



Free Questions for MS-102 by go4braindumps

Shared by Vance on 22-07-2024

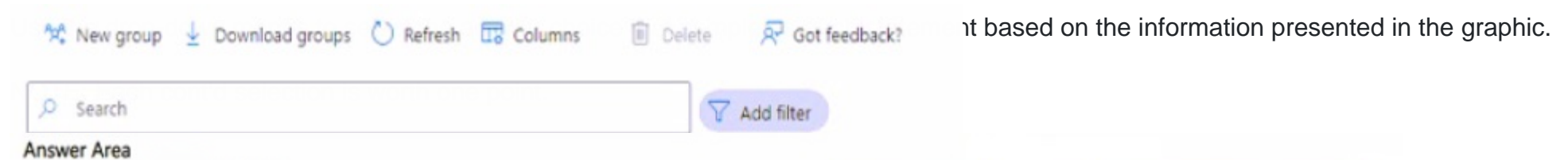
For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: Hotspot

You have a Microsoft Entra tenant that contains the groups shown in the following exhibit.



Answer Area

You can add a Microsoft Entra cloud user to [answer choice].

- Group1 only
- Group1 and Group3 only
- Group1, Group2, and Group3 only
- Group1, Group3, and Group4 only
- Group1, Group2, Group3, Group4, and Group5

Answer:

Question 2

Question Type: Hotspot

You have a Microsoft 365 subscription that uses a domain name of adatum.com.

In Microsoft Entra ID, you set Guest invite restrictions to Only users assigned to specific admin roles can invite guest users.

You can add Group5 to [answer choice].

- Group1 only
- Group3 only
- Group1 and Group3 only
- Group1, Group3, and Group4 only
- Group1, Group2, Group3, and Group4

A user named used@adatum.com reports that they can no longer invite external users from a domain named contoso.com to collaborate in Microsoft Teams.

You need to modify the Microsoft Entra ID configuration to meet the following requirements:

- * Ensure that User1 can invite the contoso.com users to Teams
- * Ensure that only the contoso.com users can be invited as guests to the Microsoft Entra tenant.
- * Follow the principle of least privilege

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

Answer Area

Ensure that User1 can invite the contoso.com users to Teams:

Assign the Guest Inviter role to User1.

Assign the User Administrator role to User1.

Assign the Teams Administrator role to User1.

Add User1 as a group owner to each team in Teams.

Answer:

Ensure that only the contoso.com users can be invited as guests to the Microsoft Entra tenant:

From the Cross-tenant access settings, edit the Outbound access settings.

From the External collaboration settings, edit the Collaboration restrictions settings.

From the External collaboration settings, edit the Guest user access restrictions settings.

Question 3

Question Type: Hotspot

Your company has a Microsoft Entra tenant that contains the users shown in the following table.

Name	Role
User1	Privileged Role Administrator
User2	User Administrator
User3	Security Administrator
User4	Billing Administrator

ed Admin1. Admin1 will be used to manage administrative accounts. External collaboration

orm the following administrative tasks:

Answer Area

Answer:

Create guest user accounts:

User4 only

User2 only

User3 only

User2 and User3 only

User1, User2, and User3 only

Question 4

Question Type: Hotspot

Add User3 to Admin1:

User2 only

User3 only

User4 only

User2 and User3 only

User1, User2, and User3 only

User1, User2, User3, and User4

You have a Microsoft 365 subscription that contains the users shown in the following table.

Name	Department	Job title
User1	IT engineering	Technician
User2	Engineering	Senior executive
User3	Engineering	Senior executive
User4	Engineering	Senior executive

Name	Role
Admin1	AU1\User Administrator
Admin2	Global Administrator

ned AU1 and configure the following AU1 dynamic membership rule.

ments shown in the following table.

Answer Area

Statements	Yes	No
Admin1 can reset the password of User1.	<input type="radio"/>	<input type="radio"/>
Admin1 can reset the password of User2.	<input type="radio"/>	<input type="radio"/>
Admin2 can reset the password of User3.	<input type="radio"/>	<input type="radio"/>

Answer:

Question 5

Question Type: Hotspot

You have a Microsoft 365 subscription.

From Microsoft Entra Privileged Identity Management (PIM), you configure Role settings for the Global Administrator role as shown in the following exhibit.



Global Administrator | Role settings

Privileged Identity Management | Microsoft Entra roles

Answer Area

To use the Global Administrator role, admin1@contoso.com must provide [answer choice].

- Azure Multi-Factor Authentication (MFA) and requires admin approval justification and Azure Multi-Factor Authentication (MFA) ticket information and justification
- Azure Multi-Factor Authentication (MFA) and requires admin approval justification and ticket information
- Azure Multi-Factor Authentication (MFA) and requires admin approval justification and requires admin approval

Answer:

Question 6

To make a new user eligible for the Global Administrator role, a PIM administrator must configure [answer choice].

