CompTIA Cloud+ Post-Assessment Practice Test (Sample)

Study Guide

Everything you need from our exam experts!

Table of Contents

Introduction

Preparing for a certification exam can feel overwhelming, but with the right tools, it becomes an opportunity to build confidence, sharpen your skills, and move one step closer to your goals. At Examzify, we believe that effective exam preparation isn't just about memorization, it's about understanding the material, identifying knowledge gaps, and building the test-taking strategies that lead to success.

This guide was designed to help you do exactly that.

Whether you're preparing for a licensing exam, professional certification, or entry-level qualification, this book offers structured practice to reinforce key concepts. You'll find a wide range of multiple-choice questions, each followed by clear explanations to help you understand not just the right answer, but why it's correct.

The content in this guide is based on real-world exam objectives and aligned with the types of questions and topics commonly found on official tests. It's ideal for learners who want to:

- **Practice answering questions under realistic conditions,**
- **Improve accuracy and speed,**
- **Review explanations to strengthen weak areas, and**
- **Approach the exam with greater confidence.**

We recommend using this book not as a stand-alone study tool, but alongside other resources like flashcards, textbooks, or hands-on training. For best results, we recommend working through each question, reflecting on the explanation provided, and revisiting the topics that challenge you most.

Remember: successful test preparation isn't about getting every question right the first time, it's about learning from your mistakes and improving over time. Stay focused, trust the process, and know that every page you turn brings you closer to success.

Let's begin.

How to Use This Guide

This guide is designed to help you study more effectively and approach your exam with confidence. Whether you're reviewing for the first time or doing a final refresh, here’s how to get the most out of your Examzify study guide:

1. Start with a Diagnostic Review

Skim through the questions to get a sense of what you know and what you need to focus on. Your goal is to identify knowledge gaps early.

2. Study in Short, Focused Sessions

Break your study time into manageable blocks (e.g. 30 – 45 minutes). Review a handful of questions, reflect on the explanations.

3. Learn from the Explanations

After answering a question, always read the explanation, even if you got it right. It reinforces key points, corrects misunderstandings, and teaches subtle distinctions between similar answers.

4. Track Your Progress

Use bookmarks or notes (if reading digitally) to mark difficult questions. Revisit these regularly and track improvements over time.

5. Simulate the Real Exam

Once you're comfortable, try taking a full set of questions without pausing. Set a timer and simulate test-day conditions to build confidence and time management skills.

6. Repeat and Review

Don’t just study once, repetition builds retention. Re-attempt questions after a few days and revisit explanations to reinforce learning. Pair this guide with other Examzify tools like flashcards, and digital practice tests to strengthen your preparation across formats.

There’s no single right way to study, but consistent, thoughtful effort always wins. Use this guide flexibly, adapt the tips above to fit your pace and learning style. You've got this!

Questions

1. **Fictional Corp has two data centers in the United States with private clouds. They want to connect them via the Internet using GRE, but GRE lacks encryption. Which option should they combine with GRE to provide encryption?**

   A. TLS

   B. SSH

   C. TLS over GRE

   D. IPsec

2. **Which team is responsible for approving or denying change requests in an ITIL-based change management process?**

   A. Service Desk

   B. Change Manager

   C. CAB

   D. Security Team

3. **What is the primary purpose of federation in cloud identity management?**

   A. To enable single sign-on across trusted domains

   B. To require MFA for every user

   C. To centralize encryption keys

   D. To enforce password history

4. **In which scenario is serverless computing most advantageous?**

   A. Long-running, stateful workloads requiring low cold-start latency

   B. Event-driven workloads with variable traffic

   C. Predictable, constant high CPU usage

   D. Applications requiring persistent connections

5. **Which cloud capability allows a system to automatically adjust resources in response to load without manual intervention?**

   A. Auto-scaling

   B. Elasticity

   C. Load balancing

   D. High availability

6. Which metric defines the maximum acceptable downtime for an IT service during a disruption?

A. Recovery Time Objective

B. Recovery Point Objective

C. Mean Time To Repair

D. Uptime

7. For disaster recovery, which approach minimizes downtime by maintaining a copy of data at a remote site?

A. Local backups

B. Cloud backups

C. Replication to a remote site

D. Tape backup only

8. In an identity federation setup between on-premises Active Directory and cloud identities, which practice helps maintain consistent access control across environments?

A. Disable MFA to reduce friction.

B. Use only cloud accounts without on-prem identity.

C. Avoid any group synchronization and rely on user passwords.

D. Enforce MFA and synchronize groups and roles.

9. For a globally deployed application that requires redundancy and fast data access, which storage method is most suitable?

