

## CV0-003<sup>Q&As</sup>

CompTIA Cloud+ Certification

### Pass CompTIA CV0-003 Exam with 100% Guarantee

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

<https://www.lead4pass.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 cloud administrator is integrating account logins with Facebook, LinkedIn, and Twitter for marketing and to increase market presence using social media platforms. Given this scenario, which of the following components are needed to match these requirements? (Select TWO).

- A. SOAP
- B. SAML assertion
- C. Security token
- D. Identity provider
- E. Session state

Correct Answer: BE

---

**QUESTION 2**

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

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

Correct Answer: D

This is the best definition of serverless computing that explains how it is different from using VMs (Virtual Machines). Serverless computing is a cloud service model that provides customers with a platform to run applications or functions

without having to manage or provision any underlying infrastructure or resources, such as servers, storage, network, OS, etc. Serverless computing is different from using VMs in the following ways:

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

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

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

---

**QUESTION 3**

A company uses multiple SaaS-based cloud applications. All the applications require authentication upon access. An administrator has been asked to address this issue and enhance security. Which of the following technologies would be the BEST solution?

- A. Single sign-on
- B. Certificate authentication
- C. Federation
- D. Multifactor authentication

Correct Answer: A

Reference: [https://en.wikipedia.org/wiki/Single\\_sign-on](https://en.wikipedia.org/wiki/Single_sign-on)

---

#### QUESTION 4

A cloud administrator is reviewing the annual contracts for all hosted solutions. Upon review of the contract for the hosted mail solution, the administrator notes the monthly subscription rate has increased every year. The provider has been in place for ten years, and there is a large amount of data being hosted. Which of the following is a barrier to switching providers?

- A. Service-level agreement
- B. Vendor lock-in
- C. Memorandum of understanding
- D. Encrypted data

Correct Answer: B

Vendor lock-in is a barrier to switching providers for a hosted mail solution that has increased its monthly subscription rate every year. Vendor lock-in is a situation where a customer becomes dependent on a vendor or provider for a product or service and faces difficulties or costs in switching to another vendor or provider. Vendor lock-in can occur due to various factors, such as proprietary technology, contractual obligations, data migration challenges, compatibility issues, etc. In this case, the customer may face vendor lock-in due to the large amount of data being hosted by the mail provider and the potential challenges or costs of transferring or migrating the data to another provider.

---

#### 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.