- Azure Multi-Factor Authentication (MFA) and requires admin approval justification and ticket information
- Azure Multi-Factor Authentication (MFA) and requires admin approval justification and requires admin approval
- Azure Multi-Factor Authentication (MFA) and requires admin approval justification and requires admin approval and ticket information
- Azure Multi-Factor Authentication (MFA) and requires admin approval justification and requires admin approval and requires admin approval

Question Type: Hotspot

You have a Microsoft 365 E5 subscription.

Expire eligible assignments after 15 day(s)

You create a Conditional Access policy named Policy1 and assign Policy1 to all users.

Allow permanent active assignment Yes

You need to configure Policy1 to enforce multi factor authentication (MFA) if the user risk level is high.

Expire active assignments after

Which two settings should you configure in Policy1? To answer, select the appropriate settings in the answer area.

Require Azure Multi-Factor Authentication Yes

Require justification on active assignment No

NOTE: Each correct selection is worth one point.

New

Conditional Access policy

Answer:

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies.
[Learn more](#)

Question 7

Question Type: Hotspot

You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

Name	Member of	Multi-Factor Auth Status
User1	Group1	Disabled
User2	Group1, Group2	Enabled
User3	Group2	Disabled

- * Include: Group1
- * Exclude: Group2
- * Controls: Require Microsoft Entra ID multifactor authentication registration
- * Policy enforcement: Enabled

You create a conditional access policy that has the following settings:

- * Name: Policy1

Name *

Policy1 ✓

Assignment

Users ⓘ

All users

Target resources ⓘ

All cloud apps

Conditions ⓘ

0 conditions selected

Access controls

Grant ⓘ

0 controls selected

Session ⓘ

0 controls selected ✓

* Assignments:

* Include: Group1

* Exclude; Group1

* Grant: Require multifactor authentication

* Enable policy. On

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

NOTE: Each coned selection is one point.

Answer Area

	Statements	Yes	No
Answer:	User1 will be required to register for MFA on the next sign-in.	<input type="radio"/>	<input type="radio"/>
	User2 will be required to register for MFA on the next sign-in.	<input type="radio"/>	<input type="radio"/>
	User3 will be required to register for MFA on the next sign-in.	<input type="radio"/>	<input type="radio"/>

Question 8

Question Type: Hotspot

You have a Microsoft 365 E5 subscription.

You need to configure Privileged Identity Management (PIM) for the User Administrator role in Microsoft Entr

a. Eligible users must meet the following requirements:

- * Always be able to request the User Administrator role.
- * Must provide a reason when requesting the User Administrator role
- * Must require multi-factor authentication (MFA) when activating the User Administrator role

The solution must minimize administrative effort.

Answer Area

Always be able to request the User Administrator role:

A screenshot of a dropdown menu with a yellow highlight on the first option. The options are:

- Select Require approval to activate.
- Set Allow permanent active assignment to Yes.
- Set Allow permanent eligible assignment to Yes.

Answer:

Must provide a reason when requesting the User Administrator role:

A screenshot of a dropdown menu with three options:

- Select Require justification on activation.
- Select Require ticket information on activation.
- Set Require justification on active assignment to Yes.

Question 9

Question Type: Hotspot

Must require MFA when activating the User Administrator role:

A screenshot of a dropdown menu with three options:

- Set On activation require to Azure MFA.
- Set On activation require to Microsoft Entra Conditional Access authentication context.
- Set Require Azure Multi-Factor Authentication on active assignment to Yes.

You have a Microsoft 365 E5 subscription.

You need to configure threat protection for Microsoft 365 to meet the following requirements:





- * Limit a user named User 1 from sending more than 30 email messages per day.
- * Prevent the delivery of a specific file based on the file hash.

Which two threat policies should you configure in Microsoft Defender for Office 365? To answer, select the appropriate threat policies in the answer area.




NOTE: Each correct selection is worth one point.

Answer Area

Policies

	Anti-phishing	Protect users from phishing attacks, and configure safety tips on suspicious messages.
	Anti-spam	Protect your organization's email from spam, including what actions to take if spam is detected
	Anti-malware	Protect your organization's email from malware, including what actions to take and who to notify if malware is detected
	Safe Attachments	Protect your organization from malicious content in email attachments and files in SharePoint, OneDrive, and Teams
	Safe Links	Protect your users from opening and sharing malicious links in email messages and Office apps

Rules

	Tenant Allow/Block Lists	Manage allow or block entries for your organization.
	Email authentication settings	Settings for Authenticated Received Chain (ARC) and DKIM in your organization.
	DKIM	Add DomainKeys Identified Mail (DKIM) signatures to your domains so recipients know that email messages actually came from your users
	Advanced delivery	Manage overrides for special system use cases.
	Enhanced filtering	Configure Exchange Online Protection (EOP) scanning to work correctly when your domain's MX record doesn't route email to EOP first
	Quarantine policies	Apply custom rules to quarantined messages by using default quarantine policies or creating your own

Answer:

To Get Premium Files for MS-102 Visit

<https://www.p2pexams.com/products/ms-102>

For More Free Questions Visit

<https://www.p2pexams.com/microsoft/pdf/ms-102>

