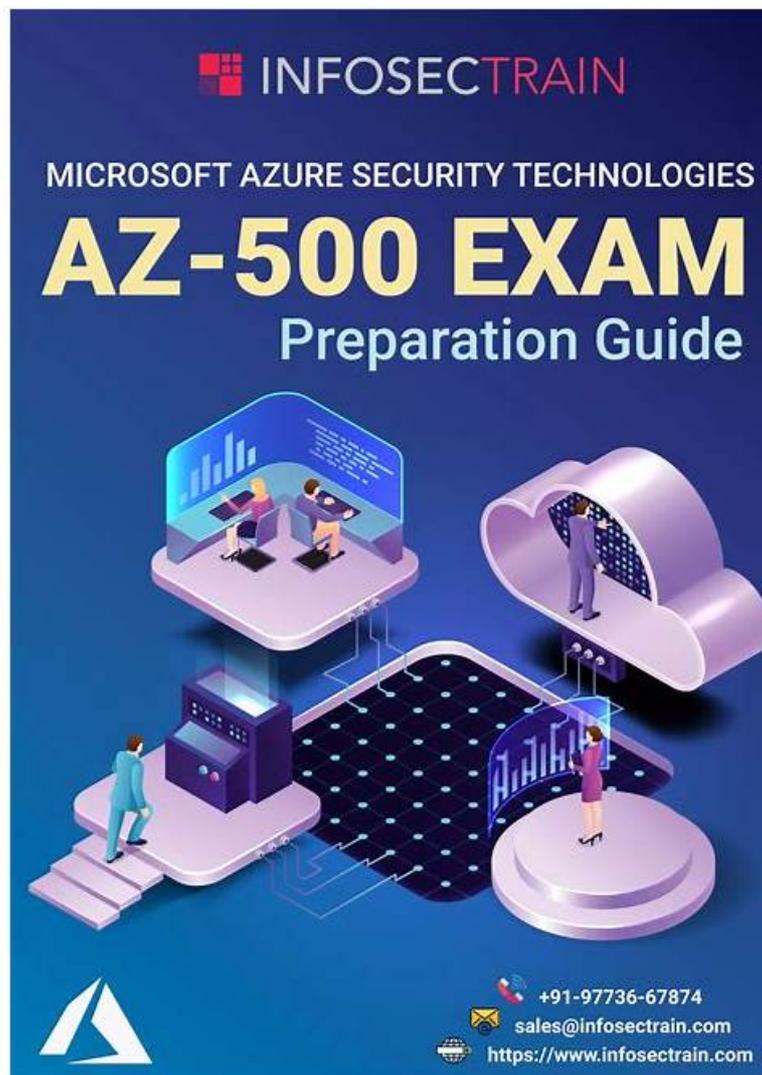


# AZ-500 Exam Sample, AZ-500 Latest Exam Pdf



BONUS!!! Download part of Itcerttest AZ-500 dumps for free: <https://drive.google.com/open?id=1LzP0yuBDxGqdBUDEgo9w9MsOXkMy7Aw3>

You can learn our AZ-500 test prep in the laptops or your cellphone and study easily and pleasantly as we have different types, or you can print our PDF version to prepare your exam which can be printed into papers and is convenient to make notes. Studying our AZ-500 exam preparation doesn't take you much time and if you stick to learning you will finally pass the exam successfully. Believe us because the AZ-500 Test Prep are the most useful and efficient, and the AZ-500 exam preparation will make you master the important information and the focus to pass the AZ-500 exam.

The Microsoft Azure Security Technologies certification exam covers a wide range of security topics such as identity and access management, platform protection, data and application protection, and security operations. AZ-500 Exam is designed to test the candidate's ability to implement and manage security controls across various Azure services, including Azure Active Directory, Azure Security Center, Azure Key Vault, and Azure Information Protection.

