

HOTSPOT -

You have an Azure Active Directory (Azure AD) tenant.

You need to create a conditional access policy that requires all users to use multi-factor authentication when they access the Azure portal.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

\* Name

Policy1

✓

Assignments

Users and groups ⓘ

>

0 users and groups selected

Cloud apps ⓘ

>

0 cloud apps selected

Conditions ⓘ

>

0 conditions selected

Access controls

Grant ⓘ

>

0 controls selected

Session ⓘ

>

Answer Area

\* Name

Policy1

✓

Assignments

Users and groups ⓘ

>

0 users and groups selected

Cloud apps ⓘ

>

0 cloud apps selected

Conditions ⓘ

>

0 conditions selected

Access controls

Grant ⓘ

>

0 controls selected

Session ⓘ

>

Correct Answer:

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 Users blade, modify the External collaboration settings.
- B. From the Custom domain names blade, add a custom domain.
- C. From the Organizational relationships blade, add an identity provider.
- D. From the Roles and administrators blade, assign the Security administrator role to Admin1.

Reveal Solution

Discussion 26

**Correct Answer:** A

Reference:

<https://techcommunity.microsoft.com/t5/Azure-Active-Directory/Generic-authorization-exception-inviting-Azure-AD-gests/td-p/274742>

You have an Azure subscription linked to an Azure Active Directory tenant. The tenant includes a user account named User1.

You need to ensure that User1 can assign a policy to the tenant root management group.

What should you do?

- A. Assign the Owner role for the Azure Subscription to User1, and then modify the default conditional access policies.
- B. Assign the Owner role for the Azure subscription to User1, and then instruct User1 to configure access management for Azure resources.
- C. Assign the Global administrator role to User1, and then instruct User1 to configure access management for Azure resources.
- D. Create a new management group and delegate User1 as the owner of the new management group.

**Correct Answer:** B

The following chart shows the list of roles and the supported actions on management groups.

Azure Role Name	Create	Rename	Move**	Delete	Assign Access	Assign Policy	Read
Owner	X	X	X	X	X	X	X
Contributor	X	X	X	X			X
MG Contributor*	X	X	X	X			X
Reader							X
MG Reader*							X
Resource Policy Contributor						X	
User Access Administrator					X	X	

Note:

Each directory is given a single top-level management group called the "Root" management group. This root management group is built into the hierarchy to have all management groups and subscriptions fold up to it. This root management group allows for global policies and Azure role assignments to be applied at the directory level. The Azure AD Global Administrator needs to elevate themselves to the User Access Administrator role of this root group initially. After elevating access, the administrator can assign any Azure role to other directory users or groups to manage the hierarchy. As administrator, you can assign your own account as owner of the root management group.

Reference:

<https://docs.microsoft.com/en-us/azure/governance/management-groups/overview>

HOTSPOT -

You have an Azure Active Directory (Azure AD) tenant named adatum.com. Adatum.com contains the groups in the following table.

Name	Group type	Membership type	Membership rule
Group1	Security	Dynamic user	(user.city -startsWith "m")
Group2	Microsoft Office 365	Dynamic user	(user.department -notIn ["human resource"])
Group3	Microsoft Office 365	Assigned	Not applicable

You create two user accounts that are configured as shown in the following table.

Name	City	Department	Office 365 license assigned
User1	Montreal	Human resources	Yes
User2	Melbourne	Marketing	No

To which groups do User1 and User2 belong? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

User1:

▼

Group1 only

Group2 only

Group3 only

Group1 and Group2 only

Group1 and Group3 only

Group2 and Group3 only

Group1, Group2, and Group3

User2:

▼

Group1 only

Group2 only

Group3 only

Group1 and Group2 only

Group1 and Group3 only

Group2 and Group3 only

Group1, Group2, and Group3

Correct Answer:

Answer Area

User1:

▼

Group1 only

Group2 only

Group3 only

Group1 and Group2 only

Group1 and Group3 only

Group2 and Group3 only

Group1, Group2, and Group3

User2:

▼

Group1 only

Group2 only

Group3 only

Group1 and Group2 only

Group1 and Group3 only

Group2 and Group3 only

Group1, Group2, and Group3

Box 1: Group 1 only -

First rule applies -

Box 2: Group1 and Group2 only -

Both membership rules apply.

Reference:

<https://docs.microsoft.com/en-us/sccm/core/clients/manage/collections/create-collections>

HOTSPOT -

You have a hybrid deployment of Azure Active Directory (Azure AD) that contains the users shown in the following table.

Name	Type	Source
User1	Member	Azure AD
User2	Member	Windows Server Active Directory
User3	Guest	Microsoft account

You need to modify the JobTitle and UsageLocation attributes for the users.

For which users can you modify the attributes from Azure AD? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

JobTitle:

User1 only

User1 and User2 only

User1 and User3 only

User1, User2, and User3

UsageLocation:

User1 only

User1 and User2 only

User1 and User3 only

User1, User2, and User3

Correct Answer:

Answer Area

JobTitle:

User1 only

User1 and User2 only

User1 and User3 only

User1, User2, and User3

UsageLocation:

User1 only

User1 and User2 only

User1 and User3 only

User1, User2, and User3

Box 1: User1 and User3 only -

You must use Windows Server Active Directory to update the identity, contact info, or job info for users whose source of authority is Windows Server Active Directory.

