AZ-500 Q&As

Microsoft Azure Security Technologies

Pass Microsoft AZ-500 Exam with 100% Guarantee

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

https://www.leads4pass.com/az-500.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

HOTSPOT

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

Name	Type	Resource group	Location
RG1	Resource group	**Not applicable**	West US
Managed1	Managed identity	RG1	West US

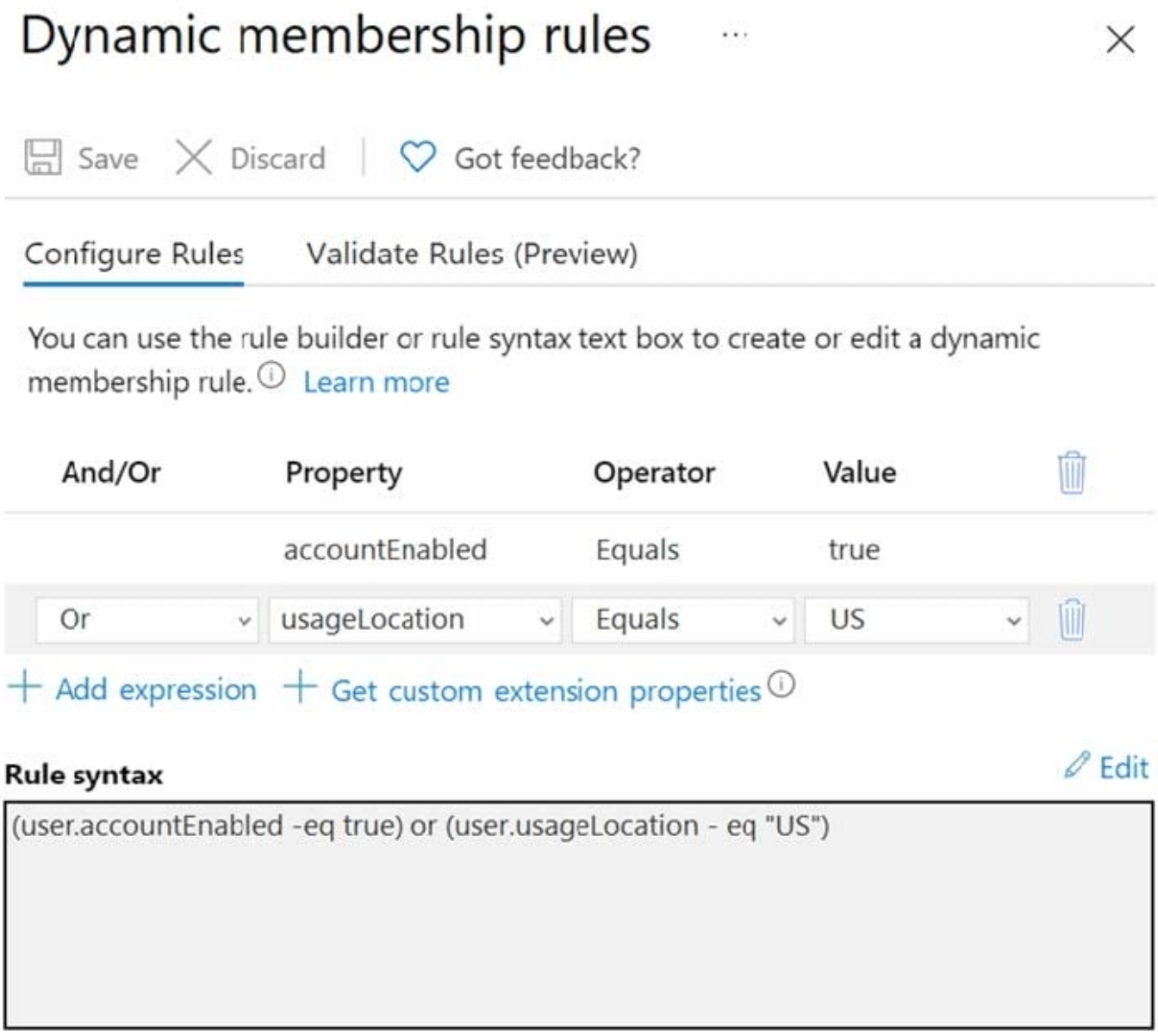
The subscription is linked to an Azure Active Directory (Azure AD) tenant that contains the users shown in the following table.

Name	Usage location
User1	United States
User2	Germany

You create the groups shown in the following table.