>> AZ-500 Exam Sample <<

## AZ-500 Latest Exam Pdf - AZ-500 Exams Training

The format name of AZ-500 practice test questions is APICS PDF Questions file, desktop practice test software, and web-based practice test software. Choose the nay type of AZ-500 Practice Exam Questions that fit your AZ-500 exam preparation requirement and budget and start preparation without wasting further time.

The tech industry has been growing at a very fast pace and anyone who is related to it needs to grow with it. If the IT professionals are slow to adopt and learn the latest technologies, they may be left behind, which can hurt their careers. In the IT field, one of the best ways to make sure that you are learning new skills is with the help of certifications.

One of the best certification providers right now is Microsoft, which offers a ton of badges that can define your career. Among those certificates, we recommend that you pay attention to Microsoft Certified: Azure Security Engineer Associate. It is the perfect choice for those who want to become a security engineer. However, to earn this credential, you will need to take the Microsoft AZ-500 Exam and ace it with flying colors. In this post, we will learn everything about this test to help you understand what you can expect from it.

## Microsoft Azure Security Technologies Sample Questions (Q119-Q124):

### NEW QUESTION # 119

You have an Azure Active Directory (Azure AD) tenant that contains the users shown in the following table.

Name	Member of	Multi-factor authentication (MFA) status
User1	Group1, Group2	Disabled
User2	Group2	Disabled

The tenant contains the named locations shown in the following table.

Name	IP address range	Trusted location
Seattle	193.77.10.0/24	Yes
Boston	154.12.18.0/24	No

You create the conditional access policies for a cloud app named App1 as shown in the following table.

Name	Include	Exclude	Condition	Grant
Policy1	Group1	Group2	Locations: Boston	Block access
Policy2	Group1	None	Locations: Any location	Grant access, Require multi-factor authentication
Policy3	Group2	Group1	Locations: Boston	Block access
Policy4	User2	None	Locations: Any location	Grant access, Require multi-factor authentication

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

**Answer Area**

Microsoft

Statements	Yes	No
User1 can access App1 from an IP address of 154.12.18.10.	<input type="radio"/>	<input type="radio"/>
User2 can access App1 from an IP address of 193.77.10.15.	<input type="radio"/>	<input type="radio"/>
User2 can access App1 from an IP address of 154.12.18.34.	<input type="radio"/>	<input type="radio"/>

**Answer:**

**Explanation:**

Answer Area



Statements

User1 can access App1 from an IP address of 154.12.18.10.

Yes  No

User2 can access App1 from an IP address of 193.77.10.15.

Yes  No

User2 can access App1 from an IP address of 154.12.18.34.

Yes  No

Explanation

Statements	Yes	No
User1 can access App1 from an IP address of 154.12.18.10.	<input type="radio"/>	<input checked="" type="radio"/>
User2 can access App1 from an IP address of 193.77.10.15.	<input checked="" type="radio"/>	<input type="radio"/>
User2 can access App1 from an IP address of 154.12.18.34.	<input type="radio"/>	<input checked="" type="radio"/>

NEW QUESTION # 120

You need to ensure that User2 can implement PIM. What should you do first?

- A. Configure the identity secure score for contoso.com.
- B. Configure authentication methods for contoso.com.
- C. Assign User2 the Global administrator role.
- D. Enable multi-factor authentication (MFA) for User2.

Answer: D

Explanation:  
Explanation

To start using PIM in your directory, you must first enable PIM.

1. Sign in to the Azure portal as a Global Administrator of your directory.

You must be a Global Administrator with an organizational account (for example, @yourdomain.com), not a Microsoft account (for example, @outlook.com), to enable PIM for a directory.

Scenario: Technical requirements include: Enable Azure AD Privileged Identity Management (PIM) for contoso.com References: <https://docs.microsoft.com/bs-latn-ba/azure/active-directory/privileged-identity-management/pim-getting-starte>

NEW QUESTION # 121

You have an Azure subscription that contains an Azure Sentinel workspace.

