

ExamsLabs

ExamsLabs

HOME

ALL VENDORS

GUARANTEE

FAQ

TESTIMONIALS

CART (0)

Pass Your Next Certification Exam Fast!

Everything you need to prepare, learn & pass your certification exam easily.

365 days free updates. First attempt guaranteed success.



Select a vendor...

Select an test...

Your email address

Free Download Demo

Try **Online Engine** before you buy

Online Test Engine: Online Tool, Convenient, easy to study. Instant Online Access. Supports All Web Browsers.

PDF format: Easy to read and print learning materials, our products are available in PDF file format.

Desktop Test Engine: Installable Software Application. Simulates Real Exam Environment. Practice Offline Anytime.

What Client's Say

"I passed today with score 80%. I confirm that it's valid in UK. Focus on "Correct answer" and forget the "Answer X from real test". I had free new questions.



Sebastian
★★★★★

"Questions from this HPE0-S51 dump are 100% valid... not all answers. I passed this exam a few days ago (in France) and got these results.



Wayne
★★★★★

<http://www.examslabs.com/>

Latest Study Materials, Valid Dumps - ExamsLabs

Exam : **GPCS**

Title : **GIAC Public Cloud Security**

Vendor : **GIAC**

Version : **DEMO**

NO.1 Which of the following is a key consideration when securing virtual private networks (VPNs) in a cloud environment?

Response:

- A.** Ensuring encryption is used for all VPN connections
- B.** Limiting VPN access to public endpoints
- C.** Disabling authentication for easier access
- D.** Allowing open access to all IP addresses

Answer: A

NO.2 How does network segmentation help secure cloud environments?

Response:

- A.** By consolidating all traffic into one network
- B.** By allowing specific security controls for different network segments
- C.** By increasing the speed of data transfers
- D.** By removing the need for firewalls

Answer: B

NO.3 In the context of cloud services, what is an effective measure to prevent data exfiltration via remote administrative interfaces?

(Choose Three)

Response:

- A.** Enforcing encryption of all data in transit.
- B.** Implementing strict access controls and authentication methods.
- C.** Using open network ports to facilitate quicker data transfer.
- D.** Monitoring and logging all administrative actions.
- E.** Restricting the use of removable media on administrative devices.

Answer: A,B,D

NO.4 What are best practices for securing virtual private networks (VPNs) in cloud environments?

(Choose two)

Response:

- A.** Use encryption for all VPN connections
- B.** Disable multi-factor authentication for VPN users
- C.** Limit access to trusted IP addresses
- D.** Allow all public IP addresses to access the VPN

Answer: A,C

NO.5 Which of the following are types of data masking suitable for protecting sensitive data in cloud environments?

(Choose Two)

Response:

- A.** Static data masking
- B.** Dynamic data masking

- C. Transparent data masking
- D. Asymmetric data masking

Answer: A,B

NO.6 What is a significant security concern in a multicloud environment?

Response:

- A. Increased computational overhead.
- B. Consistency of security policies across platforms.
- C. Decreased network traffic.
- D. Easier data management.

Answer: B

NO.7 What role does benchmarking play in cloud security?

Response:

- A. It ensures maximum throughput for all applications.
- B. It identifies the least compliance aspects of the cloud.
- C. It helps ensure that cloud configurations meet industry standards.
- D. It provides a way to reduce costs by identifying underutilized resources.

Answer: C

NO.8 How does using encryption at rest help in cloud data protection?

Response:

- A. It secures data only during transmission
- B. It prevents unauthorized access to data stored in the cloud
- C. It makes it easier to retrieve data
- D. It reduces the storage costs in the cloud

Answer: B

NO.9 What is the main purpose of cloud application firewalls?

Response:

- A. To reduce data redundancy
- B. To control access to virtual machines
- C. To block malicious traffic and prevent web-based attacks
- D. To improve data storage efficiency

Answer: C

NO.10 Which security controls should be implemented for virtual network monitoring?

(Choose two)

Response:

- A. Enable logging and network flow monitoring
- B. Disable all encryption
- C. Set up alerts for suspicious traffic patterns
- D. Allow unrestricted access to network resources

Answer: A,C

NO.11 Which technique is crucial for detecting vulnerabilities in serverless functions before deployment?

Response:

- A. Integration testing
- B. Manual code review
- C. Static code analysis
- D. Load testing

Answer: C

NO.12 Which encryption keys management practices are recommended for cloud data protection? (Choose Two)

Response:

- A. Store keys in a publicly accessible repository for easy access.
- B. Use a dedicated security module for key management.
- C. Rotate encryption keys periodically.
- D. Use the same keys across multiple platforms for consistency.

Answer: B,C

NO.13 What are key benefits of using cloud compliance benchmarking tools? (Choose two)

Response:

- A. They help assess cloud environments against industry standards
- B. They increase cloud storage capacity
- C. They ensure cloud services meet regulatory requirements
- D. They reduce the cost of cloud services

Answer: A,C

NO.14 What are best practices for securing cloud application service platforms? (Choose two)

Response:

- A. Disable logging to reduce overhead
- B. Implement role-based access control (RBAC)
- C. Enable encryption for sensitive data
- D. Allow public access to all resources

Answer: B,C

NO.15 What role do bastion hosts play in securing cloud environments?

Response:

- A. They serve as dedicated nodes for initial access and management of other servers.
- B. They act as primary data storage locations.
- C. They increase the complexity of network infrastructure.
- D. They provide physical security for server hardware.

Answer: A

NO.16 What is a primary purpose of using benchmarking tools in cloud environments?

Response:

- A.** To measure the financial performance of cloud services.
- B.** To assess compliance with security standards and frameworks.
- C.** To evaluate the physical durability of hardware.
- D.** To increase the bandwidth of network connections.

Answer: B