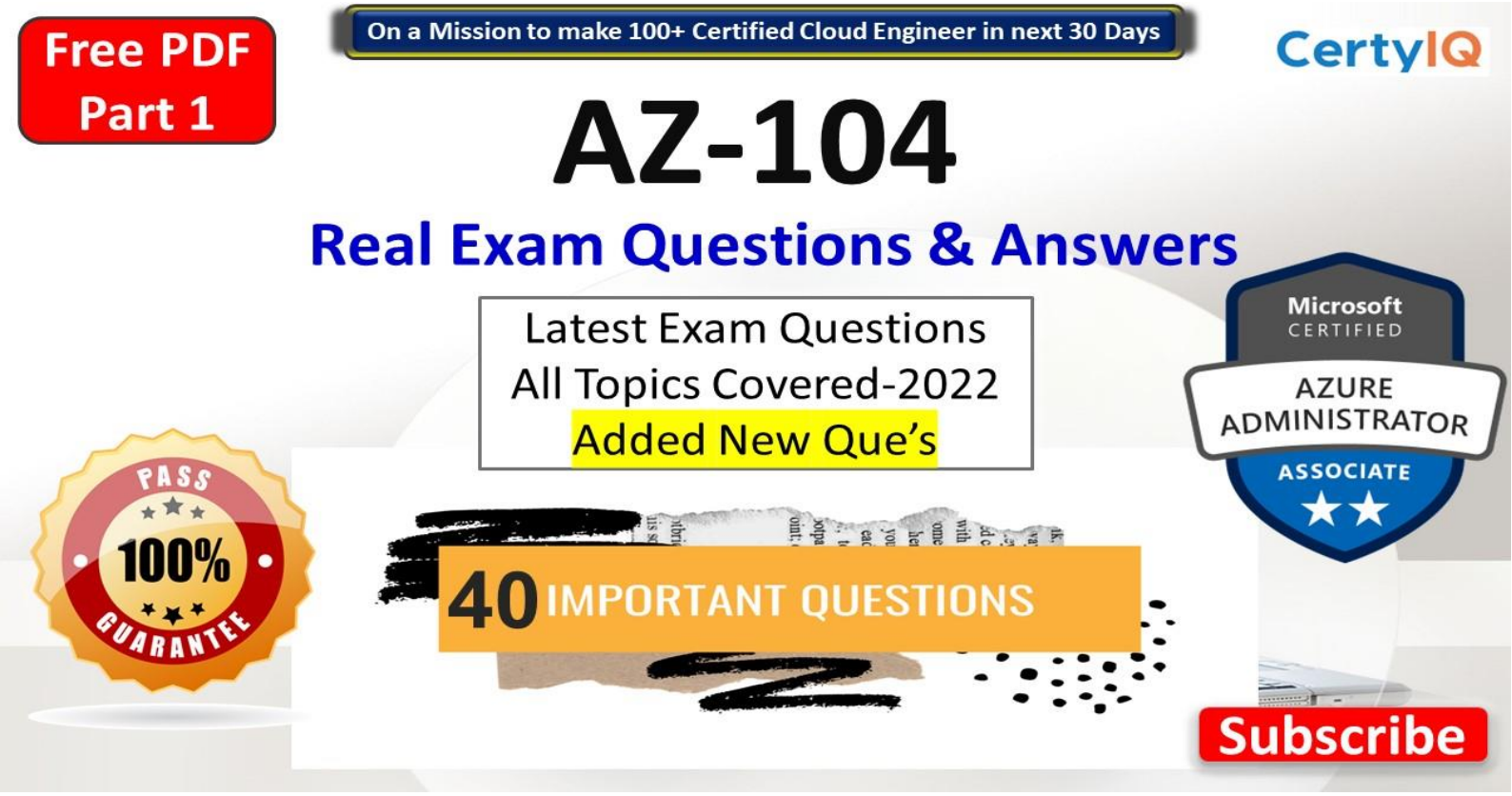


AZ-104 Microsoft Azure Administrator Exam Format

Exam Name	Microsoft AZ-104
Technology	Microsoft Azure
AZ 104 Exam Cost	USD 165.00*
Total Questions	40 – 60 Questions
Passing Score	700 points out of 1000
Exam Duration	120 Minutes
Languages	English, Japanese, French, Spanish, Chinese (Simplified), Korean, Portuguese (Brazil), Russian, German, Arabic (Saudi Arabia), Chinese (Traditional), Italian, Indonesian (Indonesia)

Skills Measured in Microsoft Azure Administrator AZ-104 Exam

- Manage Azure identities and governance (15-20%)
- Implement and manage storage (10-15%)
- Deploy and manage Azure compute resources (25-30%)
- Configure and manage virtual networking (30-35%)
- Monitor and back up Azure resources (10-15%)

Source: https://docs.microsoft.com/en-us/learn/certifications/exams/az-104

Question 1

CertyIQ

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 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

Explanation:

It is another tenant.

user2 is a global admin on the original tenant, not on the newly created tenant

Question 2

CertyIQ

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 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

Explanation:

B:No, when you create a new tenant, the creator is the only global admin and owner, he must first give access to others to allow anything. https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-access-create-new-tenant#your-user-account-in-the-new-tenant

Question 3 CertyIQ

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 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

Explanation:

B:No, when you create a new tenant, the creator is the only global admin and owner, he must first give access to others to allow anything. https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-access-create-new-tenant#your-user-account-in-the-new-tenant

Question 4

CertyIQ

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 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:

For creating a backend pool we need permission to access VNet on RG. For creating a health probe we need to have permission for deployment on Resource Group. So we both the option is Added the network Contributor Role to RG1.

Question 5 CertyIQ

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.

