MICROSOFT CERTIFIED: AZURE FUNDAMENTALS (AZ-900) PRACTICE EXAM (SAMPLE)

STUDY GUIDE

Prepare with structure. Pass with confidence

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. **Which Azure feature gives the ability to manage user credentials securely?**

   A. Azure Active Directory

   B. Azure Key Vault

   C. Azure AD Connect

   D. Azure Information Protection

2. **Which option comes with the maximum responsibility for the customer?**

   A. IaaS

   B. PaaS

   C. SaaS

   D. Equal in all options

3. **Which Azure product is primarily used for building and managing virtual machines?**

   A. Azure Functions

   B. Azure Virtual Machines

   C. Azure Kubernetes Service

   D. Azure Container Instances

4. **What helps protect Azure SQL Database and Azure Data Warehouse against the threat of malicious activity?**

   A. Transparent Data Encryption (TDE)

   B. Azure Storage Service Encryption

   C. Azure Disk Encryption

   D. All of the above

5. **What is a feature of Azure Active Directory?**

   A. B2B identity services

   B. Application management

   C. Single Sign-On (SSO)

   D. All of the above

6. What is the benefit of using managed disks over unmanaged disks?

A. Lower cost

B. Higher performance

C. No storage account required

D. More capacity options

7. Which Azure service should you use to centrally manage certificates?

A. MSIP

B. Azure AD

C. Azure Key Vault

D. Azure ATP

8. What is a primary benefit of using Azure's serverless architecture?

A. Always on services

B. No management needed

C. Enhanced security

D. Structured data storage

9. What is the process of managing and assigning policy definitions by grouping a set of policies into a single item?

A. Grouping

B. Cluster

C. Initiative

D. Startup

10. What is the primary focus of the NIST Cybersecurity Framework?

A. Data storage solutions

B. Cybersecurity risk management

C. Project management

D. Compliance auditing

Answers

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

Explanations

1. Which Azure feature gives the ability to manage user credentials securely?

A. Azure Active Directory

B. Azure Key Vault

C. Azure AD Connect

D. Azure Information Protection

The feature that provides the ability to manage user credentials securely is Azure Active Directory. This service acts as a cloud-based identity and access management solution, allowing organizations to manage user identities, authenticate users, and control access to resources securely. Azure Active Directory includes features like multi-factor authentication, self-service password reset, and conditional access policies that help in maintaining secure credentials management. While Azure Key Vault is designed for securely storing and managing sensitive information such as secrets, encryption keys, and certificates, it does not specifically focus on user credentials and identity management. Conversely, Azure AD Connect is primarily used to synchronize on-premises directories with Azure Active Directory, and Azure Information Protection helps in classifying and protecting documents and emails but does not handle user credentials. Therefore, Azure Active Directory is the comprehensive solution for managing user identities and credentials securely.

2. Which option comes with the maximum responsibility for the customer?

A. IaaS

B. PaaS

C. SaaS

D. Equal in all options

The option that comes with the maximum responsibility for the customer is indeed Infrastructure as a Service (IaaS). In an IaaS model, customers are responsible for managing everything from the operating system up to the applications they deploy. This includes not only the operating system but also networking, storage, and servers. Essentially, IaaS provides the most control to the customer because they have to handle the maintenance and management of the infrastructure while the cloud provider only manages the underlying physical hardware. This model is suited for users who need dynamic and flexible resources, giving them the freedom to manage their IT environment according to their specific needs. In contrast, Platform as a Service (PaaS) takes care of the underlying infrastructure and the platform where applications run, allowing customers to focus more on application development rather than hardware management. Software as a Service (SaaS) abstracts even further, where the provider manages everything, including applications, and users simply access the software over the internet. In summary, with IaaS, customers bear the most responsibility compared to PaaS and SaaS, making it the correct answer for maximum customer responsibility.

