WGU Managing-Cloud-Security D320 Practice Questions

Shared by Logan on 02-11-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which phase of the cloud data lifecycle implements the file, block, or object type of cloud architecture?

Options:

A- Archive
B- Store
C- Create
D- Share

P2P exams

Answer:

B

Explanation:

The Store phase of the cloud data lifecycle is responsible for maintaining data in cloud storage systems and is where file, block, and object storage architectures are implemented. Managing Cloud documentation explains that once data is created and prepared, it must be stored using appropriate storage technologies that support availability, durability, scalability, and performance requirements.

File storage is commonly used for shared access and hierarchical file systems, block storage supports high-performance workloads such as databases and virtual machines, and object storage is optimized for scalability and unstructured data. All these storage models fall under the Store phase because they represent how data is retained and managed at rest within the cloud environment.

The Archive phase focuses on long-term retention and cost optimization, often using cold or infrequent access storage. The Create phase is concerned with generating data, and the Share phase involves distributing data to other users or systems. None of these phases define the architectural storage models used to hold data. Therefore, the Store phase is the correct answer, as it directly implements the underlying cloud storage architectures required to securely and efficiently manage data.

Question 2

Question Type: MultipleChoice

A group of DevOps engineers adopted the network-as-code methodology to manage network infrastructure. During a code release, the engineers find a bug that is causing issues on a production site. Which safeguard will allow the engineers to restore functionality to the production site?

Options:

A- Staging
B- Code review
C- Code testing
D- Rollback

P2P exams

Answer:

D

Explanation:

A rollback is the safeguard that restores a system to its previous, stable state when a new code release introduces issues. In DevOps workflows, rollbacks provide a rapid recovery mechanism, reducing downtime and minimizing customer impact.

Staging, code review, and testing are preventive controls that reduce the likelihood of defects reaching production, but once a bug has already been deployed, rollback is the corrective control.

Rollback strategies often rely on version control systems, container orchestration, or infrastructure-as-code automation to quickly revert to earlier configurations. This practice is essential for maintaining reliability and availability, especially in cloud environments with continuous deployment pipelines.

P2P exams

Question 3

Question Type: MultipleChoice

An organization designing a data center wants the ability to quickly create and shut down virtual systems based on demand. Which concept describes this capability?

Options:

A- Resource scheduling
B- High availability
C- Ephemeral computing
D- Maintenance mode

Answer:

C

Explanation:

The capability to rapidly create and destroy virtual systems as demand fluctuates is known as ephemeral computing. These short-lived resources are provisioned automatically when needed and decommissioned when demand subsides.

Resource scheduling helps allocate resources but does not imply temporary lifespans. High availability ensures continuous service, and maintenance mode is used for administrative tasks.

Ephemeral computing is central to elasticity in cloud environments, reducing costs and improving scalability. For example, containers or serverless functions may run only while needed and then disappear. This model optimizes utilization, lowers expenses, and supports modern application architectures that demand agility.

Question 4

Question Type: MultipleChoice

A user creates new financial documents that will be stored in the cloud. Which action should the user take before uploading the documents to protect them against threats such as packet capture and on-path attacks?

Options:

A- Hashing
B- Encryption
C- Change tracking
D- Metadata labeling

Answer:

B

Explanation:

Before transmitting sensitive financial data to the cloud, the best defense against interception threats like packet capture and man-in-the-middle attacks is encryption. Encryption protects data in transit by converting plain text into cipher text, which can only be deciphered with the correct keys.

Hashing provides integrity verification but does not secure confidentiality. Change tracking monitors modifications but does not prevent interception. Metadata labeling adds context but does not protect against on-path attackers.

Using strong encryption protocols (e.g., TLS) ensures that even if traffic is intercepted, the attacker cannot read the data. Encryption also aligns with compliance requirements such as PCI DSS, which mandates encryption for financial data during transmission. By encrypting before upload, the user ensures end-to-end confidentiality across potentially insecure networks.

Question 5

Question Type: MultipleChoice

Which threat modeling process would a security analyst use to test a new application from a malicious actor's perspective?

Options:

A- Damage, Reproducibility, Exploitability, Affected Users, and Discoverability (DREAD)
B- Architecture, Threats, Attack Surfaces, and Mitigation (ATASM)
C- Process for Attack Simulation and Threat Analysis (PASTA)
D- Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privileges (STRIDE)

Answer:

C

Explanation:

The Process for Attack Simulation and Threat Analysis (PASTA) is a risk-centric threat modeling methodology that explicitly focuses on simulating real-world attacks from an adversary's perspective. Unlike STRIDE or DREAD, which classify threats and rate severity, PASTA evaluates how an attacker would exploit vulnerabilities step by step.

