

# Microsoft

## Exam Questions az-500

Microsoft Azure Security Technologies



**NEW QUESTION 1**

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

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

**Answer:** A

**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-started>

**NEW QUESTION 2**

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.  
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.  
You have a hybrid configuration of Azure Active Directory (AzureAD). You have an Azure HDInsight cluster on a virtual network.  
You plan to allow users to authenticate to the cluster by using their on-premises Active Directory credentials. You need to configure the environment to support the planned authentication.  
Solution: You deploy the On-premises data gateway to the on-premises network. Does this meet the goal?

- A. Yes
- B. No

**Answer:** B

**Explanation:**

Instead, you connect HDInsight to your on-premises network by using Azure Virtual Networks and a VPN gateway.  
▪ Note: To allow HDInsight and resources in the joined network to communicate by name, you must perform the following actions: Create Azure Virtual Network.  
▪ Create a custom DNS server in the Azure Virtual Network.  
▪ Configure the virtual network to use the custom DNS server instead of the default Azure Recursive Resolver. Configure forwarding between the custom DNS server and your on-premises DNS server.  
References:  
<https://docs.microsoft.com/en-us/azure/hdinsight/connect-on-premises-network>

**NEW QUESTION 3**

**HOTSPOT**  
You have an Azure Active Directory (Azure AD) tenant named contoso.com. The tenant contains the users shown in the following table.

Name	Role	Sign in frequency
User1	Password administrator	Sign in every work day
User2	Password administrator	Sign in bi-weekly
User3	Global administrator, Password administrator	Signs in every month

You configure an access review named Review1 as shown in the following exhibit.

Create an access review

Access reviews enable reviewers to attest to users access.

\* Review name

Review1

Description

\* Start date

2019-03-01

Frequency

One time

Duration (in days)

1

End

Never

End by

Occurrences

\* Number of times

0

\* End date

2019-03-20

Users

Scope

Everyone

\* Review role membership

Password administrator

Reviewers

Reviewers

Members(self)

Upon completion settings

Auto apply results to resource

Enable

Disable

Should reviewer not respond

Take recommendations

Advanced settings

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Hot Area:

### Answer Area

User3 can perform Review1 for

User3 only

User1 and User2 only

User1, User2, and User3

If User2 fails to complete Review1 by March 20, 2019

The Password administrator role will be revoked from User2

User2 will retain the Password administrator role

User3 will receive a confirmation request

- A. Mastered  
 B. Not Mastered

**Answer: A**

### Explanation:

Box 1: User3 only

Use the Members (self) option to have the users review their own role assignments.

Box 2: User3 will receive a confirmation request

Use the Should reviewer not respond list to specify what happens for users that are not reviewed by the reviewer within the review period. This setting does not impact users who have been reviewed by the reviewers manually. If the final reviewer's decision is Deny, then the user's access will be removed.

No change - Leave user's access unchanged Remove access - Remove user's access Approve access - Approve user's access

Take recommendations - Take the system's recommendation on denying or approving the user's continued access

References:

<https://docs.microsoft.com/bs-latn-ba/azure/active-directory/privileged-identity-management/pim-how-to-start-security-review>

### NEW QUESTION 4

#### HOTSPOT

Your company has two offices in Seattle and New York. Each office connects to the Internet by using a NAT device. The offices use the IP addresses shown in the following table.

Location	IP address space	Public NAT segment
Seattle	10.10.0.0/16	190.15.1.0/24
New York	172.16.0.0/16	194.25.2.0/24

The company has an Azure Active Directory (Azure AD) tenant named contoso.com. The tenant contains the users shown in the following table.