Name	Type	Membership type
Group1	Security	Dynamic User
Group2	Microsoft 365	Dynamic User

The membership rules for Group1 and Group2 are configured as shown in the following exhibit.



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:

Statements	Yes	No
User1 is a member of Group1 and Group2.	○	○
User2 is a member of Group2 only.	○	○
Managed1 is a member of Group1 and Group2.	○	○

Correct Answer:

Statements	Yes	No
User1 is a member of Group1 and Group2.	○	○
User2 is a member of Group2 only.	○	○
Managed1 is a member of Group1 and Group2.	○	○

Reference: https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/groups-dynamic-membership

QUESTION 2

You have Azure virtual machines that have Update Management enabled. The virtual machines are configured as shown in the following table.

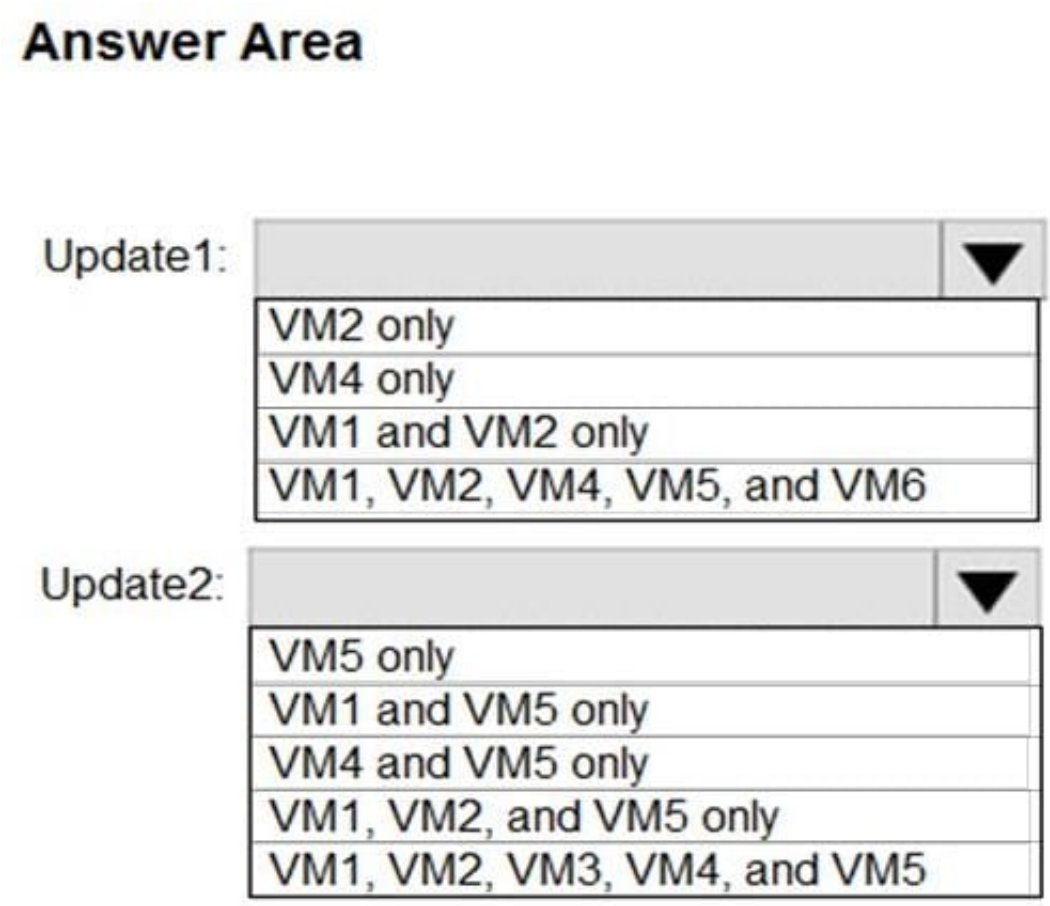
Name	Operating system	Region	Resource group
VM1	Windows Server 2012	East US	RG1
VM2	Windows Server 2012 R2	West US	RG1
VM3	Windows Server 2016	West US	RG2
VM4	Ubuntu Server 18.04 LTS	West US	RG2
VM5	Red Hat Enterprise Linux 7.4	East US	RG1
VM6	CentOS 7.5	East US	RG1

You schedule two update deployments named Update1 and Update2. Update1 updates VM3. Update2 updates VM6.

Which additional virtual machines can be updated by using Update1 and Update2? To answer, select the appropriate options in the answer area.