PASTA has seven stages, including defining objectives, decomposing applications, and simulating attacks. This methodology helps organizations understand both technical and business risks by looking at the application as an attacker would.

STRIDE categorizes threats, DREAD provides scoring, and ATASM emphasizes architecture and mitigation. While valuable, they are not primarily attack-simulation frameworks. PASTA enables proactive testing of defenses against realistic adversary behaviors, making it especially relevant in modern cloud and DevSecOps environments.

Question 6

Question Type: MultipleChoice

An organization is informed by its cloud provider that a storage device containing some of the organization's data has been seized as possible evidence in a court case, but the organization itself is not involved in any ongoing court cases. Which characteristic of a cloud environment architecture makes such a scenario possible?

Options:

A- Virtualization
B- Multitenancy
C- Software as a service (SaaS)
D- Platform as a service (PaaS)

Answer:

B

Explanation:

The scenario arises because of multitenancy, a core cloud characteristic where multiple customers share the same physical infrastructure. If a storage device containing multiple tenants' data is seized as part of a case involving another customer, unrelated organizations may still be affected.

Virtualization enables resource abstraction, but multitenancy specifically introduces shared infrastructure risks. SaaS and PaaS are service models, not architectural characteristics.

Multitenancy offers efficiency and cost benefits but raises challenges for data sovereignty, legal jurisdiction, and evidentiary control. Providers mitigate these risks through encryption, logical isolation, and contractual terms. Customers must understand these implications when handling regulated or sensitive data in cloud environments.

Question 7

Question Type: MultipleChoice

An organization wants to ensure that all entities trust any certificate generated internally in the organization. What should be used to generate these certificates?

Options:

A- Individual users' private keys
B- The organization's certificate repository server
C- The organization's certificate authority server
D- Individual systems' private keys

Answer:

C

Explanation:

Trust in digital certificates comes from their issuance by a Certificate Authority (CA). A CA is a trusted entity that validates identities and signs certificates. In internal environments, organizations often operate a private CA to issue certificates for users, systems, and services.

If certificates were generated by individual private keys or systems without central authority, there would be no unified trust chain, and validating authenticity across the organization would be impossible. A certificate repository server only distributes certificates but cannot establish trust.

By using an organizational CA server, all certificates are linked to a root of trust. Systems configured to trust the organization's CA will trust any certificate it issues. This allows secure internal communications (TLS, VPN, email signing) and ensures scalability as new services come online. It also supports compliance with enterprise PKI policies.

Question 8

Question Type: MultipleChoice

When should a cloud service provider delete customer data?

Options:

A- When the cloud provider oversubscribes its storage space
B- When the data has not been accessed in the last 30 days
C- After a scheduled data review
D- After the specified retention period

Answer:

D

Explanation:

The correct time for data deletion is after the specified retention period defined by contractual agreements, regulatory frameworks, or internal policies. Retention policies ensure that data is kept for as long as necessary for business, legal, or compliance reasons but not longer than required.

Oversubscription, inactivity, or review cycles are not valid triggers because they may conflict with compliance mandates such as GDPR, HIPAA, or PCI DSS. Deleting data prematurely could result in legal penalties or business risks, while keeping it longer than necessary could increase exposure.

By deleting data only after the retention period, providers demonstrate adherence to data governance principles and protect customer rights while minimizing storage costs and liability.

Question 9

Question Type: MultipleChoice

Which of the following is an iterative software development methodology that focuses on achieving customer satisfaction by delivering the software early in the process and welcoming changing requirements from the customer, even late in the process?

Options:

A- Agile
B- Spiral
C- Waterfall
D- Lean

Answer:

A

Explanation:

Agile is an iterative software development methodology designed to prioritize customer satisfaction, adaptability, and incremental delivery. Agile teams deliver small, working pieces of software frequently, ensuring feedback is incorporated throughout the process. This flexibility allows late-stage requirement changes to be accommodated without derailing the project.

Waterfall is a sequential approach with limited flexibility. Spiral combines iterative development with risk analysis, but it is not as customer-focused as Agile. Lean emphasizes efficiency and waste reduction but does not center on continuous delivery and adaptability.

Agile frameworks such as Scrum and Kanban embody this philosophy, supporting faster innovation, better collaboration, and responsiveness to evolving business needs.

P2P exams

To Get Premium Files for Managing-Cloud-Security Visit

https://www.p2pexams.com/products/managing-cloud-security

For More Free Questions Visit

https://www.p2pexams.com/wgu/pdf/managing-cloud-security