Azure Sentinel is configured to ingest logs from several Azure workloads. A third-party service management platform is used to manage incidents.

You need to identify which Azure Sentinel components to configure to meet the following requirements:

\* When Azure Sentinel identifies a threat, an incident must be created.

\* A ticket must be logged in the service management platform when an incident is created in Azure Sentinel.

Which component should you identify for each requirement? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

When Azure Sentinel identifies a threat, an incident must be created:

A ticket must be logged in the service management platform when an incident is created in Azure Sentinel:

▼
Analytics
Data connectors
Playbooks
Workbooks

▼
Analytics
Data connectors
Playbooks
Workbooks

**Answer:**

Explanation:

When Azure Sentinel identifies a threat, an incident must be created:

A ticket must be logged in the service management platform when an incident is created in Azure Sentinel:

▼
Analytics
Data connectors
Playbooks
Workbooks

▼
Analytics
Data connectors
Playbooks
Workbooks

Explanation:

When Azure Sentinel identifies a threat, an incident must be created:

A ticket must be logged in the service management platform when an incident is created in Azure Sentinel:

▼
Analytics
Data connectors
Playbooks
Workbooks

▼
Analytics
Data connectors
Playbooks
Workbooks

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/create-incidents-from-alerts>

<https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook>

**NEW QUESTION # 122**

You have an Azure subscription that contains the virtual machines shown in the following table.

Name	Operating system
VM1	Windows Server 2016
VM2	Ubuntu Server 18.04 LTS

From Azure Security Center, you turn on Auto Provisioning. You deploy the virtual machines shown in the following table.

Name	Operating system
VM3	Windows Server 2016
VM4	Ubuntu Server 18.04 LTS

On which virtual machines is the Log Analytics agent installed?

- A. VM3 and VM4 only
- B. VM1 and VM3 only
- C. VM1, VM2, VM3, and VM4
- D. VM3 only

**Answer: C**

Explanation:

Explanation

When automatic provisioning is On, Security Center provisions the Log Analytics Agent on all supported Azure VMs and any new ones that are created.

Supported Operating systems include: Ubuntu 14.04 LTS (x86/x64), 16.04 LTS (x86/x64), and 18.04 LTS (x64) and Windows Server 2008 R2, 2012, 2012 R2, 2016, version 1709 and 1803 Reference:

<https://docs.microsoft.com/en-us/azure/security-center/security-center-enable-data-collection>

### NEW QUESTION # 123

You have an Azure subscription that contains an Azure key vault named KeyVault1 and the virtual machines shown in the following table.

Name	Private IP address	Public IP address	Connected to
VM1	10.7.0.4	51.144.245.152	VNET1/Default
VM2	10.8.0.4	104.45.9.227	VNET2/Default

You set the Key Vault access policy to Enable access to Azure Disk Encryption for volume encryption.

KeyVault1 is configured as shown in the following exhibit.

Save Discard Microsoft

Allow access from:  All networks  Selected networks

[Configure network access control for your key vault. Learn More](#)

Virtual networks: [+ Add existing virtual networks](#) [+ Add new virtual network](#)

VIRTUAL NETWORK	SUBNET	RESOURCE GROUP	SUBSCRIPTION
VNET1	default	RG1	...

Firewall: [i](#)

IPv4 ADDRESS OR CIDR

...

Exception:

Allow trusted Microsoft services to bypass this firewall? [i](#)  Yes  No

[i](#) This setting is related to firewall only. In order to access this key vault, the trusted service must also be given explicit permissions in the Access policies section.

For each of the following statements, select Yes if the statement is true. Otherwise, select No.



myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, fga.self-archive.com, Disposable vapes

What's more, part of that Itcerttest AZ-500 dumps now are free: <https://drive.google.com/open?id=1LzP0yuBDxGqdBUEgo9w9MsOXkMy7Aw3>