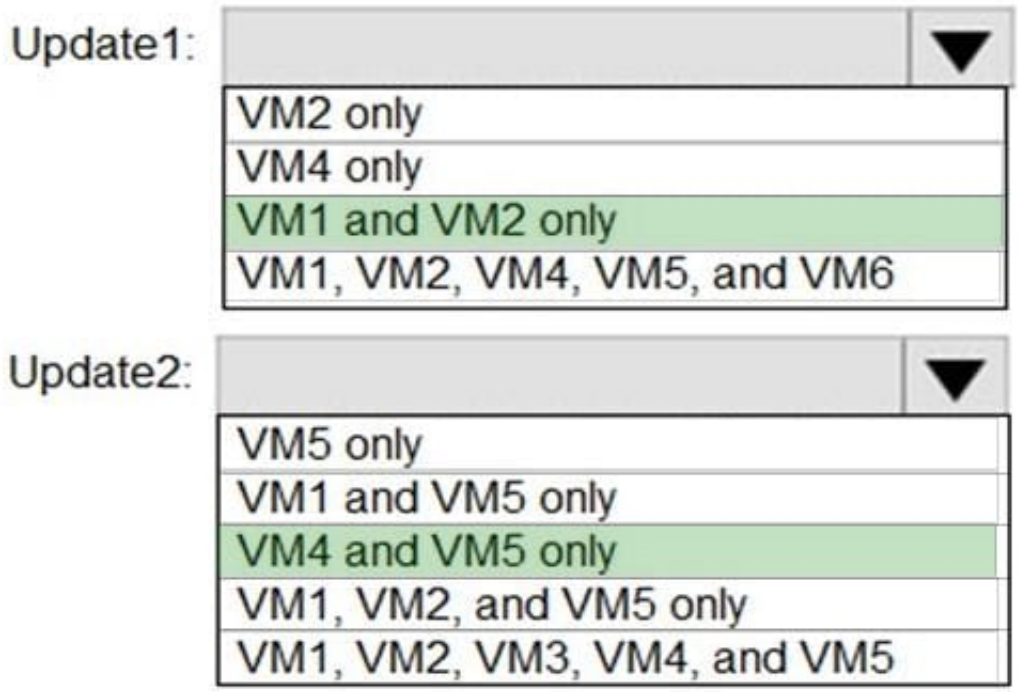
NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:

Answer Area



Update1: VM1 and VM2 only VM3: Windows Server 2016 West US RG2

Update2: VM4 and VM5 only VM6: CentOS 7.5 East US RG1

For Linux, the machine must have access to an update repository. The update repository can be private or public.

References: https://docs.microsoft.com/en-us/azure/automation/automation-update-management

QUESTION 3

You need to create Role1 to meet the platform protection requirements.

How should you complete the role definition of Role1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

```
{
   "Name":  "Role1",
   "Id":  "11111111-1111-1111-1111-111111111111",
   "IsCustom" : true,
   "Description": "VM storage operator"
   "Actions" : [
```