Name	Multi-factor authentication (MFA) status
User1	Enabled
User2	Enforced

The MFA service settings are configured as shown in the exhibit. (Click the Exhibit tab.)

trusted ips [\(learn more\)](#)

☒ Skip multi-factor authentication for requests from federated users on my intranet  
Skip multi-factor authentication for requests from following range of IP address subnets

10.10.0.0/16  
194.25.2.0/24

verification options [\(learn more\)](#)

Methods available to users:  
☒ Call to phone  
☒ Text message to phone

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:

Answer Area

	Yes	No
If User1 signs in to Azure from a device that uses an IP address of 134.18.14.10, User1 must be authenticated by using a phone.	<input type="radio"/>	<input type="radio"/>
If User2 signs in to Azure from a device in the Seattle office, User2 must be authenticated by using the Microsoft Authenticator app.	<input type="radio"/>	<input type="radio"/>
If User2 signs in to Azure from a device in the New York office, User1 must be authenticated by using a phone	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 2: No  
Use of Microsoft Authenticator is not required.  
Note: Microsoft Authenticator is a multifactor app for mobile devices that generates time-based codes used during the Two-Step Verification process. Box 3: No  
The New York IP address subnet is included in the "skip multi-factor authentication for request.  
References:  
<https://www.cayosoft.com/difference-enabling-enforcing-mfa/>

NEW QUESTION 5

Your company plans to create separate subscriptions for each department. Each subscription will be associated to the same Azure Active Directory (Azure AD) tenant.  
You need to configure each subscription to have the same role assignments. What should you use?

- A. Azure Security Center
- B. Azure Blueprints
- C. Azure AD Privileged Identity Management (PIM)
- D. Azure Policy

Answer: C

Explanation:

The Azure AD Privileged Identity Management (PIM) service also allows Privileged Role Administrators to make permanent admin role assignments.  
References:  
<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-add-role-to-user>

NEW QUESTION 6

HOTSPOT  
What is the membership of Group1 and Group2? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.  
Hot Area:

Answer Area

Group1:

No members

Only User2

Only User2 and User4

User1, User2, User3, and User4

Group2:

No members

Only User3

Only User1 and User3

User1, User2, User3, and User4

- A. Mastered
- B. Not Mastered

Answer: A

**Explanation:**  
Box 1: User1, User2, User3, User4  
Contains "ON" is true for Montreal (User1), MONTREAL (User2), London (User 3), and Ontario (User4) as string and regex operations are not case sensitive.  
Box 2: Only User3  
Match "\*on" is only true for London (User3).  
Scenario:  
Contoso.com contains the users shown in the following table.

Name	City	Role
User1	Montreal	Global administrator
User2	MONTREAL	Security administrator
User3	London	Privileged role administrator
User4	Ontario	Application administrator
User5	Seattle	Cloud application administrator
User6	Seattle	User administrator
User7	Sydney	Reports reader
User8	Sydney	None

Contoso.com contains the security groups shown in the following table.

Name	Membership type	Dynamic membership rule
Group1	Dynamic user	user.city -contains "ON"
Group2	Dynamic user	user.city -match "*on"

References:  
<https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/groups-dynamic-membership>

NEW QUESTION 7  
HOTSPOT

You are evaluating the security of the network communication between the virtual machines in Sub2. 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:



### Answer Area

Statements	Yes	No
From VM1, you can successfully ping the public IP address of VM2.	<input type="radio"/>	<input type="radio"/>
From VM1, you can successfully ping the private IP address of VM3.	<input type="radio"/>	<input type="radio"/>
From VM1, you can successfully ping the public IP address of VM5.	<input type="radio"/>	<input type="radio"/>

- A. Mastered  
 B. Not Mastered

**Answer:** A

**Explanation:**

Box 1: Yes

NSG1 has the inbound security rules shown in the following table.

Priority	Port	Protocol	Source	Destination	Action
65000	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	Any	Any	AzureLoadBalancer	Any	Allow
65500	Any	Any	Any	Any	Deny

NSG2 has the inbound security rules shown in the following table.

Priority	Port	Protocol	Source	Destination	Action
100	80	TCP	Internet	VirtualNetwork	Allow
65000	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	Any	Any	AzureLoadBalancer	Any	Allow
65500	Any	Any	Any	Any	Deny

Box 2: Yes

Box 3: No Note:

Sub2 contains the virtual machines shown in the following table.