Explanation:

Answer is B- Cluster administrators can configure Kubernetes role-based access control (Kubernetes RBAC) based on a user's identity or directory group membership. Azure AD authentication is provided to AKS clusters with OpenID Connect. OpenID Connect is an identity layer built on top of the OAuth 2.0 protocol
https://docs.microsoft.com/en-us/azure/aks/managed-aad

Question 6 CertyIQ

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

Explanation:

Only O365 groups support automatic deletion after 180 days.

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

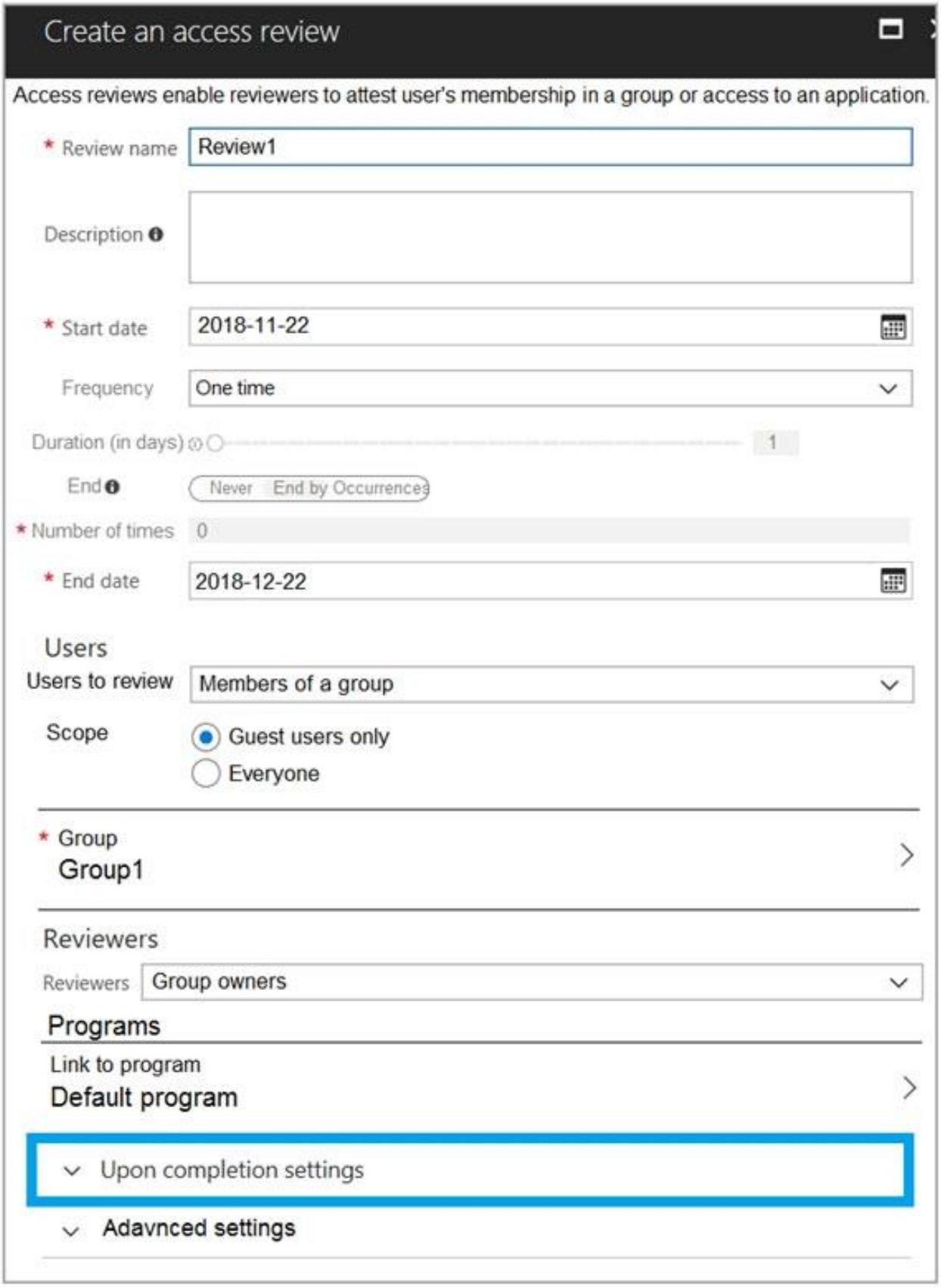
Question 7

CertyIQ

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:



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	○	○
User3 can perform an access review of UserA	○	○
User3 can perform an access review of UserB	○	○

Correct Answer:

Answer Area

Statements	Yes	No
User3 can perform an access review of User1	○	○
User3 can perform an access review of UserA	○	○
User3 can perform an access review of UserB	○	○

Explanation:

User3 can perform an access review of User1 = No
User1 is a Member and not a Guest Account, Access Review specified Guests only.

User3 can perform an access review of UserA = No
User1 is a Member and not a Guest Account, Access Review specified Guests only.

User3 can perform an access review of UserB = No
Created Group 1 and Group 2, added Group 2 as a member in Group 1,
Added guest Accounts to Group 1 and Group 2,
In the Access Review results only the Guest Accounts in Group 1 appeared for review and "Not" the Guest accounts in Group 2.

