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.geekcert.com/az-500.html

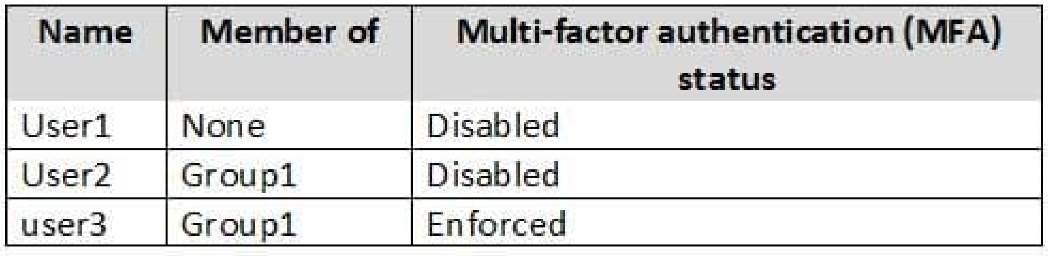
100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

HOTSPOT

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



Name	Member of	Multi-factor authentication (MFA) status
User1	None	Disabled
User2	Group1	Disabled
user3	Group1	Enforced

Azure AD Privileged Identity Management (PIM) is enabled for the tenant.

In PIM, the Password Administrator role has the following settings:

1.

Maximum activation duration (hours): 2

2.

Send email notifying admins of activation: Disable

3.

Require incident/request ticket number during activation: Disable

4.

Require Azure Multi-Factor Authentication for activation: Enable

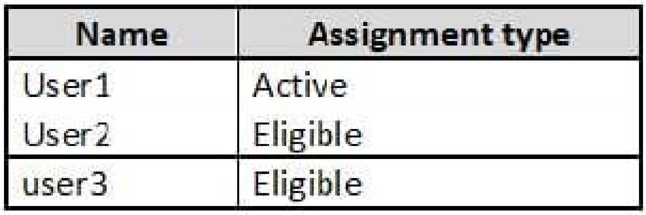
5.

Require approval to activate this role: Enable

6.

Selected approver: Group1

You assign users the Password Administrator role as shown in the following table.

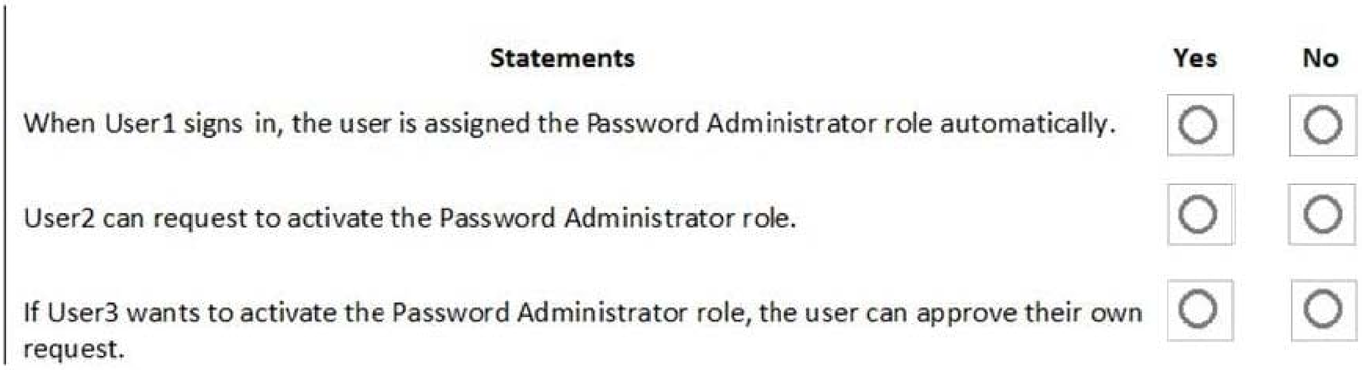


Name	Assignment type
User1	Active
User2	Eligible
user3	Eligible

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

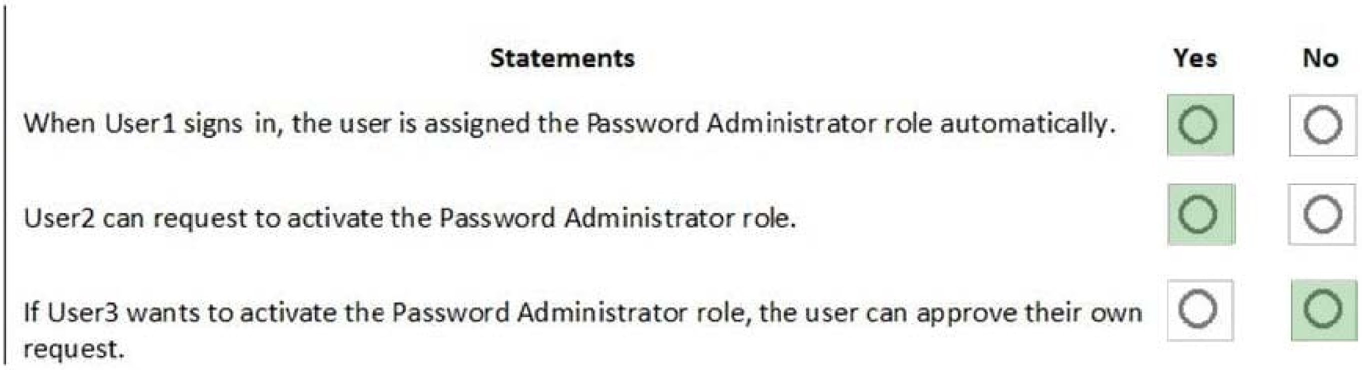
NOTE: Each correct selection is worth one point.