A. Local storage

B. Multi-regional

C. Cold storage

D. NAS

10. When data gravity is a factor, what is a best practice for architecture placement of compute and storage?

A. Move data to where compute resides

B. Remove data to avoid gravity

C. Place compute near the data

D. Data gravity has no impact

Answers

1. D
2. C
3. A
4. B
5. B
6. A
7. C
8. D
9. B
10. C

Explanations

1. **Fictional Corp has two data centers in the United States with private clouds. They want to connect them via the Internet using GRE, but GRE lacks encryption. Which option should they combine with GRE to provide encryption?**

   A. TLS

   B. SSH

   C. TLS over GRE

   D. IPsec

This question tests how to secure a GRE tunnel over the Internet. GRE creates a tunnel for carrying traffic, but it does not provide encryption, so the contents are exposed as they traverse the public network. To add encryption at the IP level, you wrap the GRE traffic in IPsec. IPsec provides confidentiality, integrity, and authentication for IP packets, and it's specifically designed for site-to-site VPNs. When you run IPsec in tunnel mode to protect the GRE tunnel, all traffic inside that GRE tunnel is encrypted and authenticated as it traverses the Internet. This combination is a standard, effective way to securely connect two data centers. The other options aren't practical for securing an entire site-to-site link. TLS and SSH operate at higher layers for individual sessions or hosts (not the entire tunnel between sites), and TLS over GRE isn't a standard, widely used approach for encrypting an entire network path.

2. **Which team is responsible for approving or denying change requests in an ITIL-based change management process?**

   A. Service Desk

   B. Change Manager

   C. CAB

   D. Security Team

In ITIL-based change management, the approval or denial of change requests is handled by the Change Advisory Board. The CAB is a cross-functional group that reviews proposed changes for risk, impact on services, resource needs, and scheduling, and then decides to authorize, defer, or reject the change. The Change Manager coordinates the process and chairs CAB meetings, but the authority to approve lies with the CAB. For urgent changes, an ECAB handles expedited approvals. The Service Desk handles incident logging and user requests, and the Security Team provides input on security implications, but neither acts as the primary approval body.

3. What is the primary purpose of federation in cloud identity management?

A. To enable single sign-on across trusted domains

B. To require MFA for every user

C. To centralize encryption keys

D. To enforce password history

Federation focuses on establishing trust between different security domains so a user authenticated in one domain can access services in another without re-entering credentials. The main payoff is single sign-on across trusted domains: after you sign in with your organization's identity provider, you receive a token (like a SAML assertion or an OpenID Connect ID token) that the service provider in another domain accepts, allowing seamless access. This keeps passwords and authentication centralized with the IdP while enabling access to multiple cloud apps or services. MFA for every user, centralized encryption keys, and enforcing password history are separate controls or policies. MFA is an authentication step, not the interoperability mechanism federation provides. Centralizing encryption keys deals with cryptographic key management, not cross-domain identity authentication. Enforcing password history is a password policy, not about enabling cross-domain access through trusted authentication.

4. In which scenario is serverless computing most advantageous?

A. Long-running, stateful workloads requiring low cold-start latency

B. Event-driven workloads with variable traffic

C. Predictable, constant high CPU usage

D. Applications requiring persistent connections

Serverless computing is most advantageous when the workload is event-driven and traffic is variable because it auto-scales with demand and you pay only for actual execution time. This means as events spike, the platform runs more function instances to handle them, and as activity drops, it scales down toward zero, eliminating idle costs and the need to over-provision. It also simplifies operations since there's no server provisioning or maintenance. In contrast, long-running, stateful workloads with low cold-start latency can suffer from startup delays and managing state across ephemeral executions. Predictable, constant high CPU usage isn't ideal for serverless due to per-invocation costs and scaling behavior, and applications requiring persistent connections can hit limits and latency issues.

5. Which cloud capability allows a system to automatically adjust resources in response to load without manual intervention?

A. Auto-scaling

B. Elasticity

C. Load balancing

D. High availability

Elasticity is the cloud capability that automatically increases or decreases resources in response to demand, without human intervention. When the load goes up, the system can add more compute or storage; when it goes down, it can release resources. This automatic adjustment helps maintain performance while controlling costs. A common way to achieve elasticity is through auto-scaling, which dynamically provisions or deprovisions resources based on monitored metrics. Load balancing distributes traffic across existing resources but doesn't by itself change the total amount of resources, and high availability focuses on uptime and redundancy rather than automatic scaling.