Question 8 CertyIQ

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

Name	In management group
Tenant Root Group	*Not applicable*
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.	○	○
You can create a virtual machine in Subscription2.	○	○
You can add Subscription1 to ManagementGroup11.	○	○

Correct Answer:

Answer Area

Statements	Yes	No
You can create a virtual network in Subscription1.	○	○
You can create a virtual machine in Subscription2.	○	○
You can add Subscription1 to ManagementGroup11.	○	○

Explanation:

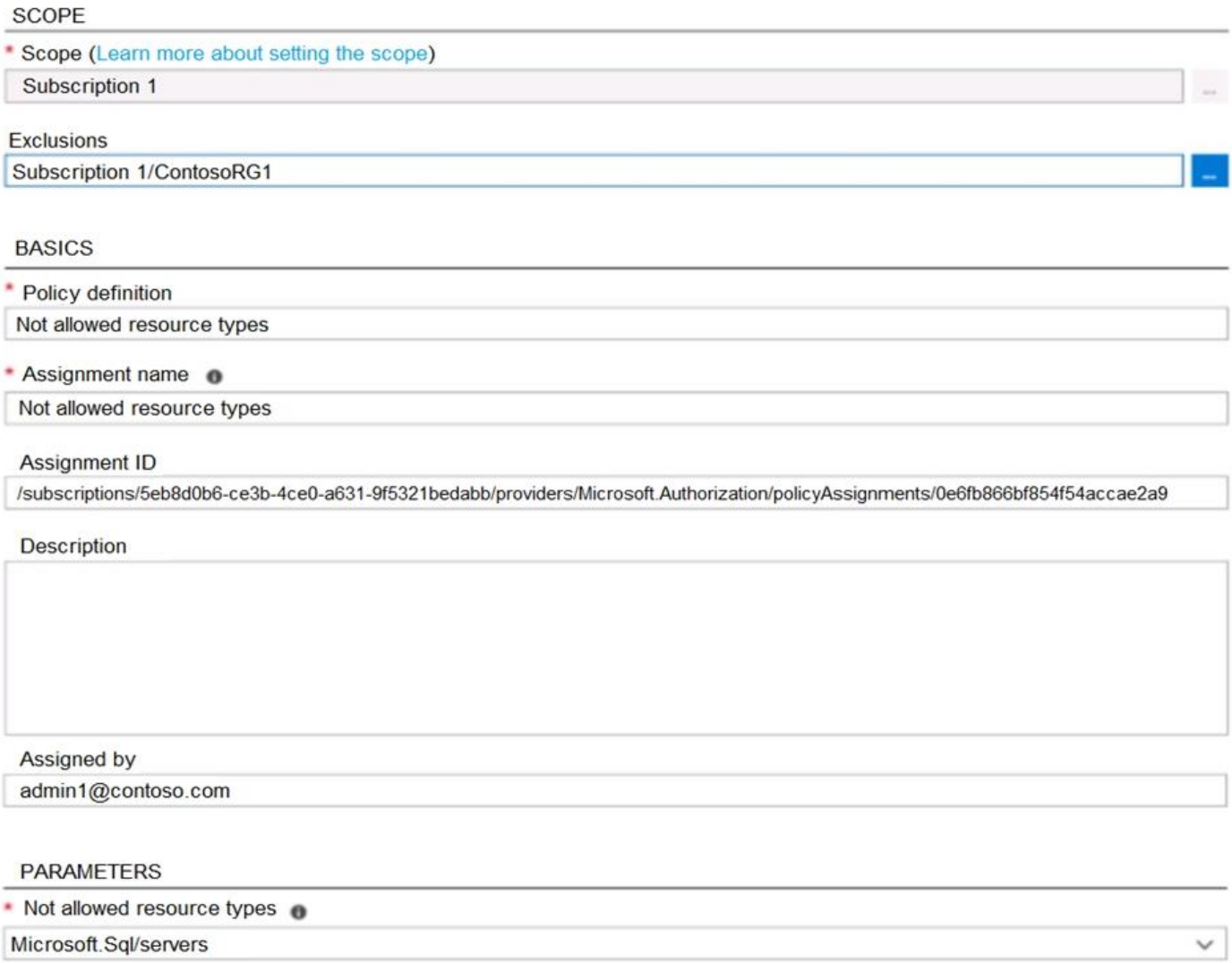
- NO: Subscription 1: is not allowed to create a VNET.
- NO: Subscription 2: Allowed to create a VNET which restricts anything else.

- NO: Subscription 1: already in one Management group called 21, so cannot add into another. A Subscription can be assigned to 1 Management Group.

Question 9

CertyIQ

You have an Azure policy as shown in the following exhibit:



What is the effect of the policy?

A. You are prevented from creating Azure SQL servers anywhere in Subscription 1.

B. You can create Azure SQL servers in ContosoRG1 only.

C. You are prevented from creating Azure SQL Servers in ContosoRG1 only.

D. You can create Azure SQL servers in any resource group within Subscription 1.

Explanation:

You are prevented from creating Azure SQL servers anywhere in Subscription 1 with the exception of ContosoRG1

Question 10

CertyIQ

HOTSPOT -
You have an Azure subscription that contains the resources shown in the following table:

Name	Type	Resource group	Tag
RG6	Resource group	*Not applicable*	*None*
VNET1	Virtual network	RG6	Department: D1

You assign a policy to RG6 as shown in the following table:

Section	Setting	Value
Scope	Scope	Subscription1/RG6
	Exclusions	*None*
Basics	Policy definition	Apply tag and its default value
	Assignment name	Apply tag and its default value
Parameters	Tag name	Label
	Tag value	Value1

To RG6, you apply the tag: RGroup: RG6.
You deploy a virtual network named VNET2 to RG6.
Which tags apply to VNET1 and VNET2? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Hot Area:

Answer Area

VNET1:

- None
- Department: D1 only
- Department: D1, and RGroup: RG6 only
- Department: D1, and Label: Value1 only
- Department: D1, RGroup: RG6, and Label: Value1

VNET2:

- None
- RGroup: RG6 only
- Label: Value1 only
- RGroup: RG6, and Label: Value1

Answer Area

Correct Answer:

VNET1:

- None
- Department: D1 only
- Department: D1, and RGroup: RG6 only
- Department: D1, and Label: Value1 only
- Department: D1, RGroup: RG6, and Label: Value1

VNET2:

- None
- RGroup: RG6 only
- Label: Value1 only
- RGroup: RG6, and Label: Value1

Explanation:

Resources created before policy creation will not inherit the policy rules. so, VNET1 will only have Department: D1 tag, VNET 2 will have Label : Value1

Question 11

CertyIQ

You have an Azure subscription named AZPT1 that contains the resources shown in the following table:

Name	Type
storage1	Azure Storage account
VNET1	Virtual network
VM1	Azure virtual machine
VM1Managed	Managed disk for VM1
RVAULT1	Recovery Services vault for the site recovery of VM1

You create a new Azure subscription named AZPT2.
You need to identify which resources can be moved to AZPT2.
Which resources should you identify?