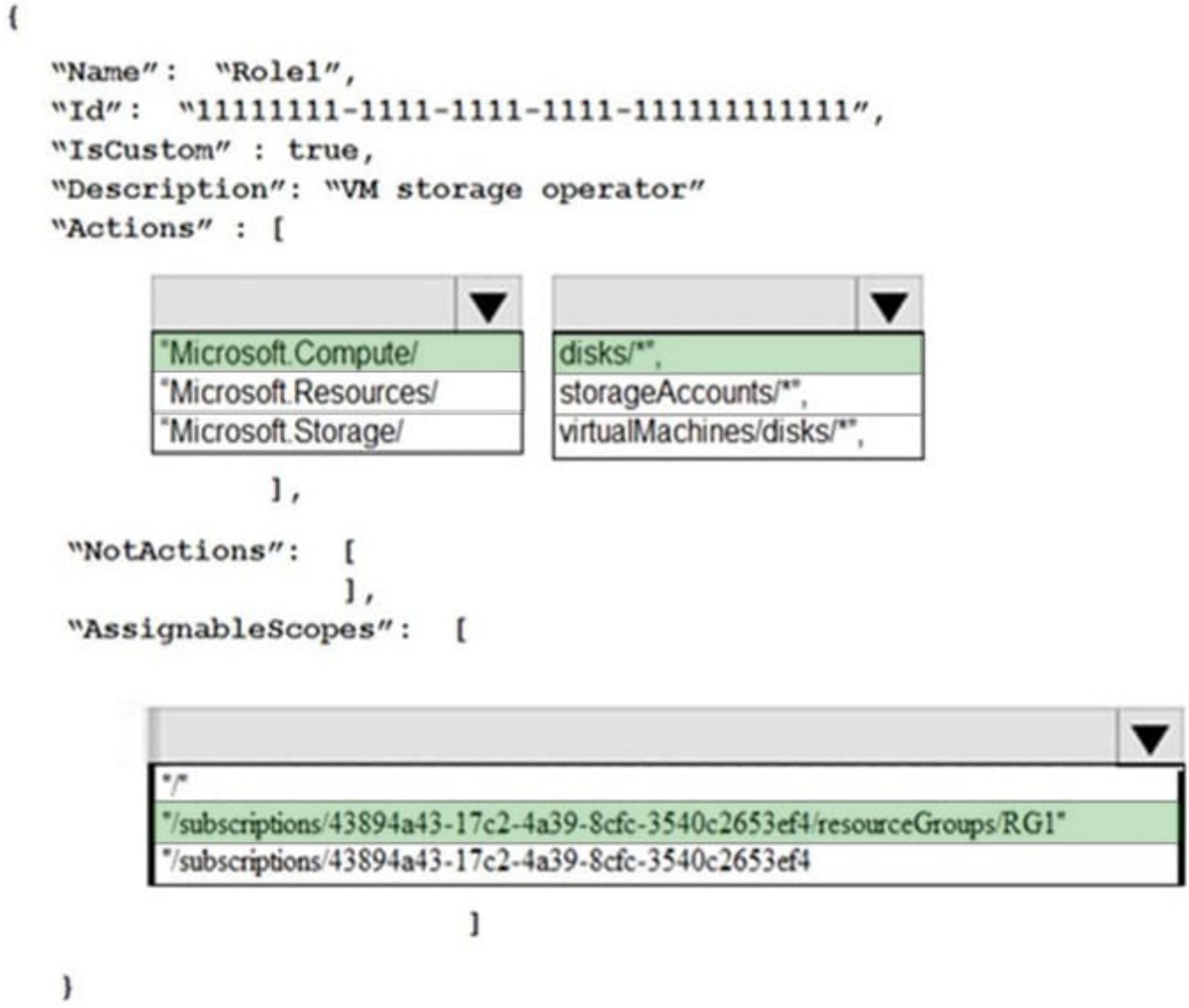
"Microsoft.Compute/	disks/*",
"Microsoft.Resources/	storageAccounts/*",
"Microsoft.Storage/	virtualMachines/disks/*",

```
         ],
   "NotActions":  [
                  ],
   "AssignableScopes":  [
```

"/"
"/subscriptions/43894a43-17c2-4a39-8cfc-3540c2653ef4/resourceGroups/RG1"
"/subscriptions/43894a43-17c2-4a39-8cfc-3540c2653ef4

```
                        ]
}
```

Correct Answer:



1) Microsoft.Compute/

2) disks

3) /subscrption/{subscriptionId}/resourceGroups/{Resource Group Id}

A new custom RBAC role named Role1 must be used to delegate the administration of the managed disks in Resource Group1. Role1 must be available only for Resource Group1.

QUESTION 4

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.

Correct Answer: A

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

---

QUESTION 5

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

Correct Answer: C

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

---

QUESTION 6

SIMULATION

You need to configure a weekly backup of an Azure SQL database named Homepage. The backup must be retained for eight weeks.

To complete this task, sign in to the Azure portal.

A. See the explanation below.

Correct Answer: A

You need to configure the backup policy for the Azure SQL database.

1.

In the Azure portal, type Azure SQL Database in the search box, select Azure SQL Database from the search results then select Homepage. Alternatively, browse to Azure SQL Database in the left navigation pane.

2.

Select the server hosting the Homepage database and click on Manage backups.

3.

Click on Configure policies.

4.

Ensure that the Weekly Backups option is ticked.

5.

Configure the How long would you like weekly backups to be retained option to 8 weeks.

6.

Click Apply to save the changes.

QUESTION 7

You create resources in an Azure subscription as shown in the following table.