6. Which metric defines the maximum acceptable downtime for an IT service during a disruption?

A. Recovery Time Objective

B. Recovery Point Objective

C. Mean Time To Repair

D. Uptime

The maximum acceptable downtime during a disruption is defined by the Recovery Time Objective. It sets the time window within which the IT service must be restored after an outage to prevent unacceptable business impact, guiding how you design and implement recovery strategies (like failover, backups, and automation) to meet that target. Recovery Point Objective covers how much data loss is tolerable, expressed as the age of the data that can be lost; Mean Time To Repair is the average time to fix a fault, an operational metric about repair speed; and uptime describes how often a service is available, but does not specify the allowed downtime duration.

7. For disaster recovery, which approach minimizes downtime by maintaining a copy of data at a remote site?

A. Local backups

B. Cloud backups

C. Replication to a remote site

D. Tape backup only

Maintaining a copy of data at a remote site through replication minimizes downtime because the disaster recovery site already has an up-to-date copy of the data and can take over quickly. With replication, the remote environment stays in sync with the primary, so switching over to the DR site can happen almost immediately, often with little or no data loss depending on whether the replication is synchronous or asynchronous. Local backups require a restore process to bring services back online, which takes time. Cloud or tape backups involve locating, transferring, and restoring data, adding further delay. Replication provides the fastest path to availability by keeping the data ready at the remote site.

8. In an identity federation setup between on-premises Active Directory and cloud identities, which practice helps maintain consistent access control across environments?

A. Disable MFA to reduce friction.

B. Use only cloud accounts without on-prem identity.

C. Avoid any group synchronization and rely on user passwords.

D. Enforce MFA and synchronize groups and roles.

When you have a federation between on-premises Active Directory and cloud identities, the goal is to have authentication and authorization decisions feel seamless across environments. That means enforcing a strong, consistent authentication method and making sure the same group and role assignments exist in both places so permissions line up. Enforcing MFA across the board provides a uniform, stronger check on who is signing in, reducing the risk of compromised credentials and ensuring that access policies apply equally whether users are authenticating on-prem or in the cloud. At the same time, synchronizing groups and roles ensures that membership changes in the on-prem directory are reflected in the cloud, and vice versa, so entitlements and permissions remain aligned. This combination keeps access control consistent and manageable across environments. Disabling MFA weakens security and creates divergent authentication behavior between on-prem and cloud. Relying only on cloud accounts without the on-prem identity breaks the federated model and can lead to drift between environments. Not syncing groups and relying on passwords alone creates inconsistent permissions and undermines centralized governance.

9. For a globally deployed application that requires redundancy and fast data access, which storage method is most suitable?

A. Local storage

B. Multi-regional

C. Cold storage

D. NAS

The key idea is delivering data from multiple geographic regions to keep access fast for users worldwide while staying resilient to regional failures. Multi-regional storage replicates data across several regions, so users connect to the closest region, which minimizes latency, and if one region experiences an outage, others keep serving data. That combination of low latency for a global audience and built-in redundancy makes it the best fit for a globally deployed application. Local storage holds data in a single location, so it has no built-in cross-region redundancy and can suffer from higher latency or outages affecting everyone. Cold storage is designed for long-term archival and rarely accessed data, so retrieval is slow and expensive, not suitable for fast data access. NAS is typically tied to a single network or data center, offering centralized storage but not inherently distributed globally, which leads to higher latency for distant users and adds complexity to achieve global redundancy.

10. When data gravity is a factor, what is a best practice for architecture placement of compute and storage?

A. Move data to where compute resides

B. Remove data to avoid gravity

C. Place compute near the data

D. Data gravity has no impact

Data gravity describes how large datasets pull workloads toward them because moving that data is expensive in terms of bandwidth, latency, and cost. When data gravity is a factor, the best architectural move is to place compute near the data so processing happens where the data resides. This minimizes cross-network transfers, reducing latency and bandwidth usage while lowering data-egress costs, which is crucial for analytics and big data workloads. Trying to move the data to the compute location would still incur substantial data transfer overhead as datasets grow, making it less scalable. Suggesting that data gravity has no impact ignores real constraints in cloud environments, and simply removing data isn't a practical or scalable solution.

Next Steps

Congratulations on reaching the final section of this guide. You've taken a meaningful step toward passing your certification exam and advancing your career.

As you continue preparing, remember that consistent practice, review, and self-reflection are key to success. Make time to revisit difficult topics, simulate exam conditions, and track your progress along the way.

If you need help, have suggestions, or want to share feedback, we'd love to hear from you. Reach out to our team at hello@examzify.com.

Or visit your dedicated course page for more study tools and resources:

https://comptiacloudpluspostassmt.examzify.com

We wish you the very best on your exam journey. You've got this!