A. VM1, storage1, VNET1, and VM1Managed only

B. VM1 and VM1Managed only

C. VM1, storage1, VNET1, VM1Managed, and RVAULT1

D. RVAULT1 only

Explanation:

All of them. Moving a resource only moves it to a new Resource Group or Subscription. It doesn't change the location of the resource.

You can move a VM and its associated resources to a different subscription by using the Azure portal.
You can now move an Azure Recovery Service (ASR) Vault to either a new resource group within the current subscription

or to a new subscription.
Reference:
https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/move-resource-group-and-subscription

Question 12

CertyIQ

You recently created a new Azure subscription that contains a user named Admin1.
Admin1 attempts to deploy an Azure Marketplace resource by using an Azure Resource Manager template.
Admin1 deploys the template by using Azure
PowerShell and receives the following error message: User failed validation to purchase resources. Error message: Legal terms have not been accepted for this item on this subscription. To accept legal terms, please go to the Azure portal (http://go.microsoft.com/fwlink/?LinkId=534873) and configure programmatic deployment for the Marketplace item or create it there for the first time.
You need to ensure that Admin1 can deploy the Marketplace resource successfully.
What should you do?

A. From Azure PowerShell, run the Set-AzApiManagementSubscription cmdlet

B. From the Azure portal, register the Microsoft.Marketplace resource provider

C. From Azure PowerShell, run the Set-AzMarketplaceTerms cmdlet

D. From the Azure portal, assign the Billing administrator role to Admin1

Explanation:

Set-AzMarketplaceTerms -Publisher <String> -Product <String> -Name <String> [-Accept] [-Terms <PSAgreementTerms>] [-DefaultProfile <IAzureContextContainer>] [-WhatIf] [-Confirm] [<CommonParameters>]

Reference:

https://docs.microsoft.com/en-us/powershell/module/Az.MarketplaceOrdering/Set-AzMarketplaceTerms?view=azps-4.6.0

Question 13

CertyIQ

You have an Azure Active Directory (Azure AD) tenant that contains 5,000 user accounts.
You create a new user account named AdminUser1.
You need to assign the User administrator administrative role to AdminUser1.
What should you do from the user account properties?

A. From the Licenses blade, assign a new license

B. From the Directory role blade, modify the directory role

C. From the Groups blade, invite the user account to a new group

Explanation:

Active Directory -> Manage Section -> Roles and administrators-> Search for Admin and assign a user to it.

Assign a role to a user -
1. Sign in to the Azure portal with an account that's a global admin or privileged role admin for the directory.
2. Select Azure Active Directory, select Users, and then select a specific user from the list.
3. For the selected user, select Directory role, select Add role, and then pick the appropriate admin roles from the Directory roles list, such as Conditional access administrator.
4. Press Select to save.

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-users-assign-role-azure-portal

Question 14

CertyIQ

You have an Azure Active Directory (Azure AD) tenant named contoso.onmicrosoft.com that contains 100 user accounts.
You purchase 10 Azure AD Premium P2 licenses for the tenant.
You need to ensure that 10 users can use all the Azure AD Premium features.
What should you do?

A. From the Licenses blade of Azure AD, assign a license

B. From the Groups blade of each user, invite the users to a group

C. From the Azure AD domain, add an enterprise application

D. From the Directory role blade of each user, modify the directory role

Explanation:

Correct Answer: A

Active Directory-> Manage Section > Choose Licenses -> All Products -> Select Azure Active Directory Premium P2 -> Then assign a user to it.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/license-users-groups

Question 15

CertyIQ

You have an Azure subscription named Subscription1 and an on-premises deployment of Microsoft System Center Service Manager.
Subscription1 contains a virtual machine named VM1.
You need to ensure that an alert is set in Service Manager when the amount of available memory on VM1 is below 10 percent.
What should you do first?

A. Create an automation runbook

B. Deploy a function app

C. Deploy the IT Service Management Connector (ITSM)

D. Create a notification

Explanation:

Correct Answer: C

IT Service Management Connector (ITSMC) allows you to connect Azure to a supported IT Service Management (ITSM) product or service. Azure services like Azure Log Analytics and Azure Monitor provide tools to detect, analyze, and troubleshoot problems with your Azure and non-Azure resources. But the work items related to an issue typically reside in an ITSM product or service. ITSMC provides a bi-directional connection between Azure and ITSM tools to help you resolve issues faster. ITSMC supports connections with the following ITSM tools: ServiceNow, System Center Service Manager, Provance, Cherwell.

Reference:

https://docs.microsoft.com/en-us/azure/azure-monitor/alerts/itsmc-overview

Question 16

CertyIQ

You sign up for Azure Active Directory (Azure AD) Premium.
You need to add a user named admin1@contoso.com as an administrator on all the computers that will be joined to the Azure AD domain.
What should you configure in Azure AD?