Name	Type	Region
RG1	Resource group	West Europe
VNET1	Azure virtual network	West Europe
Contoso1901	Azure Storage account	West Europe

VNET1 contains two subnets named Subnet1 and Subnet2. Subnet1 has a network ID of 10.0.0.0/24. Subnet2 has a network ID of 10.1.1.0/24. Contoso1901 is configured as shown in the exhibit. (Click the Exhibit tab.)

```
PS C:\> (Get-AzStorageAccount -ResourceGroupName RG1 -Name contoso1901).NetworkRuleSet

ByPass              : Logging, Metrics
DefaultAction       : Deny
IpRules             : [193.77.0.0/16,...]
VirtualNetworkRules : [/subscriptions/a90c8c8f-d8bc-4112-abfb-
                      dac4906573dd/resourceGroups/RG1/providers/Microsoft.Network/
                      virtualNetworks/VNET1/subnets/Subnet1,...]

PS C:\> (Get-AzStorageAccount -ResourceGroupName RG1 -Name contoso1901).NetworkRuleSet.
                                                                              IpRules

Action  IPAddressOrRange
------  ----------------
Allow   193.77.0.0/16


PS C:\> (Get-AzStorageAccount -ResourceGroupName RG1 -Name contoso1901).NetworkRules

Action  VirtualNetworkResourceId
------  ------------------------                                              State
 Allow  /subscriptions/a90c8c8f-d8bc-4112-abfb dac4906573dd/resourceGroups/     ------
        RG1/providers/Microsoft.Network/virtualNetworks/VNET1/subnets/Subnet1  Succeeded

PS C:\> _
```

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
An Azure virtual machine on Subnet1 can access data in Contoso1901.	○	○
An Azure virtual machine on Subnet2 can access data in Contoso1901.	○	○
A computer on the Internet that has an IP address of 193.77.10.2 can access data in Contoso1901.	○	○

Correct Answer:

Answer area

Statements	Yes	No
An Azure virtual machine on Subnet1 can access data in Contoso1901.	○	○
An Azure virtual machine on Subnet2 can access data in Contoso1901.	○	○
A computer on the Internet that has an IP address of 193.77.10.2 can access data in Contoso1901.	○	○

Box 1: Yes

Access from Subnet1 is allowed.

Box 2: No

No access from Subnet2 is allowed.

Box 3: Yes

Access from IP address 193.77.10.2 is allowed.

QUESTION 8

You have an Azure Active Directory (Azure AD) tenant named contoso.onmicrosoft.com.

The User administrator role is assigned to a user named Admin1.

An external partner has a Microsoft account that uses the user1@outlook.com sign in.

Admin1 attempts to invite the external partner to sign in to the Azure AD tenant and receives the following error message: "Unable to invite user user1@outlook.com Generic authorization exception."

You need to ensure that Admin1 can invite the external partner to sign in to the Azure AD tenant.

What should you do?

A. From the Roles and administrators blade, assign the Security administrator role to Admin1.

B. From the Organizational relationships blade, add an identity provider.

C. From the Custom domain names blade, add a custom domain.

D. From the Users blade, modify the External collaboration settings.

Correct Answer: D

You need to allow guest invitations in the External collaboration settings.

QUESTION 9

You have been tasked with delegate administrative access to your company\\'s Azure key vault.

You have to make sure that a specific user can set advanced access policies for the key vault. You also have to make sure that access is assigned based on the principle of least privilege.

Which of the following options should you use to achieve your goal?

A. A key vault access policy

B. Azure policy

C. Azure AD Privileged Identity Management (PIM)

D. Azure DevOps

Correct Answer: A

Reference: https://docs.microsoft.com/en-us/azure/key-vault/key-vault-secure-your-key-vault

QUESTION 10

You need to ensure that users can access VM0. The solution must meet the platform protection requirements. What should you do?

A. Move VM0 to Subnet1.

B. On Firewall, configure a network traffic filtering rule.

C. Assign RT1 to AzureFirewallSubnet.

D. On Firewall, configure a DNAT rule.

Correct Answer: A

Azure Firewall has the following known issue:

Conflict with Azure Security Center (ASC) Just-in-Time (JIT) feature.

If a virtual machine is accessed using JIT, and is in a subnet with a user-defined route that points to Azure Firewall as a default gateway, ASC JIT doesn\\'t work. This is a result of asymmetric routing – a packet comes in via the virtual machine

public IP (JIT opened the access), but the return path is via the firewall, which drops the packet because there is no established session on the firewall.