Name	Network interface	Application security group	Connected to
VM1	NIC1	ASG1	Subnet1.1
VM2	NIC2	ASG2	Subnet1.1
VM3	NIC3	None	Subnet1.2
VM4	NIC4	ASG1	Subnet1.3
VM5	NIC5	None	Subnet2.1

Name	Subnet
VNetwork1	Subnet1.1, Subnet1.2 and Subent1.3
VNetwork2	Subnet2.1

Sub2 contains the network security groups (NSGs) shown in the following table.

Name	Associated to
NSG1	NIC2
NSG2	Subnet1.1
NSG3	Subnet1.3
NSG4	Subnet2.1

Question Set 3

**NEW QUESTION 8**

You have Azure Resource Manager templates that you use to deploy Azure virtual machines.

You need to disable unused Windows features automatically as instances of the virtual machines are provisioned. What should you use?

- A. device compliance policies in Microsoft Intune  
 B. Azure Automation State Configuration  
 C. application security groups  
 D. Azure Advisor

**Answer:** B

**Explanation:**

You can use Azure Automation State Configuration to manage Azure VMs (both Classic and Resource Manager), on-premises VMs, Linux machines, AWS VMs,

and on-premises physical machines.  
Note: Azure Automation State Configuration provides a DSC pull server similar to the Windows Feature DSC-Service so that target nodes automatically receive configurations, conform to the desired state, and report back on their compliance. The built-in pull server in Azure Automation eliminates the need to set up and maintain your own pull server. Azure Automation can target virtual or physical Windows or Linux machines, in the cloud or on-premises.  
References:  
<https://docs.microsoft.com/en-us/azure/automation/automation-dsc-getting-started>

**NEW QUESTION 9**

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 a subnet named HubVNetSubnet0.
SpokeVNet	East US	SpokeVNet is a virtual network connected to HubVNet by using VNet peering. SpokeVNet contains a subnet named SpokeVNetSubnet0.

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

Azure FirewallSubnet

GatewaySubnet

HubVNetSubnet0

Answer Area

RT1:

RT2:

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Subnets

Azure FirewallSubnet

GatewaySubnet

HubVNetSubnet0

Answer Area

RT1:

GatewaySubnet

RT2:

HubVNetSubnet0

**NEW QUESTION 10**

HOTSPOT

You have an Azure subscription named Sub1.  
You create a virtual network that contains one subnet. On the subnet, you provision the virtual machines shown in the following table.



Name	Network interface	Application security group assignment	IP address
VM1	NIC1	AppGroup12	10.0.0.10
VM2	NIC2	AppGroup12	10.0.0.11
VM3	NIC3	AppGroup3	10.0.0.100
VM4	NIC4	AppGroup4	10.0.0.200

Currently, you have not provisioned any network security groups (NSGs). You need to implement network security to meet the following requirements:

- \_ Allow traffic to VM4 from VM3 only.
- \_ Allow traffic from the Internet to VM1 and VM2 only. Minimize the number of NSGs and network security rules.

How many NSGs and network security rules should you create? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

## Answer Area

NSGs:

▼

1

2

3

4

Network security rules:

▼

1

2

3

4

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

NSGs: 2  
 Network security rules: 3  
 Not 2: You cannot specify multiple service tags or application groups) in a security rule.  
 References:  
<https://docs.microsoft.com/en-us/azure/virtual-network/security-overview>

**NEW QUESTION 10**

You are testing an Azure Kubernetes Service (AKS) cluster. The cluster is configured as shown in the exhibit. (Click the Exhibit tab.)

<b>BASICS</b>	
Subscription	Microsoft Azure Sponsorship
Resource group	AzureBackupRG_eastus2_1
Region	East US
Kubernetes cluster name	akscluster2
Kubernetes version	1.1 1.5
DNS name prefix	akscluster2
Node count	3
Node size	Standard_DS2_v2
Virtual nodes (preview)	Disabled
<b>AUTHENTICATION</b>	
Enable RBAC	No
<b>NETWORKING</b>	
HTTP application routing	Yes
Network configuration	Basic
<b>MONITORING</b>	
Enable container monitoring	No
<b>TAGS</b>	

You plan to deploy the cluster to production. You disable HTTP application routing.  
 You need to implement application routing that will provide reverse proxy and TLS termination for AKS services by using a single IP address. What should you do?