A. Device settings from the Devices blade

B. Providers from the MFA Server blade

C. User settings from the Users blade

D. General settings from the Groups blade

Explanation:

Correct Answer: A
When you connect a Windows device with Azure AD using an Azure AD join, Azure AD adds the following security principles to the local administrators group on the device:
- The Azure AD global administrator role
- The Azure AD device administrator role
- The user performing the Azure AD join

In the Azure portal, you can manage the device administrator role on the Devices page. To open the Devices page:
1. Sign in to your Azure portal as a global administrator or device administrator.
2. On the left navbar, click Azure Active Directory.
3. In the Manage section, click Devices.
4. On the Devices page, click Device settings.
5. To modify the device administrator role, configure Additional local administrators on Azure AD joined devices

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/devices/assign-local-admin

Question 17

CertyIQ

HOTSPOT -
You have Azure Active Directory tenant named Contoso.com that includes following users:

Name	Role
User1	Cloud device administrator
User2	User administrator

Contoso.com includes following Windows 10 devices:

Name	Join type
Device1	Azure AD registered
Device2	Azure AD joined

You create following security groups in Contoso.com:

Name	Membership Type	Owner
Group1	Assigned	User2
Group2	Dynamic Device	User2

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
User1 can add Device2 to Group1	○	○
User2 can add Device1 to Group1	○	○
User2 can add Device2 to Group2	○	○

Correct Answer:

Answer Area

Statements	Yes	No
User1 can add Device2 to Group1	○	○
User2 can add Device1 to Group1	○	○
User2 can add Device2 to Group2	○	○

Explanation:

Groups can contain both registered and joined devices as members.
As a global administrator or cloud device administrator, you can manage the registered or joined devices. Intune Service administrators can update and delete devices. User administrator can manage users but not devices.
User1 is a cloud device administrator. Users in this role can enable, disable, and delete devices in Azure AD and read Windows 10 BitLocker keys (if present) in the Azure portal. The role does not grant permissions to manage any other properties on the device.

User2 is the owner of Group1. He can add Device1 to Group1.

Group2 is configured for dynamic membership. The properties on which the membership of a device in a group of the type dynamic device are defined cannot be changed by either an end user or an user administrator. User2 cannot add any device to Group2.

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/devices/device-management-azure-portal

Question 18

CertyIQ

You have an Azure subscription that contains a resource group named RG26.
RG26 is set to the West Europe location and is used to create temporary resources for a project. RG26 contains the resources shown in the following table.

Name	Type	Location
VM1	Virtual machine	North Europe
RGV1	Recovery Services vault	North Europe
SQLD01	Azure SQL database	North Europe
AZSQL01	Azure SQL database server	North Europe
sa001	Storage account	West Europe

SQLDB01 is backed up to RGV1.
When the project is complete, you attempt to delete RG26 from the Azure portal. The deletion fails.
You need to delete RG26.
What should you do first?

A. Delete VM1

B. Stop VM1

C. Stop the backup of SQLDB01

D. Delete sa001

Explanation:

Answer: C (Stop the backup of SQLDB01) is correct.
In addition to removing all the resources, You can do the following.
- need to stop the backup up first

- disable the Soft Delete Feature in Recovery Vault (because if you delete the backup then it will be in the recycle bin for the next 14 days and until that you wouldn't be able to remove the RV [RV > Properties > Security Settings > Soft Delete > Disable].
- Delete the all backup
- now you will be able to delete all resources along with RV.

Question 19

CertyIQ

You have an Azure subscription named Subscription1 that contains a virtual network named VNet1. VNet1 is in a resource group named RG1.
Subscription1 has a user named User1. User1 has the following roles:

- Reader
- Security Admin

Security Reader -

You need to ensure that User1 can assign the Reader role for VNet1 to other users.
What should you do?

A. Remove User1 from the Security Reader role for Subscription1. Assign User1 the Contributor role for Subscription1.

B. Assign User1 the Owner role for VNet1.

C. Assign User1 the Network Contributor role for VNet1.

D. Assign User1 the Network Contributor role for RG1.

Explanation:

B is correct. (All other options are wrong)

Contributors can manage the resources but cannot grant access to others.

However, if we consider the principle of least privilege, then the more appropriate role should be User Access Administrator.

Reference:

https://docs.microsoft.com/en-us/azure/role-based-access-control/rbac-and-directory-admin-roles#azure-roles

Question 20

CertyIQ

You have an Azure Active Directory (Azure AD) tenant named contosocloud.onmicrosoft.com.
Your company has a public DNS zone for contoso.com.
You add contoso.com as a custom domain name to Azure AD.
You need to ensure that Azure can verify the domain name.
Which type of DNS record should you create?

A. MX

B. NSEC

C. PTR

D. RRSIG

Explanation:

TXT and MX are valid answers.

To verify your custom domain name (example)
1. Sign in to the Azure portal using a Global administrator account for the directory.
2. Select Azure Active Directory, and then select Custom domain names.
3. On the Fabrikam - Custom domain names page, select the custom domain name, Contoso.
4. On the Contoso page, select Verify to make sure your custom domain is properly registered and is valid for Azure AD.
Use either the TXT or the MX record type.
Note:
There are several versions of this question in the exam. The question can have two correct answer:
1. MX
2. TXT
The question can also have other incorrect answer options, including the following:
1. SRV
2. NSEC3
Reference:
https://docs.microsoft.com/en-us/azure/dns/dns-web-sites-custom-domain

Question 21

CertyIQ

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 have an Azure Directory (Azure AD) tenant named Adatum and an Azure Subscription named Subscription1. Adatum contains a group named Developers.
Subscription1 contains a resource group named Dev.
You need to provide the Developers group with the ability to create Azure logic apps in the Dev resource group.
Solution: On Subscription1, you assign the DevTest Labs User role to the Developers group.
Does this meet the goal?

A. Yes

B. No

Explanation:

The Azure DevTest Labs is a role used for Azure DevTest Labs, not for Logic Apps.

DevTest Labs User role only lets you connect, start, restart, and shutdown virtual machines in your Azure DevTest Labs.

The Logic App Contributor role lets you manage logic app, but not access to them. It provides access to view, edit, and update a logic app.