Solution: To work around this issue, place the JIT virtual machines on a separate subnet that doesn\\'t have a user-defined route to the firewall. Scenario:

VM0	Virtual machine	VM0 is an Azure virtual machine that runs Windows Server 2016, connects to Subnet0, and has just in time (JIT) VM access configured.

w

Following the implementation of the planned changes, the IT team must be able to connect to VM0 by using JIT VM access.

Name	Type	Description
Firewall1	Azure Firewall	An Azure firewall on VNet1.
RT1	Route table	A route table that will contain a route pointing to Firewall1 as the default gateway and will be assigned to Subnet0.

References: https://docs.microsoft.com/en-us/azure/firewall/overview

QUESTION 11

SIMULATION

You need to prevent HTTP connections to the rg1lod10598168n1 Azure Storage account.

To complete this task, sign in to the Azure portal.

A. See the explanation below.

Correct Answer: A

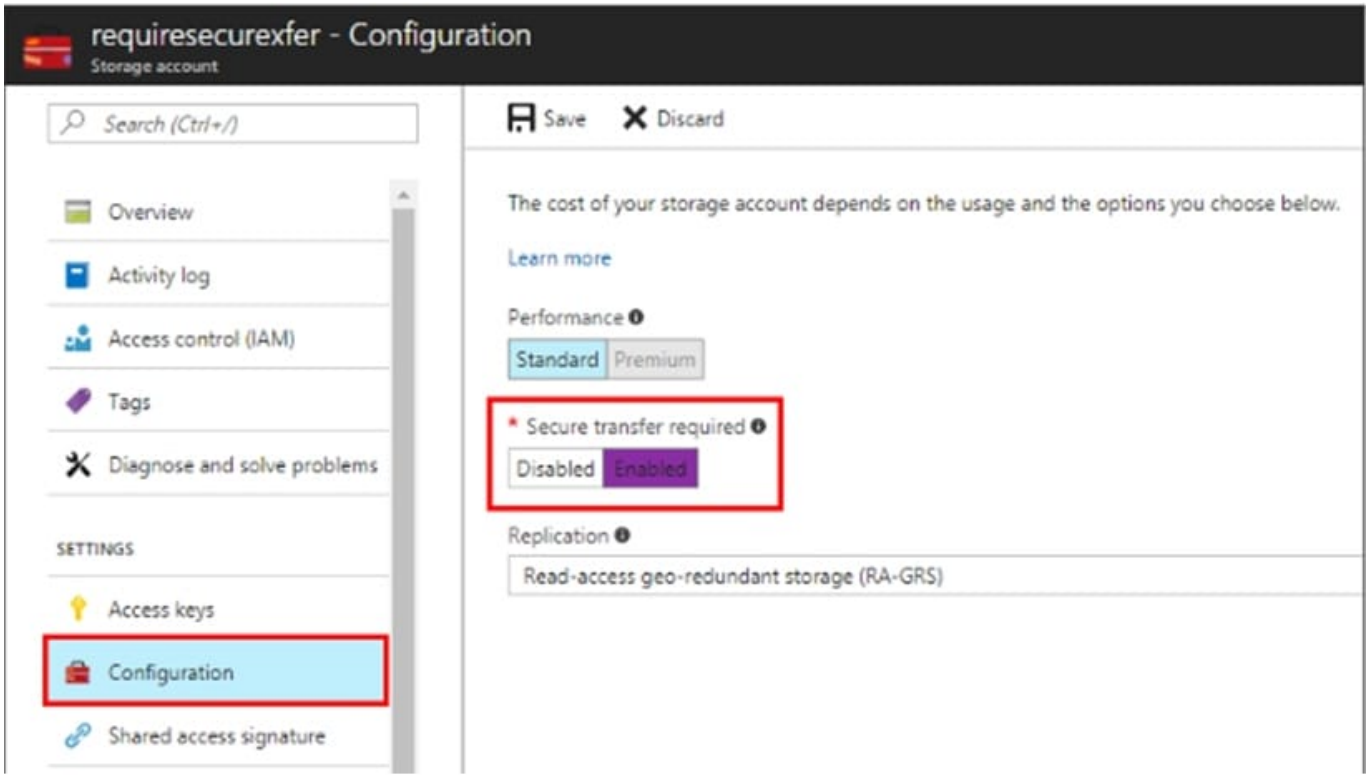
The "Secure transfer required" feature is now supported in Azure Storage account. This feature enhances the security of your storage account by enforcing all requests to your account through a secure connection. This feature is disabled by default.

1.

In Azure Portal select you Azure Storage account rg1lod10598168n1.

2.

Select Configuration, and Secure Transfer required.