Hot Area:



Statements	Yes	No
When User1 signs in, the user is assigned the Password Administrator role automatically.	○	○
User2 can request to activate the Password Administrator role.	○	○
If User3 wants to activate the Password Administrator role, the user can approve their own request.	○	○

Correct Answer:



Statements	Yes	No
When User1 signs in, the user is assigned the Password Administrator role automatically.	●	○
User2 can request to activate the Password Administrator role.	●	○
If User3 wants to activate the Password Administrator role, the user can approve their own request.	○	●

Box 1: Yes

Active assignments don\\'t require the member to perform any action to use the role. Members assigned as active have the privileges assigned to the role at all times.

Box 2: Yes

While Multi-Factor Authentication is disabled for User2 and the setting Require Azure Multi-Factor Authentication for activation is enabled, User2 can request the role but will need to enable MFA to use the role.

Note: Eligible assignments require the member of the role to perform an action to use the role. Actions might include performing a multi-factor authentication

(MFA) check, providing a business justification, or requesting approval from designated approvers.

Box 3: No

User3 is Group1, which is a Selected Approver Group, however, self-approval is not allowed and someone else from group is required to approve the request.

Reference:

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

QUESTION 2

HOTSPOT

You have 20 Azure subscriptions and a security group named Group1. The subscriptions are children of the root management group.

Each subscription contains a resource group named RG1.

You need to ensure that for each subscription RG1 meets the following requirements:

1.

The members of Group1 are assigned the Owner role.

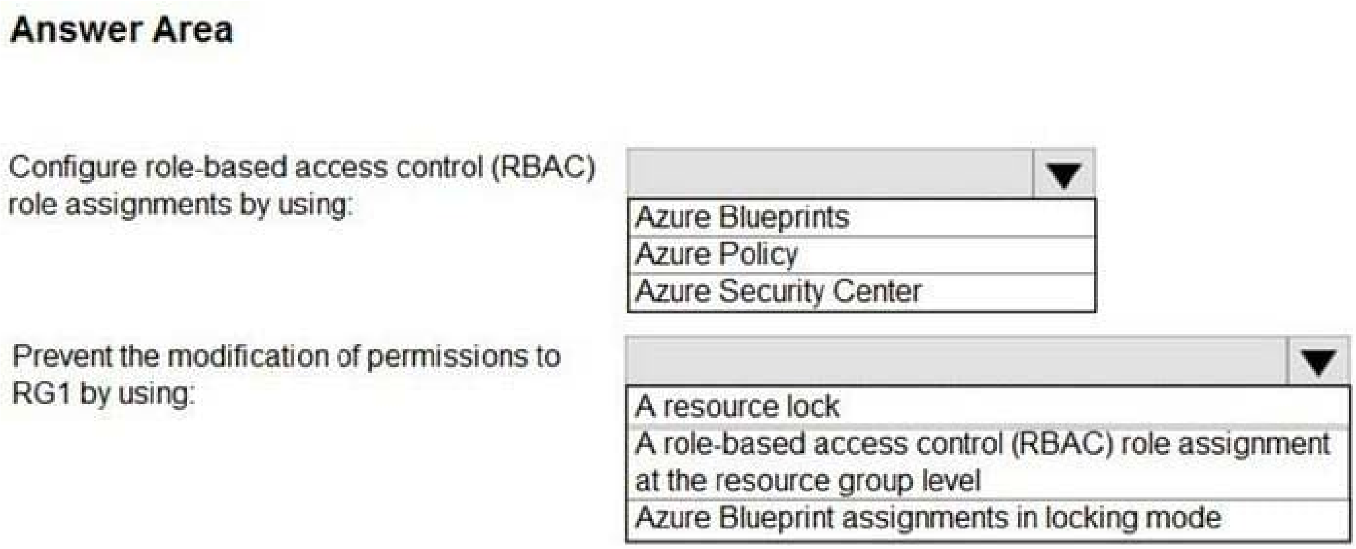
2.

The modification of permissions to RG1 is prevented.

