

# AZ-500<sup>Q&As</sup>

Microsoft Azure Security Technologies

## Pass Microsoft AZ-500 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.pass2lead.com/az-500.html>

100% Passing Guarantee  
100% Money Back Assurance

Following Questions and Answers are all new published by Microsoft  
Official Exam Center

- ⚙️ **Instant Download** After Purchase
- ⚙️ **100% Money Back** Guarantee
- ⚙️ **365 Days** Free Update
- ⚙️ **800,000+** Satisfied Customers



**QUESTION 1**

**HOTSPOT**

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

Name	Type	Attached to	NSG
NSG1	Network security group (NSG)	VM5	Not applicable
NSG2	Network security group (NSG)	Subnet1	Not applicable
Subnet1	Subnet	Not applicable	Not applicable
VM5	Virtual machine	Subnet1	NSG1

An IP address of 10.1.0.4 is assigned to VM5. VM5 does not have a public IP address. VM5 has just in time (JIT) VM access configured as shown in the following exhibit.

### JIT VM access configuration ✕

VM5

+ Add  
 📁 Save  
 ✕ Discard

---

Configure the ports for which the just-in-time VM access will be applicable

Port	Protocol	Allowed source IPs	IP range	Time range (hours)	
3389	Any	Per request	N/A	3 hours	...

You enable JIT VM access for VM5.

NSG1 has the inbound rules shown in the following exhibit.

Priority	Name	Port	Protocol	Source	Destination	Action
100	🚩 SecurityCenter-JITRule-...	3389	Any	Any	10.1.0.4	🟢 Allow
1000	SecurityCenter-JITRule_341...	3389	Any	Any	10.1.0.4	🔴 Deny
1001	RDP	3389	TCP	Any	Any	🟢 Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	🟢 Allow
65001	AllowAzureLoadBalancerIn...	Any	Any	AzureLoadBalancer	Any	🟢 Allow
65500	DenyAllInBound	Any	Any	Any	Any	🔴 Deny

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

NOTE: Each correct selection is worth one point.

Hot Area:

	Yes	No
Deleting the security rule that has a priority of 100 will revoke the approved JIT access request.	<input type="radio"/>	<input type="radio"/>
Remote Desktop access to VMS is blocked	<input type="radio"/>	<input type="radio"/>
An Azure Bastion host will enable Remote Desktop access to VMS from the internet	<input type="radio"/>	<input type="radio"/>

Correct Answer:

	Yes	No
Deleting the security rule that has a priority of 100 will revoke the approved JIT access request.	<input checked="" type="radio"/>	<input type="radio"/>
Remote Desktop access to VMS is blocked	<input checked="" type="radio"/>	<input type="radio"/>
An Azure Bastion host will enable Remote Desktop access to VMS from the internet	<input type="radio"/>	<input checked="" type="radio"/>

## QUESTION 2

### HOTSPOT

You have an Azure subscription named Sub 1 that is associated to an Azure Active Directory (Azure AD) tenant named contoso.com. The tenant contains the users shown in the following table.

Name	Type
User1	Global administrator
User2	Security administrator
User3	Security reader
User4	License administrator

Each user is assigned an Azure AD Premium P2 license.

You plan to onboard and configure Azure AD Identity Protection.

Which users can onboard Azure AD Identity Protection, remediate users, and configure policies? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

### Answer Area

Users who can onboard Azure AD Identity Protection:

	▼
User1 only	
User1 and User2 only	
User1,User2, and User3 only	
User1,User2, User3, and User4 only	

Users who can remediate users and configure policies:

	▼
User1 and User2 only	
User1 and User3 only	
User1, User2, and User3 only	
User1, User2, User3, and User4	

Correct Answer:

### Answer Area

Users who can onboard Azure AD Identity Protection:

	▼
User1 only	
User1 and User2 only	
User1,User2, and User3 only	
User1,User2, User3, and User4 only	

Users who can remediate users and configure policies:

	▼
User1 and User2 only	
User1 and User3 only	
User1, User2, and User3 only	
User1, User2, User3, and User4	

### QUESTION 3

HOTSPOT

You have an Azure SQL database named DB1 that contains a table named Table1.

You need to configure DB1 to meet the following requirements:

Sensitive data in Table1 must be identified automatically.

Only the first character and last character of the sensitive data must be displayed in query results.

Which two features should you configure? To answer, select the features in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

 Search (Ctrl+/)

 Auditing

 Ledger

 Data Discovery & Classification

 Dynamic Data Masking

 Microsoft Defender for Cloud

 Transparent data encryption

### Intelligent Performance

 Performance overview

 Performance recommendations

 Query Performance Insight

 Automatic tuning

### Monitoring

 Alerts

 Metrics

 Diagnostic settings

 Logs

Correct Answer:

 Search (Ctrl+/)

 Auditing

 Ledger

 Data Discovery & Classification

 Dynamic Data Masking

 Microsoft Defender for Cloud

 Transparent data encryption

### Intelligent Performance

 Performance overview

 Performance recommendations

 Query Performance Insight

 Automatic tuning

### Monitoring

 Alerts

 Metrics

 Diagnostic settings

 Logs



**QUESTION 4**

**DRAG DROP**

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

Name	Region	Description
HubVNet	East US	HubVNet is a virtual network connected to the on-premises network by using a site-to-site VPN that has BGP route propagation enabled. HubVNet contains subnets named HubVNetSubnet0 and GatewaySubnet. Virtual network gateway is connected to GatewaySubnet.
SpokeVNet	East US	SpokeVNet is a virtual network connected to HubVNet by using VNet peering. SpokeVNet contains subnets named SpokeVNetSubnet0 and AzureFirewallSubnet.

The Azure virtual machines on SpokeVNetSubnet0 can communicate with the computers on the on-premises network.

You plan to deploy an Azure firewall to HubVNet.

You create the following two routing tables:

1.

RT1: Includes a user-defined route that points to the private IP address of the Azure firewall as a next hop address

2.

RT2: Disables BGP route propagation and defines the private IP address of the Azure firewall as the default gateway

You need to ensure that traffic between SpokeVNetSubnet0 and the on-premises network flows through the Azure firewall.

To which subnet should you associate each route table? To answer, drag the appropriate subnets to the correct route tables. Each subnet may be used once, more than once, or not at all. You may need to drag the split bar between panes or

scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:

**Subnets**

- AzureFirewallSubnet
- GatewaySubnet
- SpokeVNetSubnet0

**Answer Area**

RT1:

RT2:

Correct Answer:

**Subnets**

- AzureFirewallSubnet
- GatewaySubnet
- SpokeVNetSubnet0

**Answer Area**

RT1:

RT2:

**QUESTION 5**

You need to deploy Microsoft Antimalware to meet the platform protection requirements. What should you do? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Hot Area:

**Answer Area**

Create a custom policy definition that has effect set to:

	▼
Append	
Deny	
DeployIfNotExists	

Create a policy assignment and modify:

	▼
The Create a Managed Identify setting	
The exclusion settings	
The scope	

Correct Answer:

**Answer Area**

Create a custom policy definition that has effect set to:

	▼
Append	
Deny	
DeployIfNotExists	

Create a policy assignment and modify:

	▼
The Create a Managed Identify setting	
The exclusion settings	
The scope	