Reference: https://techcommunity.microsoft.com/t5/Azure/quot-Secure-transfer-required-quot-is-available-in-Azure-Storage/m-p/82475

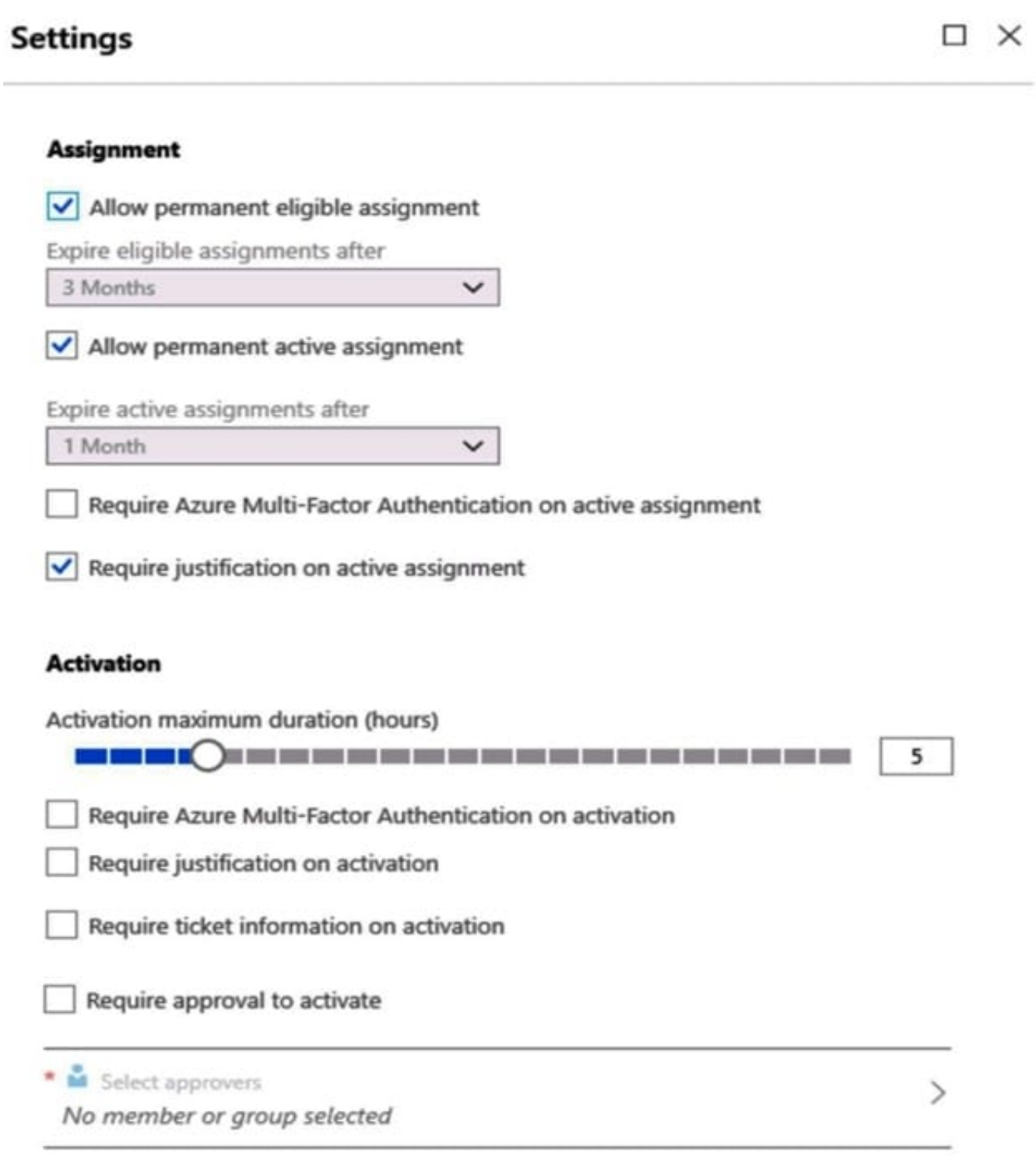
QUESTION 12

HOTSPOT

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

Name	Member of
User1	Group1
User2	Group2
User3	Group1, Group2

From Azure AD Privileged Identity Management (PIM), you configure the settings for the Security Administrator role as shown in the following exhibit.



From PIM, you assign the Security Administrator role to the following groups:

1.

Group1: Active assignment type, permanently assigned

2.