Box 2: User1, User2, and User3 -

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-users-profile-azure-portal>

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 need to ensure that an Azure Active Directory (Azure AD) user named Admin1 is assigned the required role to enable Traffic Analytics for an Azure subscription.

Solution: You assign the Network Contributor role at the subscription level to Admin1.

Does this meet the goal?

A. Yes

B. No

Correct Answer: A

Your account must meet one of the following to enable traffic analytics:

Your account must have any one of the following Azure roles at the subscription scope: owner, contributor, reader, or network contributor.

Reference:

<https://docs.microsoft.com/en-us/azure/network-watcher/traffic-analytics-faq>

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 need to ensure that an Azure Active Directory (Azure AD) user named Admin1 is assigned the required role to enable Traffic Analytics for an Azure subscription.

Solution: You assign the Owner role at the subscription level to Admin1.

Does this meet the goal?

A. Yes

B. No

Hide Solution

Discussion 14

**Correct Answer: A**

Your account must meet one of the following to enable traffic analytics:

Your account must have any one of the following Azure roles at the subscription scope: owner, contributor, reader, or network contributor.

Reference:

<https://docs.microsoft.com/en-us/azure/network-watcher/traffic-analytics-faq>

## Question #38

## Topic 1

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 need to ensure that an Azure Active Directory (Azure AD) user named Admin1 is assigned the required role to enable Traffic Analytics for an Azure subscription.

Solution: You assign the Reader role at the subscription level to Admin1.

Does this meet the goal?

A. Yes

B. No

Hide Solution

Discussion 43

**Correct Answer: A**

Your account must meet one of the following to enable traffic analytics:

Your account must have any one of the following Azure roles at the subscription scope: owner, contributor, reader, or network contributor.

Reference:

<https://docs.microsoft.com/en-us/azure/network-watcher/traffic-analytics-faq>

## Question #39

## Topic 1

You have an Azure subscription that contains a user named User1.

You need to ensure that User1 can deploy virtual machines and manage virtual networks. The solution must use the principle of least privilege.

Which role-based access control (RBAC) role should you assign to User1?

A. Owner

B. Virtual Machine Contributor

C. Contributor

D. Virtual Machine Administrator Login

Hide Solution

Discussion 100

**Correct Answer: B**

Virtual Machine Contributor: Lets you manage virtual machines, but not access to them, and not the virtual network or storage account they're connected to.

Incorrect Answers:

A: Owner: Grants full access to manage all resources, including the ability to assign roles in Azure RBAC.

C: Contributor: Grants full access to manage all resources, but does not allow you to assign roles in Azure RBAC.

D: Virtual Machine Administrator Login: View Virtual Machines in the portal and login as administrator.

Reference:

<https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles>

HOTSPOT -

You have an Azure Active Directory (Azure AD) tenant that contains three global administrators named Admin1, Admin2, and Admin3. The tenant is associated to an Azure subscription. Access control for the subscription is configured as shown in the Access control exhibit. (Click the Access Control tab.)

Manage access to Azure resources for users, groups, service principals and managed identities at this scope by creating role assignments. [Learn more](#)

Name ⓘ

Scope ⓘ  

All scopes

Type ⓘ  

All

Group by ⓘ  

Role

Role ⓘ  

Owner

☒ Select all  
☒ Owner

1 items (1 Users)

☐

NAME

TYPE

ROLE

SCOPE

OWNER

AD

Admin3

Admin3@contltd...

User

Owner ⓘ

This resource

You sign in to the Azure portal as Admin1 and configure the tenant as shown in the Tenant exhibit. (Click the Tenant tab.)

Save

Discard

Directory properties

\* Name

Cont190525outlook

✓

Country or region

Slovenia

Location

EU Model Clause compliant datacenters

Notification language

English

▼

Directory ID

a93d91a6-faca-4fa6-a749-f6c25469152e

Technical contact

✓

Global privacy contact

✓

Privacy statement URL

✓

Access management for Azure resources

Admin1@Cont190525outlook.onmicrosoft.com (Admin1@Cont190525outlook.onmicrosoft.com) can manage access to all Azure subscriptions and management groups in this directory. [Learn more](#)

Yes

No



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
Admin1 can add Admin 2 as an owner of the subscription.	<input type="radio"/>	<input type="radio"/>
Admin3 can add Admin 2 as an owner of the subscription.	<input type="radio"/>	<input type="radio"/>
Admin2 can create a resource group in the subscription.	<input type="radio"/>	<input type="radio"/>

Answer Area

Statements	Yes	No
Admin1 can add Admin 2 as an owner of the subscription.	<input type="radio"/>	<input checked="" type="radio"/>
Admin3 can add Admin 2 as an owner of the subscription.	<input checked="" type="radio"/>	<input type="radio"/>
Admin2 can create a resource group in the subscription.	<input type="radio"/>	<input checked="" type="radio"/>

Correct Answer:

Box 1: No -

Only Admin3, the owner, can assign ownership.

Box 2: Yes -

Box 3: No -

Reference:

<https://docs.microsoft.com/en-us/azure/cost-management-billing/manage/add-change-subscription-administrator>