Reference:

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

https://docs.microsoft.com/en-us/azure/logic-apps/logic-apps-securing-a-logic-app

https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#devtest-labs-user

Question 22

CertyIQ

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 have an Azure Directory (Azure AD) tenant named Adatum and an Azure Subscription named Subscription1. Adatum contains a group named Developers.
Subscription1 contains a resource group named Dev.
You need to provide the Developers group with the ability to create Azure logic apps in the Dev resource group.
Solution: On Subscription1, you assign the Logic App Operator role to the Developers group.
Does this meet the goal?

A. Yes

B. No

Explanation:

Correct Answer: B

You would need the Logic App Contributor role.

Logic App Operator - Lets you read, enable, and disable logic apps, but not edit or update them.

Logic App Contributor - Lets you create, manage logic apps, but not access to them.

Reference:

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

https://docs.microsoft.com/en-us/azure/logic-apps/logic-apps-securing-a-logic-app

https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#logic-app-operator

Question 23

CertyIQ

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 have an Azure Directory (Azure AD) tenant named Adatum and an Azure Subscription named Subscription1. Adatum contains a group named Developers.

Subscription1 contains a resource group named Dev.
You need to provide the Developers group with the ability to create Azure logic apps in the Dev resource group.
Solution: On Dev, you assign the Contributor role to the Developers group.
Does this meet the goal?

A. Yes

B. No

Explanation:

Correct Answer: A

The Contributor role can manage all resources (and add resources) in a Resource Group. Contributor role can create logic apps.

Alternatively, we can use the Logic App Contributor role, which lets you manage logic app, but not access to them. It provides access to view, edit, and update a logic app.

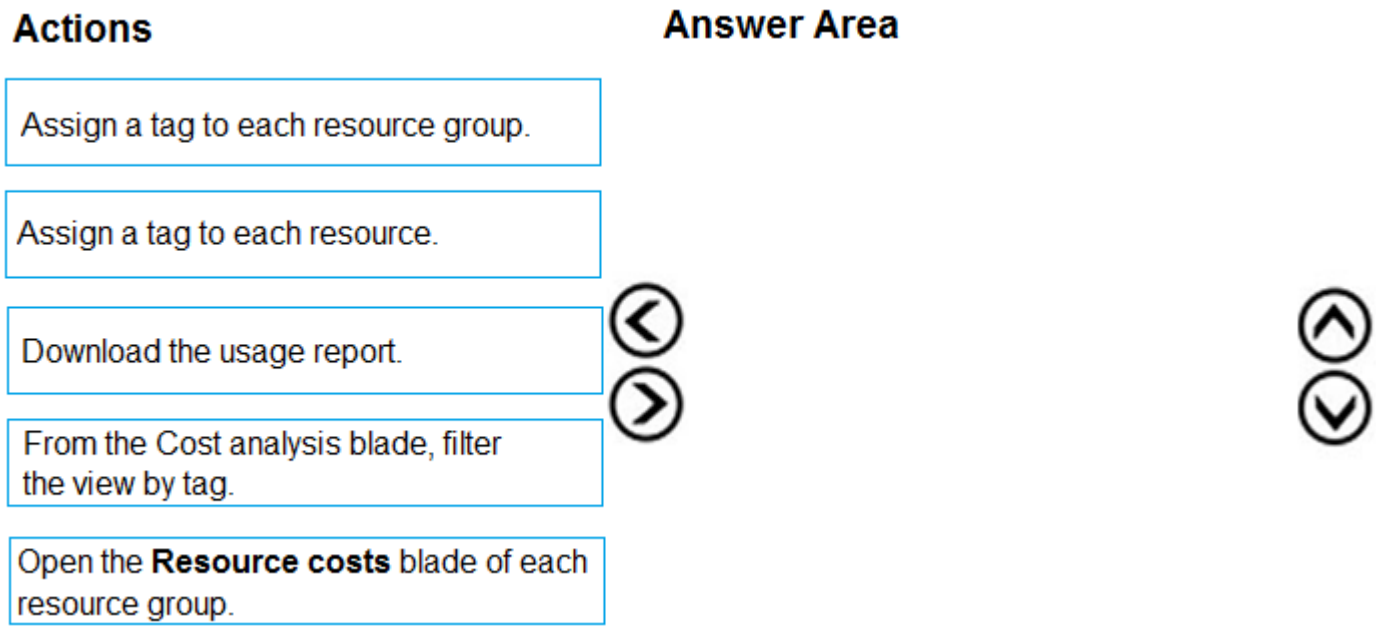
Reference:

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

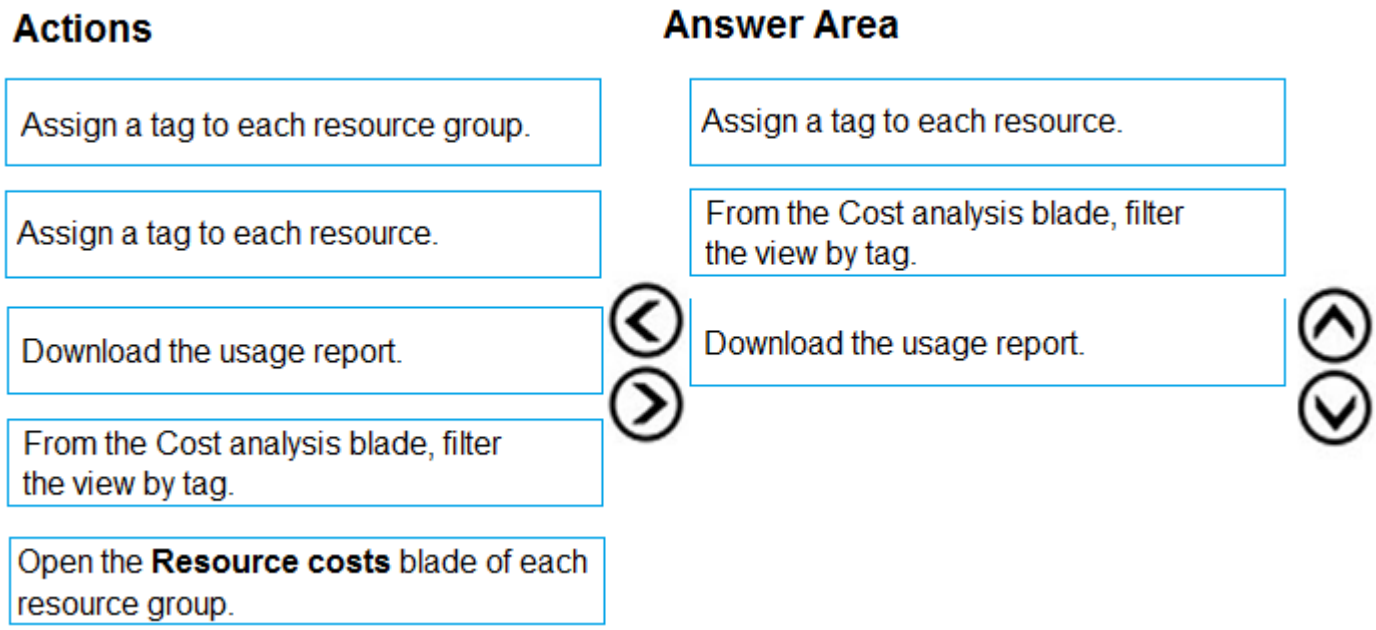
https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#logic-app-contributor

Question 24 CertyIQ

DRAG DROP -
You have an Azure subscription that is used by four departments in your company. The subscription contains 10 resource groups. Each department uses resources in several resource groups.
You need to send a report to the finance department. The report must detail the costs for each department.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.
Select and Place:



Correct Answer:



Explanation:

Box 1: Assign a tag to each resource.
You apply tags to your Azure resources giving metadata to logically organize them into a taxonomy. After you apply tags, you can retrieve all the resources in your subscription with that tag name and value. Each resource or resource group can have a maximum of 15 tag name/value pairs. Tags applied to the resource group are not inherited by the resources in that resource group.
Box 2: From the Cost analysis blade, filter the view by tag
After you get your services running, regularly check how much they're costing you. You can see the current spend and burn rate in Azure portal.
1. Visit the Subscriptions blade in Azure portal and select a subscription.
You should see the cost breakdown and burn rate in the popup blade.
2. Click Cost analysis in the list to the left to see the cost breakdown by resource. Wait 24 hours after you add a service for the data to populate.
3. You can filter by different properties like tags, resource group, and timespan. Click Apply to confirm the filters and Download if you want to export the view to a
Comma-Separated Values (.csv) file.
Box 3: Download the usage report
Reference:
https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-using-tags
https://docs.microsoft.com/en-us/azure/billing/billing-getting-started

Question 25

CertyIQ

You have an Azure subscription named Subscription1 that contains an Azure Log Analytics workspace named Workspace1.
You need to view the error from a table named Event.
Which query should you run in Workspace1?

A. Get-Event Event | where {$_.EventType == "error"}

B. search in (Event) "error"

C. select * from Event where EventType == "error"

D. Get-Event Event | where {$_.EventTye "eq "error"}

Explanation:

To work with Log Analytics data, you need to use the Kusto Query Language (KQL) eg: search in (Event) "error"

Reference:

https://docs.microsoft.com/en-us/azure/azure-monitor/log-query/search-queries

https://docs.microsoft.com/en-us/azure/azure-monitor/log-query/get-started-portal

https://docs.microsoft.com/en-us/azure/data-explorer/kusto/query/searchoperator?pivots=azuredataexplorer

Question 26

CertyIQ

HOTSPOT -
You have an Azure subscription that contains a virtual network named VNET1 in the East US 2 region. A network interface named VM1-NI is connected to
VNET1.
You successfully deploy the following resources in an Azure Resource Manager template.

```
{
    "apiVersion": "2017-03-30",
    "type": "Microsoft.Compute/virtualMachines",
    "name": "VM1"
    "zones": "1",
    "location": "EastUS2",
    "dependsOn": [
      "[resourceId('Microsoft.Network/networkInterfaces', 'VM1-NI')]"
    ],
    "properties": {
      "hardwareProfile": {
        "vmSize": "Standard_A2_v2"
      },
      "osProfile": {
         "computerName": "VM1",
         "adminUsername": "AzureAdmin",
         "adminPassword": "[parameters('adminPassword')]"
      },
    "storageProfile": {
      "imageReference": "[variables('image')]",
      "osDisk": {
        "createOption": "FromImage"
      }
    },
    "networkProfile": {
      "networkInterfaces": [
        {
          "id": "[resourceId('Microsoft.Network/networkInterfaces', 'VM1-NI')]"
        }
      ]
    }
   }
},
{
  "apiVersion": "2017-03-30",
  "type": "Microsoft.Compute/virtualMachines",
  "name": "VM2",
  "zones": "2",
  "location": "EastUS2",
  "dependsOn": [
     "[resourceId('Microsoft.Network/networkInterfaces', 'VM2-NI')]"
  ],
  "properties": {
    "hardwareProfile": {
       "vmSize": "Standard_A2_v2"
    },
    "osProfile": {
      "computerName": "VM2",
      "adminUsername": "AzureAdmin",
      "adminPassword": "[parameters('adminPassword')]"
    },
    "storageProfile": {
      "imageReference": "[variables('image')]",
      "osDisk": {
        "createOption": "FromImage"
      }
    },
    "networkProfile": {
      "networkInterfaces": [
        {
          "id": "[resourceId('Microsoft.Network/networkInterfaces', 'VM2-NI')]"
        }
      ]
    }
   }
}
```

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
VM1 and VM2 can connect to VNET1	○	○
If an Azure datacenter becomes unavailable, VM1 or VM2 will be available.	○	○
If the East US 2 region becomes unavailable, VM1 or VM2 will be available.	○	○

Correct Answer:

Answer Area

Statements	Yes	No
VM1 and VM2 can connect to VNET1	○	○
If an Azure datacenter becomes unavailable, VM1 or VM2 will be available.	○	○
If the East US 2 region becomes unavailable, VM1 or VM2 will be available.	○	○

Explanation:

Correct Answer:

Box 1: Yes

VNET1 is in the same region as VM1 and VM2, so it can connect with both.

