MICROSOFT AZURE SECURITY TECHNOLOGIES (AZ-500) PRACTICE TEST (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://microsoftazuresecuritytechnologies-az500.examzify.com

Copyright © 2026 by Examzify - A Kaluba Technologies Inc. product.

ALL RIGHTS RESERVED.

No part of this book may be reproduced or transferred in any form or by any means, graphic, electronic, or mechanical, including photocopying, recording, web distribution, taping, or by any information storage retrieval system, without the written permission of the author.

Notice: Examzify makes every reasonable effort to obtain accurate, complete, and timely information about this product from reliable sources.

SAMPLE

Table of Contents

Copyright 1

Table of Contents 2

Introduction 3

How to Use This Guide 4

Questions 5

Answers 8

Explanations 10

Next Steps 16

SAMPLE

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.

SAMPLE

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!

SAMPLE

Questions

SAMPLE

1. **What must be installed on an Azure virtual machine to ensure Docker containers can access Azure Storage and Azure SQL databases via a service endpoint?**

   A. Create an application security group

   B. Install the container network interface (CNI) plug-in

   C. Create an AKS Ingress controller

   D. Deploy an Azure Load Balancer

2. **Which Azure feature enhances compliance for data protection globally?**

   A. Azure Blueprints

   B. Azure Monitor

   C. Azure Policy

   D. Azure Key Vault

3. **Which compliance manager helps organizations manage their compliance needs in Azure?**

   A. Microsoft Security Manager

   B. Microsoft Compliance Manager

   C. Azure Governance Manager

   D. Azure Compliance Tool

4. **Which Azure feature allows secure management of application credentials?**

   A. Azure Storage Accounts

   B. Azure Key Vault

   C. Azure Resource Manager

   D. Azure Monitor

5. **What pricing tier is required to modify operating system security configurations via Azure Security Center?**

   A. Advanced

   B. Premium

   C. Standard

   D. Free

SAMPLE

6. Which identity management feature in Azure helps with identity governance?

A. Azure Multi-Factor Authentication

B. Azure Active Directory Access Reviews

C. Azure Resource Manager

D. Azure Policy Compliance

7. Which action is required to create custom alert rules in Azure Security Center after creating an Azure subscription?

A. You should create an Azure Log Analytics workspace.

B. You should create a DLP policy.

C. You should make sure that Azure AD Identity Protection is removed.

D. You should make sure that Security Center has the necessary tier configured.

8. When creating a custom role-based access control (RBAC), which property must you configure to read an Azure Storage account?

A. NotActions []

B. DataActions []

C. AssignableScopes []

D. Actions []

9. What feature does Azure Key Vault provide to manage certificates?

A. Automated expiration alerts

B. Rapid deployment capabilities

C. Version control for secrets

D. Secure storage and access policies

10. Will creating a new stored access policy revoke access to an Azure Storage account?

A. Yes

B. No

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. What must be installed on an Azure virtual machine to ensure Docker containers can access Azure Storage and Azure SQL databases via a service endpoint?

A. Create an application security group

B. Install the container network interface (CNI) plug-in

C. Create an AKS Ingress controller

D. Deploy an Azure Load Balancer

To enable Docker containers running on an Azure virtual machine to access Azure Storage and Azure SQL databases via a service endpoint, it is necessary to install the container network interface (CNI) plug-in. The CNI plug-in is vital as it facilitates advanced networking capabilities for the containers, allowing them to connect securely to Azure resources over the virtual network. By installing the CNI plug-in, the containers can utilize Azure's networking features, such as service endpoints. This enhances communication with Azure services by providing direct access to the Azure backbone instead of routing traffic over the public internet. As a result, data transfer becomes more secure and efficient. The other alternatives do not provide the specific functionality required for secure network access from Docker containers to Azure services. Creating an application security group primarily focuses on managing network security in Azure, while an AKS Ingress controller is related to managing external access to services within Azure Kubernetes Service, not standalone virtual machines. Deploying an Azure Load Balancer is relevant for distributing network traffic but does not directly affect a container's access to Azure Storage or SQL databases through service endpoints.

