



-The original certification question!

<https://www.it-exams.com>

Exam Number/Code:AZ-104

Exam Name: Microsoft Azure
Administrator

Version: Demo

Question Set 1

Q1

You have an Azure subscription that contains the following users in an Azure Active Directory tenant named contoso.onmicrosoft.com:

Name	Role	Scope
User1	Global administrator	Azure Active Directory
User2	Global administrator	Azure Active Directory
User3	User administrator	Azure Active Directory
User4	Owner	Azure Subscription

User1 creates a new Azure Active Directory tenant named external.contoso.onmicrosoft.com.

You need to create new user accounts in external.contoso.onmicrosoft.com.

Solution: You instruct User2 to create the user accounts.

Does that meet the goal?

- A. Yes
- B. No

Answer: A

Explanation:

Only a global administrator can add users to this tenant.

Reference:

<https://docs.microsoft.com/en-us/azure/devops/organizations/accounts/add-users-to-azure-ad>

Q2

You have an Azure subscription that contains the following users in an Azure Active Directory tenant named contoso.onmicrosoft.com:

Name	Role	Scope
User1	Global administrator	Azure Active Directory
User2	Global administrator	Azure Active Directory
User3	User administrator	Azure Active Directory
User4	Owner	Azure Subscription

User1 creates a new Azure Active Directory tenant named external.contoso.onmicrosoft.com.

You need to create new user accounts in external.contoso.onmicrosoft.com.

Solution: You instruct User4 to create the user accounts.

Does that meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

Only a global administrator can add users to this tenant.

Reference:

<https://docs.microsoft.com/en-us/azure/devops/organizations/accounts/add-users-to-azure-ad>

Q3

You have an Azure subscription that contains the following users in an Azure Active Directory tenant named contoso.onmicrosoft.com:

Name	Role	Scope
User1	Global administrator	Azure Active Directory
User2	Global administrator	Azure Active Directory
User3	User administrator	Azure Active Directory
User4	Owner	Azure Subscription

User1 creates a new Azure Active Directory tenant named external.contoso.onmicrosoft.com.

You need to create new user accounts in external.contoso.onmicrosoft.com.

Solution: You instruct User3 to create the user accounts.

Does that meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

Only a global administrator can add users to this tenant.

Reference:

<https://docs.microsoft.com/en-us/azure/devops/organizations/accounts/add-users-to-azure-ad>

Q4

HOTSPOT

You have an Azure subscription named Subscription1 that contains a resource group named RG1.

In RG1, you create an internal load balancer named LB1 and a public load balancer named LB2.

You need to ensure that an administrator named Admin1 can manage LB1 and LB2. The solution must follow the principle of least privilege.

Which role should you assign to Admin1 for each task? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

To add a backend pool to LB1:

	▼
Contributor on LB1	
Network Contributor on LB1	
Network Contributor on RG1	
Owner on LB1	

To add a health probe to LB2:

	▼
Contributor on LB2	
Network Contributor on LB2	
Network Contributor on RG1	
Owner on LB2	

Answer:

Answer Area

To add a backend pool to LB1:

	▼
Contributor on LB1	
Network Contributor on LB1	
Network Contributor on RG1	
Owner on LB1	

To add a health probe to LB2:

	▼
Contributor on LB2	
Network Contributor on LB2	
Network Contributor on RG1	
Owner on LB2	

Explanation:

The Network Contributor role lets you manage networks, but not access them.

Reference:

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

Q5

You have an Azure subscription that contains an Azure Active Directory (Azure AD) tenant named contoso.com and an Azure Kubernetes Service (AKS) cluster named AKS1.

An administrator reports that she is unable to grant access to AKS1 to the users in contoso.com.

You need to ensure that access to AKS1 can be granted to the contoso.com users.

What should you do first?

- A. From contoso.com, modify the Organization relationships settings.
- B. From contoso.com, create an OAuth 2.0 authorization endpoint.

- C. Recreate AKS1.
- D. From AKS1, create a namespace.

Answer: B

Reference:

<https://kubernetes.io/docs/reference/access-authn-authz/authentication/>

Q6

You have a Microsoft 365 tenant and an Azure Active Directory (Azure AD) tenant named contoso.com.