- A. Create an AKS Ingress controller.
- B. Install the container network interface (CNI) plug-in.
- C. Create an Azure Standard Load Balancer.
- D. Create an Azure Basic Load Balancer.

**Answer:** A

**Explanation:**

An ingress controller is a piece of software that provides reverse proxy, configurable traffic routing, and TLS termination for Kubernetes services.

References:

<https://docs.microsoft.com/en-us/azure/aks/ingress-tls>

**NEW QUESTION 12**

You need to ensure that you can meet the security operations requirements.

What should you do first?

- A. Turn on Auto Provisioning in Security Center.
- B. Integrate Security Center and Microsoft Cloud App Security.
- C. Upgrade the pricing tier of Security Center to Standard.
- D. Modify the Security Center workspace configuration.

**Answer:** C

**Explanation:**

The Standard tier extends the capabilities of the Free tier to workloads running in private and other public clouds, providing unified security management and threat protection across your hybrid cloud workloads. The Standard tier also adds advanced threat detection capabilities, which uses built-in behavioral analytics and machine learning to identify attacks and zero-day exploits, access and application controls to reduce exposure to network attacks and malware, and more.

Scenario: Security Operations Requirements

Litware must be able to customize the operating system security configurations in Azure Security Center. References:

<https://docs.microsoft.com/en-us/azure/security-center/security-center-pricing>

Question Set 3

**NEW QUESTION 17**

You have an Azure subscription named Sub1 that is associated to an Azure Active Directory (Azure AD) tenant named contoso.com.

You are assigned the Global administrator role for the tenant. You are responsible for managing Azure Security Center settings. You need to create a custom sensitivity label.

What should you do first?

- A. Create a custom sensitive information type.
- B. Elevate access for global administrators in Azure AD.
- C. Upgrade the pricing tier of the Security Center to Standard.
- D. Enable integration with Microsoft Cloud App Security.

**Answer:** A

**Explanation:**

First, you need to create a new sensitive information type because you can't directly modify the default rules.

References:

<https://docs.microsoft.com/en-us/office365/securitycompliance/customize-a-built-in-sensitive-information-type>

**NEW QUESTION 22**

You need to configure WebApp1 to meet the data and application requirements.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Upload a public certificate.
- B. Turn on the HTTPS Only protocol setting.
- C. Set the Minimum TLS Version protocol setting to 1.2.
- D. Change the pricing tier of the App Service plan.
- E. Turn on the Incoming client certificates protocol setting.

**Answer:** AC

**Explanation:**

A: To configure Certificates for use in Azure Websites Applications you need to upload a public Certificate.

C: Over time, multiple versions of TLS have been released to mitigate different vulnerabilities. TLS 1.2 is the most current version available for apps running on Azure App Service.

Incorrect Answers:

B: We need support the http url as well.

Note:

**WebApp1 is an Azure web app that is accessible by using <https://litwareinc.com> and <http://www.litwareinc.com>.**

References:

<https://docs.microsoft.com/en-us/azure/app-service/app-service-web-configure-tls-mutual-auth>

<https://azure.microsoft.com/en-us/updates/app-service-and-functions-hosted-apps-can-now-update-tls-versions/>





**NEW QUESTION 26**

DRAG DROP

You need to configure SQLDB1 to meet the data and application requirements.

Which three actions should you recommend be performed in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place:

Actions	Answer Area
From the Azure portal, create an Azure AD administrator for LitwareSQLServer1.	
In SQLDB1, create contained database users.	
Connect to SQLDB1 by using Microsoft SQL Server Management Studio (SSMS).	 
In Azure AD, create a system-assigned managed identity.	 
In Azure AD, create a user-assigned managed identity.	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Step 1: Connect to SQLDB1 by using Microsoft SQL Server Management Studio (SSMS)

Step 2: In SQLDB1, create contained database users.

Create a contained user in the database that represents the VM's system-assigned identity.

Step 3: In Azure AD,create a system-assigned managed identity.