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

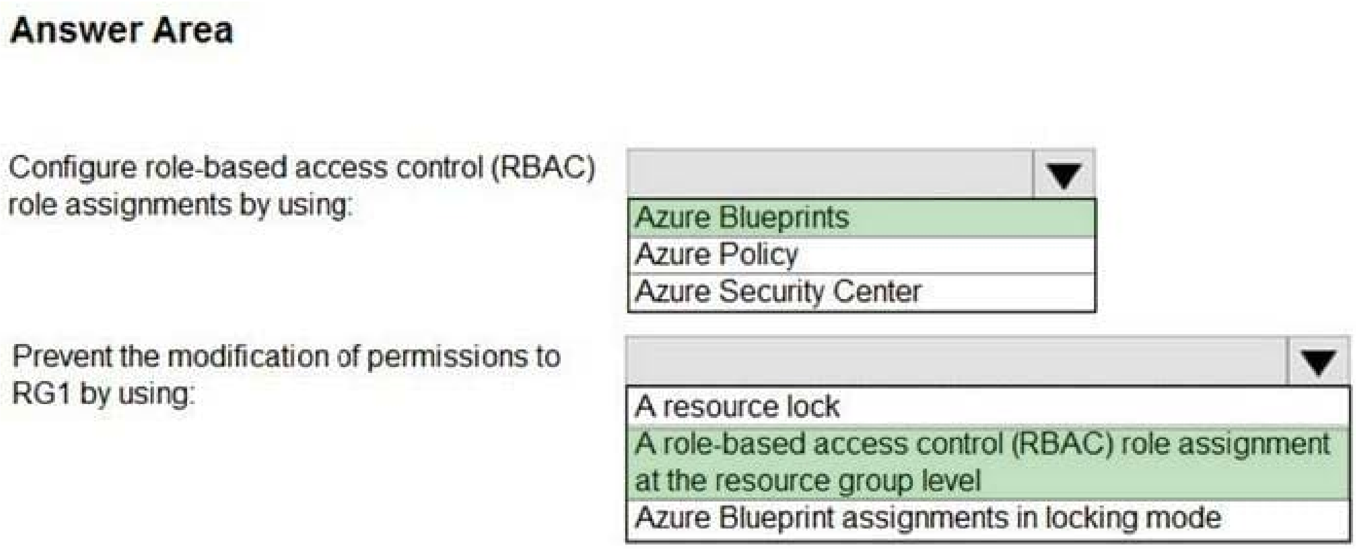
Configure role-based access control (RBAC) role assignments by using:

- Azure Blueprints
- Azure Policy
- Azure Security Center

Prevent the modification of permissions to RG1 by using:

- A resource lock
- A role-based access control (RBAC) role assignment at the resource group level
- Azure Blueprint assignments in locking mode

Correct Answer:



Answer Area

Configure role-based access control (RBAC) role assignments by using:

[✓ Azure Blueprints]
Azure Policy
Azure Security Center

Prevent the modification of permissions to RG1 by using:

A resource lock
[✓ A role-based access control (RBAC) role assignment at the resource group level]
Azure Blueprint assignments in locking mode

QUESTION 3

Your network contains an on-premises Active Directory domain named adatum.com that syncs to Azure Active Directory (Azure AD). Azure AD Connect is installed on a domain member server named Server1.

You need to ensure that a domain administrator for the adatum.com domain can modify the synchronization options. The solution must use the principle of least privilege.

Which Azure AD role should you assign to the domain administrator?

A. Security administrator

B. Global administrator

C. User administrator

Correct Answer: B

Reference: https://docs.microsoft.com/en-us/azure/active-directory/hybrid/reference-connect-accounts-permissions

QUESTION 4

You have an Azure subscription named Sub1.

In Azure Security Center, you have a workflow automation named WF1. WF1 is configured to send an email message to a user named User1.

You need to modify WF1 to send email messages to a distribution group named Alerts.

What should you use to modify WF1?

A. Azure Application Insights

B. Azure Monitor

C. Azure Logic Apps Designer

D. Azure DevOps

Correct Answer: C

Configure email notifications for security alerts.

By default, Microsoft Defender for Cloud emails subscription owners whenever a high-severity alert is triggered for their subscription. This page explains how to customize these notifications.\\'

Workflow automation feature of Microsoft Defender for Cloud.

This feature can trigger consumption logic apps on security alerts, recommendations, and changes to regulatory compliance. For example, you might want Defender for Cloud to email a specific user when an alert occurs.

Reference:

https://learn.microsoft.com/en-us/azure/defender-for-cloud/workflow-automation

QUESTION 5

You have an Azure subscription.

You plan to create a custom role-based access control (RBAC) role that will provide permission to read the Azure Storage account.

Which property of the RBAC role definition should you configure?

A. NotActions []

B. DataActions []

C. AssignableScopes []

D. Actions []

Correct Answer: D

To `Read a storage account\\', ie. list the blobs in the storage account, you need an `Action\\' permission. To read the data in a storage account, ie. open a blob, you need a `DataAction\\' permission.

Reference: https://docs.microsoft.com/en-us/azure/role-based-access-control/role-definitions