2. Which Azure feature enhances compliance for data protection globally?

A. Azure Blueprints

B. Azure Monitor

C. Azure Policy

D. Azure Key Vault

The feature that enhances compliance for data protection globally is Azure Policy. This service enables organizations to create, assign, and manage policies that enforce specific rules and effects over their resources, ensuring that they adhere to desired compliance standards. Azure Policy helps maintain compliance by assessing resources against your set of rules and providing insights into non-compliant resources. It allows organizations to implement policies that target specific regulatory requirements, such as GDPR, HIPAA, or ISO standards, streamlining the process of ensuring compliance across various geographic regions. By defining policy rules, Azure Policy helps automate compliance checks and can even enforce real-time policy compliance by preventing non-compliant resources from being created in the first place. This proactive approach not only enhances data protection but also minimizes the risk associated with potential non-compliance, leading to improved governance and security postures across the organization. The other features mentioned, while valuable for other aspects of Azure security and management, do not focus specifically on enforcing compliance for data protection as Azure Policy does. Azure Blueprints primarily aid in the deployment and management of compliant environments, Azure Monitor provides insights into performance and health, and Azure Key Vault is focused on securing keys and secrets rather than overall policy compliance.

SAMPLE

3. Which compliance manager helps organizations manage their compliance needs in Azure?

A. Microsoft Security Manager

B. Microsoft Compliance Manager

C. Azure Governance Manager

D. Azure Compliance Tool

The correct answer is Microsoft Compliance Manager, which is a dedicated tool that assists organizations in managing their compliance requirements effectively within the Azure environment. This service helps businesses adhere to regulatory requirements and standards by providing a centralized dashboard that tracks compliance status, offers assessments, and provides recommendations for compliance improvements. Microsoft Compliance Manager integrates with Microsoft 365 and other cloud services, enabling organizations to assess their compliance posture against a variety of regulations and standards, such as GDPR, ISO 27001, and HIPAA. It offers features like risk assessments, actionable insights, and detailed reporting, making it a vital component for businesses seeking to navigate the complex landscape of data protection and compliance. The other options, while they may sound relevant, do not specifically focus on compliance management in the same way. For instance, the Microsoft Security Manager typically focuses on security aspects rather than compliance, the Azure Governance Manager deals with managing governance policies and resource allocation rather than compliance directly, and the Azure Compliance Tool isn't a recognized service in managing compliance needs in Azure. Hence, Microsoft Compliance Manager stands out as the most appropriate choice for compliance management in the Azure context.

4. Which Azure feature allows secure management of application credentials?

A. Azure Storage Accounts

B. Azure Key Vault

C. Azure Resource Manager

D. Azure Monitor

Azure Key Vault is specifically designed for the secure management of application credentials, including secrets, keys, and certificates. It allows users to securely store sensitive information, providing features that enable applications to access that information securely without hardcoding it into application code. Key Vault helps enhance security by providing access control policies, which allow you to manage access to the credentials based on the principle of least privilege. This means you can specify who or what can access the stored secrets. Additionally, Key Vault integrates seamlessly with other Azure services, making it easier for applications to pull required secrets during deployment and runtime. Using Azure Key Vault minimizes the risk of exposure to sensitive information because it centralizes credential management and reduces the chances of credentials being accidentally revealed in source code or logs.

SAMPLE

5. What pricing tier is required to modify operating system security configurations via Azure Security Center?

A. Advanced

B. Premium

C. Standard

D. Free

The Standard pricing tier is the appropriate choice for modifying operating system security configurations via Azure Security Center. This tier includes enhanced security features that go beyond basic monitoring and compliance. Specifically, it provides capabilities such as the ability to assess and perform security recommendations for your operating systems, manage security policies, and detect vulnerabilities. With the Standard tier, organizations gain access to valuable tools and functionalities that enable them to proactively address security configurations and maintain robust security postures. This tier is designed for organizations looking to implement comprehensive security measures across their Azure resources, making it essential for users needing to modify operating system security settings effectively. In contrast, the Free tier offers limited features focused mainly on basic security posture management and visibility, while the Advanced and Premium tiers focus on additional services and integrations that may not directly relate to modifying security configurations. Therefore, the Standard tier stands out as the necessary option for managing operating system security configurations within Azure Security Center.

6. Which identity management feature in Azure helps with identity governance?

A. Azure Multi-Factor Authentication

B. Azure Active Directory Access Reviews

C. Azure Resource Manager

D. Azure Policy Compliance

Azure Active Directory Access Reviews is a critical feature for identity governance in Azure. It allows organizations to regularly review and manage users' access to applications and resources within the Azure environment. By conducting access reviews, administrators can ensure that only the right users have access to the necessary resources, which helps in maintaining security compliance and reducing the risk of unauthorized access. This feature enables organizations to automate and streamline the process of verifying user access against business requirements. It facilitates periodic reviews where managers can approve or revoke access based on current roles and responsibilities. As a result, it fosters accountability and ensures that access rights are aligned with the principle of least privilege. In the context of identity governance, which focuses on managing identities and their access rights effectively, Azure Active Directory Access Reviews stands out as the most relevant feature.

