packets between two endpoints, such as routers, firewalls, or VPN gateways. IPSec can also provide integrity, confidentiality, and replay protection for the data. Reference: CompTIA Cloud+ Certification Exam Objectives, Domain 2.0 Security, Objective 2.2 Given a scenario, implement appropriate network security controls for a cloud environment.

QUESTION 3

Based on the shared responsibility model, which of the following solutions passes the responsibility of patching the OS to the customer?

A. PaaS

B. DBaaS

C. IaaS

D. SaaS

Correct Answer: C

Reference: https://cloudsecurityalliance.org/blog/2020/08/26/shared-responsibility-model-explained/

QUESTION 4

An administrator has been informed that some requests are taking a longer time to respond than other requests of the same type. The cloud consumer is using multiple network service providers and is performing link load balancing for bandwidth aggregation. Which of the following commands will help the administrator understand the possible latency issues?

A. ping

B. ipconfig

C. traceroute

D. netstat

Correct Answer: C

QUESTION 5

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

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

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

A. Remove rules 1, 2, and 5.

B. Remove rules 1, 3, and 4.

C. Remove rules 2, 3, and 4.

D. Remove rules 3, 4, and 5.

Correct Answer: A

To ensure the web servers in the public subnet allow only secure communications and remediate any possible issue, the analyst should remove rules 1, 2, and 5 from the stateful configuration. These rules are allowing insecure or unnecessary traffic to or from the web servers, which may pose security risks or performance issues. The rules are: Rule 1: This rule allows inbound traffic on port 80 (HTTP) from any source to any destination. HTTP is an unencrypted and insecure protocol that can expose web traffic to interception, modification, or spoofing. The analyst should remove this rule and use HTTPS (port 443) instead, which encrypts and secures web traffic. Rule 2: This rule allows outbound traffic on port 25 (SMTP) from any source to any destination. SMTP is a protocol that is used to send email messages. The web servers in the public subnet do not need to send email messages, as this is not their function. The analyst should remove this rule and block outbound SMTP traffic, which may prevent spamming or phishing attacks from compromised web servers. Rule 5: This rule allows inbound traffic on port 22 (SSH) from any source to any destination. SSH is a protocol that allows remote access and management of systems or devices using a command-line interface. The web servers in the public subnet do not need to allow SSH access from any source, as this may expose them to unauthorized or malicious access. The analyst should remove this rule and restrict SSH access to specific sources, such as the administrator\\'s workstation or a bastion host.