



Free Questions for AZ-500

Shared by Vega on 29-01-2024

For More Free Questions and Preparation Resources

[Check the Links on Last Page](#)



## Question 1

---

Question Type: MultipleChoice

---

Case Study: Mix Questions

---

### Mix Questions

#### AZ-500 Mix Questions IN THIS CASE STUDY

You have an Azure subscription.

You plan to deploy a new Conditional Access policy named CAPolicy1.

You need to use the What If tool to evaluate how CAPolicy1 will affect user1. The solution must minimize the impact of CAPolicy1 on the users.

To what should you set the Enable policy setting for CAPolicy1?

Options:

---

A- Off

B- On

C- Report only

Answer:

---

C

## Question 2

---

Question Type: MultipleChoice

---

Case Study: Mix Questions

---

### Mix Questions

#### AZ-500 Mix Questions IN THIS CASE STUDY

You have a Microsoft Entra tenant that contains a user named User1.

You plan to enable passwordless authentication for the tenant.

You need to ensure that User1 can enable the combined registration experience. The solution must use the principle of least privilege.

Which role should you assign to User1?

### Options:

- A- Security Administrator
- B- Global Administrator
- C- Privileged Role Administrator
- D- Authentication Administrator

### Answer:

D

## Question 3

Question Type: Hotspot

Case Study: Mix Questions

## Mix Questions

### AZ-500 Mix Questions IN THIS CASE STUDY

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

Name	Role
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.

## Answer Area

Users who can onboard Azure AD Identity Protection:

  

- User1 only
- User1 and User2 only
- User1, User 2, and User3 only
- User1, User 2, User3, and User 4 only

Users who can remediate users and configure policies:

  

- User1 and User2 only
- User1 and User3 only
- User1, User 2, and User3 only
- User1, User 2, User3, and User 4

Answer:

See the Answer in the Premium Version!



## Question 4

Question Type: MultipleChoice

Case Study: Mix Questions

### Mix Questions

#### AZ-500 Mix Questions IN THIS CASE STUDY

You have an Azure AD turned that contains a user named User1.

You purchase an App named App1.

User1 needs to publish App1 by using Azure AD Application Proxy.

Which role should you assign to User1?



Options:

- A- Hybrid identity Administrator
- B- Cloud App Security Administrator
- C- Application Administrator
- D- Cloud Application Administrate

Answer:

C

## Question 5

Question Type: Hotspot

Case Study: Mix Questions

### Mix Questions

#### AZ-500 Mix Questions IN THIS CASE STUDY

You have a Microsoft Entra tenant that contains the users shown in the following table.

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

You create and enforce a Microsoft Entra Identity Protection sign-in risk policy that has the following settings:

- \* Assignments: Include Group1, exclude Group2
- \* Conditions: Sign-in risk level: Low and above
- \* Access: Allow access, Require multi-factor authentication

You need to identify what occurs when the users sign in to Microsoft Entra ID.

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

NOTE: Each correct selection is worth one point.

#### Answer Area

When User1 signs in from an anonymous IP address, the user will:

- Be prompted for MFA
- Be blocked
- Be prompted for MFA
- Sign in by using a username and password only

When User2 signs in from an unfamiliar location, the user will:

- Be blocked
- Be blocked
- Be prompted for MFA
- Sign in by using a username and password only

#### Answer:

See the Answer in the Premium Version!

## Question 6

---

Question Type: MultipleChoice

---

Case Study: Mix Questions

---

### Mix Questions

#### AZ-500 Mix Questions IN THIS CASE STUDY

Lab Task

Task 2

You need to ensure that the events in the NetworkSecurityGroupRuleCounter log of the VNET01-Subnet0-NSG network security group (NSG) are stored in the logs31330471 Azure Storage account for 30 days.

Options:

---

A- see the task answer with step by step below

Answer:

---

A

Explanation:

---

Enable diagnostic resource logging for the NSG. You can use the Azure portal, Azure PowerShell, or the Azure CLI to do this. You need to select theRule countercategory under Logs and choose thelogs31330471storage account as the destination.

Configure the retention policy for the storage account to keep the logs for 30 days. You can use the Azure portal, Azure PowerShell, or the Azure CLI to do this. You need to specify thedaysparameter as 30 for the Set-AzStorageServiceProperty cmdlet or the az storage logging update command.

View and analyze the logs in the storage account. You can use any tool that can read JSON files, such as Azure Storage Explorer or Visual Studio Code.You can also export the logs to any visualization tool, SIEM solution, or IDS of your choice

To Get Premium Files for AZ-500 Visit

<https://www.p2pexams.com/products/az-500>

For More Free Questions Visit

<https://www.p2pexams.com/microsoft/pdf/az-500>

**20%**  
**DISCOUNT**

**P2P**  
exams