You plan to grant three users named User1, User2, and User3 access to a temporary Microsoft SharePoint document library named Library1.

You need to create groups for the users. The solution must ensure that the groups are deleted automatically after 180 days.

Which two groups should you create? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. a Microsoft 365 group that uses the Assigned membership type
- B. a Security group that uses the Assigned membership type
- C. a Microsoft 365 group that uses the Dynamic User membership type
- D. a Security group that uses the Dynamic User membership type
- E. a Security group that uses the Dynamic Device membership type

Answer: AC

Explanation:

You can set expiration policy only for Office 365 groups in Azure Active Directory (Azure AD).

Note: With the increase in usage of Office 365 Groups, administrators and users need a way to clean up unused groups. Expiration policies can help remove inactive groups from the system and make things cleaner.

When a group expires, all of its associated services (the mailbox, Planner, SharePoint site, etc.) are also deleted.

You can set up a rule for dynamic membership on security groups or Office 365 groups.

Incorrect Answers:

B, D, E: You can set expiration policy only for Office 365 groups in Azure Active Directory (Azure AD).

Reference:

[https://docs.microsoft.com/en-us/office365/admin/create-groups/office-365-groups-expiration-policy? view=o365-worldwide](https://docs.microsoft.com/en-us/office365/admin/create-groups/office-365-groups-expiration-policy?view=o365-worldwide)

Q7

HOTSPOT

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

Name	Type	Member of
User1	Member	Group1
User2	Guest	Group1
User3	Member	None
UserA	Member	Group2
UserB	Guest	Group2

User3 is the owner of Group1.

Group2 is a member of Group1.

You configure an access review named Review1 as shown in the following exhibit:

Create an access review

Access reviews enable reviewers to attest user's membership in a group or access to an application.

* Review name

Description

* Start date

Frequency

Duration (in days)

End

* Number of times

* End date

Users

Users to review

Scope Guest users only Everyone

* Group

Reviewers

Reviewers

Programs

Link to program

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
User3 can perform an access review of User1	<input type="radio"/>	<input type="radio"/>
User3 can perform an access review of UserA	<input type="radio"/>	<input type="radio"/>
User3 can perform an access review of UserB	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
User3 can perform an access review of User1	<input type="radio"/>	<input checked="" type="radio"/>
User3 can perform an access review of UserA	<input type="radio"/>	<input checked="" type="radio"/>
User3 can perform an access review of UserB	<input checked="" type="radio"/>	<input type="radio"/>

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/governance/create-access-review>

Q8

HOTSPOT

You have the Azure management groups shown in the following table:

Name	In management group
Tenant Root Group	<i>Not applicable</i>
ManagementGroup11	Tenant Root Group
ManagementGroup12	Tenant Root Group
ManagementGroup21	ManagementGroup11

You add Azure subscriptions to the management groups as shown in the following table:

Name	Management group
Subscription1	ManagementGroup21
Subscription2	ManagementGroup12

You create the Azure policies shown in the following table:

Name	Parameter	Scope
Not allowed resource types	virtualNetworks	Tenant Root Group
Allowed resource types	virtualNetworks	ManagementGroup12

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
You can create a virtual network in Subscription1.	<input type="radio"/>	<input type="radio"/>
You can create a virtual machine in Subscription2.	<input type="radio"/>	<input type="radio"/>
You can add Subscription1 to ManagementGroup11.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
You can create a virtual network in Subscription1.	<input type="radio"/>	<input checked="" type="radio"/>
You can create a virtual machine in Subscription2.	<input checked="" type="radio"/>	<input type="radio"/>
You can add Subscription1 to ManagementGroup11.	<input checked="" type="radio"/>	<input type="radio"/>

Explanation:

Box 1: No

Virtual networks are not allowed at the root and is inherited. Deny overrides allowed.

Box 2: Yes

Virtual Machines can be created on a Management Group provided the user has the required RBAC permissions.

Box 3: Yes

Subscriptions can be moved between Management Groups provided the user has the required RBAC permissions.

Reference:

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

<https://docs.microsoft.com/en-us/azure/governance/management-groups/manage#moving-management-groups-and-subscriptions>