3. Which Azure product is primarily used for building and managing virtual machines?

A. Azure Functions

B. Azure Virtual Machines

C. Azure Kubernetes Service

D. Azure Container Instances

Azure Virtual Machines is the correct choice for building and managing virtual machines in the Azure cloud. This service allows users to deploy and manage VMs quickly and easily, giving them the flexibility to run applications and workloads in a virtualized environment. It provides full control over the VM infrastructure with complete customization options related to operating systems, configurations, and application deployment. Azure Functions is primarily designed for serverless computing, allowing developers to run event-driven code without having to explicitly provision or manage servers. It is more focused on executing small pieces of code in response to events rather than managing virtual machines. Azure Kubernetes Service is a container orchestration service, which is used to manage and scale containerized applications through Kubernetes. While it might be related to virtualization in a broader sense, its primary purpose is not to create and manage traditional virtual machines but rather to manage containers. Azure Container Instances is a service that allows you to run containers without managing virtual machines or adopting a higher-level container orchestration service like Kubernetes. It provides a simpler way to run containers but does not focus on the management of VMs in the same way Azure Virtual Machines does.

4. What helps protect Azure SQL Database and Azure Data Warehouse against the threat of malicious activity?

A. Transparent Data Encryption (TDE)

B. Azure Storage Service Encryption

C. Azure Disk Encryption

D. All of the above

The correct answer is the option that emphasizes Transparent Data Encryption (TDE). TDE is specifically designed to protect Azure SQL Database and Azure Data Warehouse from malicious activities by encrypting the data at rest. This ensures that sensitive information is safeguarded, even if unauthorized access to the underlying storage occurs. TDE helps to mitigate risks of data breaches and compliance violations by protecting the databases without requiring extensive application changes. While other options also provide significant encryption benefits within Azure, they are not as directly tied to the protection of Azure SQL Database and Azure Data Warehouse specifically against malicious activity. Azure Storage Service Encryption is aimed at Azure Storage accounts, while Azure Disk Encryption pertains primarily to virtual machines. Therefore, although all these encryption methods contribute to a secure Azure environment, TDE is uniquely focused on SQL databases, making it the most relevant answer regarding the protection of Azure SQL Database and Azure Data Warehouse from threats specifically tied to data breaches.

5. What is a feature of Azure Active Directory?

A. B2B identity services

B. Application management

C. Single Sign-On (SSO)

D. All of the above

All of the mentioned features—B2B identity services, application management, and Single Sign-On (SSO)—are integral components of Azure Active Directory (Azure AD). B2B identity services allow organizations to securely share their applications and services with guest users from any organization while maintaining control over their own data. This capability facilitates collaboration between businesses and enhances productivity. Application management is a crucial feature that provides the ability to manage applications; this includes adding, configuring, and controlling access to applications, ensuring that users can access the resources they need while maintaining security and compliance. Single Sign-On (SSO) enables users to log in once and gain access to multiple applications without being prompted for credentials repeatedly. This not only improves the user experience by streamlining access to applications but also enhances security by managing authentication more effectively. Given that all these features are essential and work together to provide a robust identity and access management solution in Azure, the comprehensive option indicating all these features accurately reflects Azure Active Directory's offerings.

6. What is the benefit of using managed disks over unmanaged disks?

A. Lower cost

B. Higher performance

C. No storage account required

D. More capacity options

Using managed disks presents the significant advantage of not requiring a separate storage account. With managed disks, Azure handles the storage account creation and management behind the scenes, simplifying the process of provisioning and managing disks. This eliminates the need for users to manually create and manage an Azure storage account to hold the disks, allowing for easier scalability and management. Managed disks also benefit from enhanced reliability and performance due to Azure managing the underlying storage. However, the key differentiator remains the streamlined process of not needing to deal with the complexities of storage accounts, which is a major factor for many users adopting Azure services. In summary, while other factors like cost, performance, and capacity options are important, the lack of a need for a separate storage account is a prominent benefit that leads to reduced complexity in managing your Azure resources.