SAMPLE

7. Which action is required to create custom alert rules in Azure Security Center after creating an Azure subscription?

A. You should create an Azure Log Analytics workspace.

B. You should create a DLP policy.

C. You should make sure that Azure AD Identity Protection is removed.

D. You should make sure that Security Center has the necessary tier configured.

Creating custom alert rules in Azure Security Center primarily involves setting up the right environment to analyze and respond to security threats effectively. The action necessary for this process is to ensure that Security Center has the appropriate tier configured. Azure Security Center operates in different tiers, namely Free and Standard, with the Standard tier providing enhanced capabilities, including advanced threat protection, the ability to create custom alert rules, and additional security management features. To set up custom alert rules, users must upgrade to the Standard tier because custom rules are not available in the Free tier. This tier provides greater functionality to monitor and respond to security incidents, making it essential for organizations seeking to implement tailored security measures in Azure. While creating an Azure Log Analytics workspace can enhance data exploration and analysis, particularly when it comes to querying logs and analytics data, it is not a direct requirement for creating custom alert rules in Azure Security Center itself. Similarly, DLP policies and the management of Azure AD Identity Protection do not pertain to the creation of custom alert rules within the context of Azure Security Center's operational capabilities.

8. When creating a custom role-based access control (RBAC), which property must you configure to read an Azure Storage account?

A. NotActions []

B. DataActions []

C. AssignableScopes []

D. Actions []

To read an Azure Storage account when creating a custom role-based access control (RBAC), the property that must be configured is the Actions property. This property defines the operations that users assigned to the role are allowed to perform on Azure resources. In the context of Azure Storage, to enable read access, the appropriate actions related to reading data, such as "Microsoft.Storage/storageAccounts/read" and potentially others that pertain to reading blob or file data, need to be included within the Actions property. These actions specify the permissions granted to users under this role. Other properties like NotActions are used to explicitly deny certain actions even if they are generally allowed by other roles. DataActions, on the other hand, are utilized for actions that specifically pertain to data plane operations but are not used to define basic permissions like reading a storage account. AssignableScopes is a property that identifies where the custom role can be assigned, such as at the subscription or resource group level, but does not define what actions the role allows. Thus, the Actions property is essential for specifying the permissions required to read from Azure Storage accounts.

SAMPLE

9. What feature does Azure Key Vault provide to manage certificates?

A. Automated expiration alerts

B. Rapid deployment capabilities

C. Version control for secrets

D. Secure storage and access policies

Azure Key Vault is designed to securely manage cryptographic keys and secrets used by cloud applications and services, and one of its important features regarding certificates is secure storage and access policies. Key Vault allows you to store certificates in a secure manner, providing a central place to manage all your certificates, which ensures that sensitive data is well-protected. In addition to secure storage, Azure Key Vault also offers robust access policy configurations that allow you to control who can access the certificates and what operations they can perform on them. This level of control is essential for maintaining security and compliance within an organization. The other features mentioned have their own merits, but they don't specifically capture the essence of what Azure Key Vault offers for certificate management. For instance, automated expiration alerts can be useful for reminders but are not a primary function of Key Vault. Rapid deployment capabilities may relate to how you use Key Vault, and version control for secrets is an important aspect but isn't directly aligned with the main function of certificates within Key Vault. Therefore, secure storage and access policies is the defining feature that Azure Key Vault provides to manage certificates effectively.

10. Will creating a new stored access policy revoke access to an Azure Storage account?

A. Yes

B. No

Creating a new stored access policy does not revoke access to an Azure Storage account; rather, it serves as a mechanism for managing and controlling access permissions to the resources associated with that storage account. A stored access policy is essentially a named set of permissions that can be applied to shared access signatures (SAS). When you create a new stored access policy, it defines a set of permissions, start and expiry times, and allows you to update those parameters without having to regenerate the SAS token. Existing SAS tokens that were issued with earlier policies remain unaffected unless specifically updated or invalidated. This ability to create stored access policies enhances the management of access rights, but it does not directly revoke access. Any access defined by existing SAS tokens continues to function until those tokens expire or are explicitly revoked. Thus, creating a new policy does not disrupt any existing access that might be granted via current SAS tokens associated with previous access policies or directly with the storage account itself.

SAMPLE

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://microsoftazuresecuritytechnologies-az500.examzify.com

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

SAMPLE