A system-assigned identity for a Windows virtual machine (VM) can be used to access an Azure SQL server. Managed Service Identities are automatically managed by Azure and enable you to authenticate to services that support Azure AD authentication, without needing to insert credentials into your code.

References:

<https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/tutorial-windows-vm-access-sql>

Question Set 2

NEW QUESTION 30

From the Azure portal, you are configuring an Azure policy.

You plan to assign policies that use the DeployIfNotExist, AuditIfNotExist, Append, and Deny effects. Which effect requires a managed identity for the assignment?

- A. AuditIfNotExist
- B. Append
- C. DeployIfNotExist
- D. Deny

Answer: C

Explanation:

When Azure Policy runs the template in the deployIfNotExists policy definition, it does so using a managed identity.

References:

<https://docs.microsoft.com/bs-latn-ba/azure/governance/policy/how-to/remediate-resources>

NEW QUESTION 33

HOTSPOT

You need to create an Azure key vault. The solution must ensure that any object deleted from the key vault be retained for 90 days.

How should you complete the command? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

New-AzureRmKeyVault -VaultName 'KeyVault1' -ResourceGroupName 'RG1'

-Location 'East US'

-EnabledForDeployment

-EnablePurgeProtection

-Tag

-Confirm

-DefaultProfile

-EnableSoftDelete

-SKU

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: -EnablePurgeProtection  
If specified, protection against immediate deletion is enabled for this vault; requires soft delete to be enabled as well.  
Box 2: -EnableSoftDelete  
Specifies that the soft-delete functionality is enabled for this key vault. When soft-delete is enabled, for a grace period, you can recover this key vault and its contents after it is deleted.  
References:  
<https://docs.microsoft.com/en-us/powershell/module/azurerm.keyvault/new-azurermkeyvault>

NEW QUESTION 35

DRAG DROP  
You have an Azure subscription named Sub1 that contains an Azure Storage account named Contosostorage1 and an Azure key vault named Contosokeyvault1. You plan to create an Azure Automation runbook that will rotate the keys of Contosostorage1 and store them in Contosokeyvault1. You need to implement prerequisites to ensure that you can implement the runbook. Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.  
Select and Place:

Actions

Run Set-AzureRmKeyVaultAccessPolicy

Create an Azure Automation account.

Import PowerShell modules to the Azure Automation account.

Create a user-assigned managed identity.

Create a connection resource in the Azure Automation account.

Answer Area

⬅

➡

⬆

⬆

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Step 1: Create an Azure Automation account  
Runbooks live within the Azure Automation account and can execute PowerShell scripts.  
Step 2: Import PowerShell modules to the Azure Automation account  
Under 'Assets' from the Azure Automation account Resources section select 'to add in Modules to the runbook. To execute key vault cmdlets in the runbook, we need to add AzureRM.profile and AzureRM.key vault.  
Step 3: Create a connection resource in the Azure Automation account  
You can use the sample code below, taken from the AzureAutomationTutorialScript example runbook, to authenticate using the Run As account to manage Resource Manager resources with your runbooks. The AzureRunAsConnection is a connection asset automatically created when we created 'run as accounts' above. This can be found under Assets -> Connections. After the authentication code, run the same code above to get all the keys from the vault.  
\$connectionName = "AzureRunAsConnection" try  
{  
# Get the connection "AzureRunAsConnection"  
\$servicePrincipalConnection=Get-AutomationConnection -Name \$connectionName  
"Logging in to Azure..." Add-AzureRmAccount `  
-ServicePrincipal `  
-TenantId \$servicePrincipalConnection.TenantId `  
-ApplicationId \$servicePrincipalConnection.ApplicationId `  
-CertificateThumbprint \$servicePrincipalConnection.CertificateThumbprint  
}

References:

<https://www.rahulpnath.com/blog/accessing-azure-key-vault-from-azure-runbook/>

#### **NEW QUESTION 38**

.....



## Thank You for Trying Our Product

### We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

### az-500 Practice Exam Features:

- \* az-500 Questions and Answers Updated Frequently
- \* az-500 Practice Questions Verified by Expert Senior Certified Staff
- \* az-500 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- \* az-500 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The az-500 Practice Test Here](#)**