Group2: Eligible assignment type, permanently eligible

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:

Statements	Yes	No
User1 can only activate the Security Administrator role in five hours.	○	○
If User2 activates the Security Administrator role, the user will be assigned the role immediately.	○	○
User3 can activate the Security Administrator role.	○	○

Correct Answer:

Statements	Yes	No
User1 can only activate the Security Administrator role in five hours.	○	○
If User2 activates the Security Administrator role, the user will be assigned the role immediately.	○	○
User3 can activate the Security Administrator role.	○	○

Box 1: Yes

Eligible Type: A role assignment that requires a user to perform one or more actions to use the role. If a user has been made eligible for a role, that means they can activate the role when they need to perform privileged tasks. There\\'s no

difference in the access given to someone with a permanent versus an eligible role assignment. The only difference is that some people don\\'t need that access all the time.

You can choose from two assignment duration options for each assignment type (eligible and active) when you configure settings for a role. These options become the default maximum duration when a user is assigned to the role in

Privileged Identity Management.

Use the Activation maximum duration slider to set the maximum time, in hours, that a role stays active before it expires. This value can be from one to 24 hours.

Box 2: Yes

Active Type: A role assignment that doesn\\'t require a user to perform any action to use the role. Users assigned as active have the privileges assigned to the role

Box 3: Yes

User3 is member of Group2.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure

https://docs.microsoft.com/bs-cyrl-ba/azure/active-directory/privileged-identity-management/pim-resource-roles-configure-role-settings

QUESTION 13

You have an Azure subscription that contains an Azure Blob storage account bolb1.

You need to configure attribute-based access control (ABAC) for blob1.

Which attributes can you use in access conditions?

A. blob index tags only

B. blob index tags and container names only

C. file extensions and container names only

D. blob index tags, file extensions, and container names

Correct Answer: B

https://learn.microsoft.com/en-us/azure/role-based-access-control/conditions-overview

QUESTION 14

You have the Azure Information Protection conditions shown in the following table.

Name	Pattern	Case sensitivity
Condition1	White	On
Condition2	Black	Off

You have the Azure Information Protection labels shown in the following table.

Name	Applies to	Use label	Set the default label
Global	*Not applicable*	*None*	None
Policy1	User1	Label1	None
Policy2	User1	Label2	None

You need to identify how Azure Information Protection will label files.

What should you identify? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

If User1 creates a Microsoft Word file that includes the text "Black and White", the file will be assigned:

- No label
- Label1 only
- Label2 only
- Label1 and Label2

If User1 creates a Microsoft Notepad file that includes the text "Black or white", the file will be assigned:

- No label
- Label1 only
- Label2 only
- Label1 and Label2

Correct Answer:

Answer Area

If User1 creates a Microsoft Word file that includes the text "Black and White", the file will be assigned:

- No label
- Label1 only
- **Label2 only**
- Label1 and Label2

If User1 creates a Microsoft Notepad file that includes the text "Black or white", the file will be assigned:

- **No label**
- Label1 only
- Label2 only
- Label1 and Label2

Box 1: Label 2 only How multiple conditions are evaluated when they apply to more than one label

1.

The labels are ordered for evaluation, according to their position that you specify in the policy: The label positioned first has the lowest position (least sensitive) and the label positioned last has the highest position (most sensitive).

2.

The most sensitive label is applied.

3.

The last sublabel is applied.

Box 2: No Label

Automatic classification applies to Word, Excel, and PowerPoint when documents are saved, and apply to Outlook when emails are sent. Automatic classification does not apply to Microsoft Notepad.

References:

https://docs.microsoft.com/en-us/azure/information-protection/configure-policy-classification

---

QUESTION 15

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 an Azure Subscription named Sub1.

You have an Azure Storage account named Sa1 in a resource group named RG1.

Users and applications access the blob service and the file service in Sa1 by using several shared access signatures (SASs) and stored access policies.

You discover that unauthorized users accessed both the file service and the blob service.

You need to revoke all access to Sa1.

Solution: You regenerate the access keys.

Does this meet the goal?

A. Yes

B. No

Correct Answer: A

To revoke a stored access policy, you can either delete it, or rename it by changing the signed identifier. Changing the

signed identifier breaks the associations between any existing signatures and the stored access policy. Deleting or renaming the stored access policy immediately effects all of the shared access signatures associated with it.

References:

https://docs.microsoft.com/en-us/rest/api/storageservices/Establishing-a-Stored-Access- Policy