7. Which Azure service should you use to centrally manage certificates?

A. MSIP

B. Azure AD

C. Azure Key Vault

D. Azure ATP

The correct answer is Azure Key Vault, which is specifically designed for securely storing and managing cryptographic keys, secrets, and certificates. This service allows organizations to centrally manage their certificates, ensuring that they are stored securely and accessed only by authorized applications and users. Azure Key Vault provides various features that make certificate management efficient, such as automatic certificate renewal, which simplifies maintenance processes. Additionally, it integrates with other Azure services, which enhances its functionality and allows for greater security and ease of use. Using Azure Key Vault for certificate management not only helps in maintaining compliance with security policies but also reduces the risk of unauthorized access and potential data breaches. Its role in centralized management and security makes it the preferred choice for handling certificates in an Azure environment. Other options, while valuable for various tasks in Azure, do not specifically cater to the centralized management of certificates.

8. What is a primary benefit of using Azure's serverless architecture?

A. Always on services

B. No management needed

C. Enhanced security

D. Structured data storage

The primary benefit of using Azure's serverless architecture is that it eliminates the need for management. This model allows developers to focus on building applications and writing code without worrying about the underlying infrastructure, server provisioning, or maintenance. In a serverless environment, resources are automatically managed by Azure, scaling up or down according to demand, which leads to efficient resource use and reduced operational overhead. This allows for faster development cycles and enables teams to concentrate on delivering value through their applications rather than managing servers. The other options provided, while they may have benefits in different contexts, do not capture the primary advantage of serverless architecture as effectively. Always-on services imply a constant availability that may not align with the pay-as-you-go model of serverless computing. Enhanced security is indeed a consideration with any cloud service, but it is not a unique feature of serverless architecture. Structured data storage relates more to database services that Azure provides, which doesn't directly pertain to the serverless concept.

9. What is the process of managing and assigning policy definitions by grouping a set of policies into a single item?

A. Grouping

B. Cluster

C. Initiative

D. Startup

The correct answer is initiative. In the context of Azure policy management, an initiative is a collection of policy definitions that are grouped together. This approach simplifies the management process, allowing you to apply a set of related policies as a single entity. It enables better organization and governance of resources within an Azure environment, as you can define compliance rules that address multiple aspects of resource management by combining specific policies into one cohesive unit. This is particularly useful for large environments where managing individual policy definitions could become cumbersome and inefficient. By implementing initiatives, organizations can ensure comprehensive policy coverage and compliance across their Azure resources. Grouping, clustering, and startup do not accurately reflect this specific process within Azure policy management. Grouping can refer to putting things together, but it does not have the precise meaning that initiative conveys in this context. Clustering is more often associated with data grouping for performance or availability rather than policy management. Startup generally relates to the initialization of applications or services, making it unrelated to the grouping of policy definitions.

10. What is the primary focus of the NIST Cybersecurity Framework?

A. Data storage solutions

B. Cybersecurity risk management

C. Project management

D. Compliance auditing

The primary focus of the NIST Cybersecurity Framework is indeed on cybersecurity risk management. This framework was developed to help organizations better manage and reduce cybersecurity risk and to improve their ability to respond to and recover from cyber incidents. It provides a policy framework of computer security guidance for how organizations can assess and improve their ability to prevent, detect, and respond to cyber attacks. The framework is structured around five core functions: Identify, Protect, Detect, Respond, and Recover. These functions help organizations to understand their cybersecurity risks, protect their systems and data, detect cybersecurity events, respond effectively to incidents, and recover from any disruptions. By focusing on risk management, the framework allows organizations to tailor their cybersecurity posture to their specific needs, circumstances, and risk tolerance. While data storage solutions, project management, and compliance auditing can play important roles in the broader context of information technology and security, they do not encapsulate the central goal of the NIST Cybersecurity Framework. This framework is distinctly designed to enhance the understanding and management of cybersecurity risks, making it a vital tool for organizations aiming to strengthen their cybersecurity strategies.

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://az900.examzify.com

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