Box 2: Yes

Because both VMs are in different Availability Zone, hence either one would be available if one Data Center fails.

Box 3: No

If the Region fails then both VMs, which are present in the Region will not be available.

Reference:

https://docs.microsoft.com/en-us/azure/architecture/resiliency/recovery-loss-azure-region

Question 27

CertyIQ

You have an Azure subscription named Subscription1. Subscription1 contains the resource groups in the following table.

Name	Azure region	Policy
RG1	West Europe	Policy1
RG2	North Europe	Policy2
RG3	France Central	Policy3

RG1 has a web app named WebApp1. WebApp1 is located in West Europe.
You move WebApp1 to RG2.
What is the effect of the move?

A. The App Service plan for WebApp1 remains in West Europe. Policy2 applies to WebApp1.

B. The App Service plan for WebApp1 moves to North Europe. Policy2 applies to WebApp1.

C. The App Service plan for WebApp1 remains in West Europe. Policy1 applies to WebApp1.

D. The App Service plan for WebApp1 moves to North Europe. Policy1 applies to WebApp1.

Explanation:

You can only move a resource to a Resource Group or Subscription, but the location stays the same. When you move WebApp1 to RG2, the resource will be restricted based on the policy of the new Resource Group (Policy2).

Reference:

https://docs.microsoft.com/en-us/azure/app-service/app-service-plan-manage

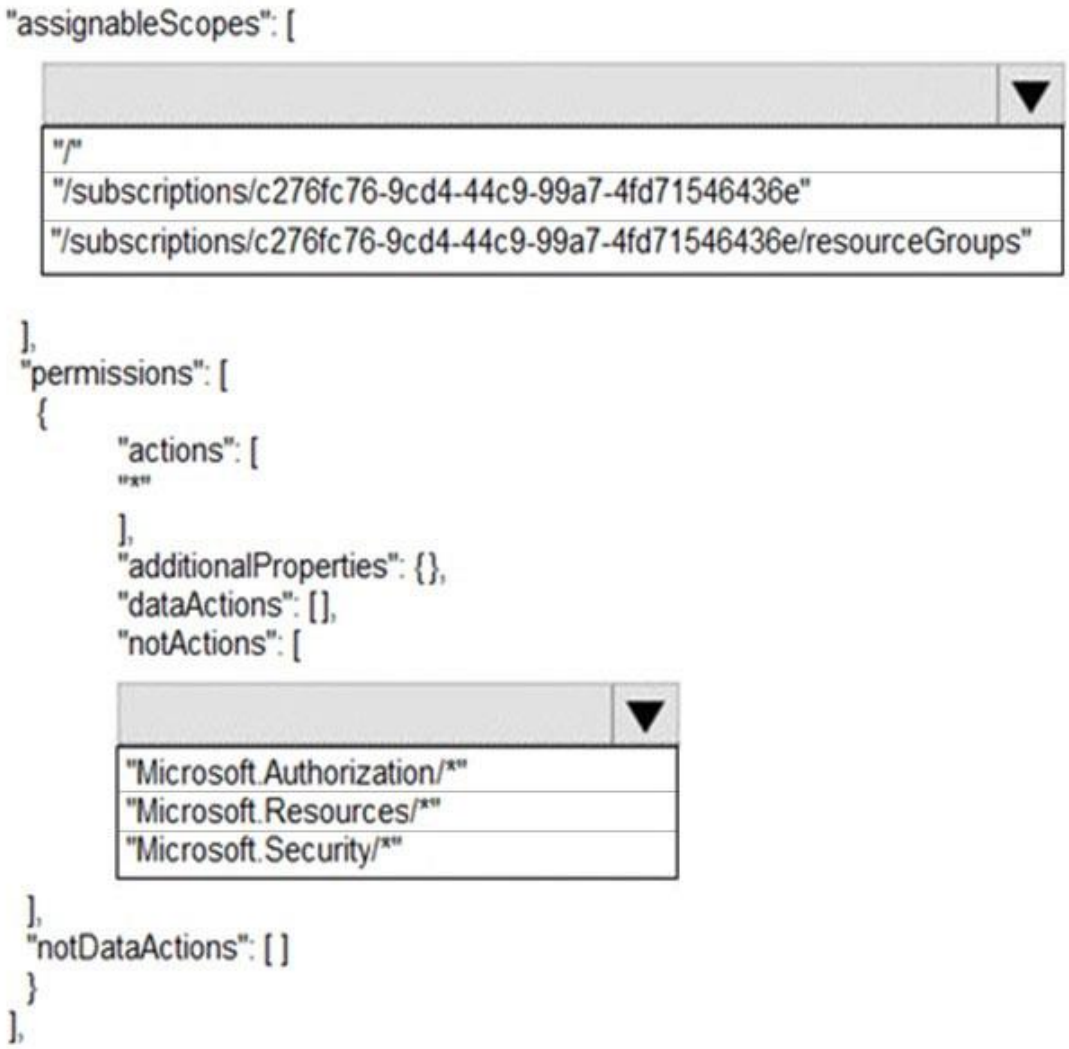
Question 28

CertyIQ

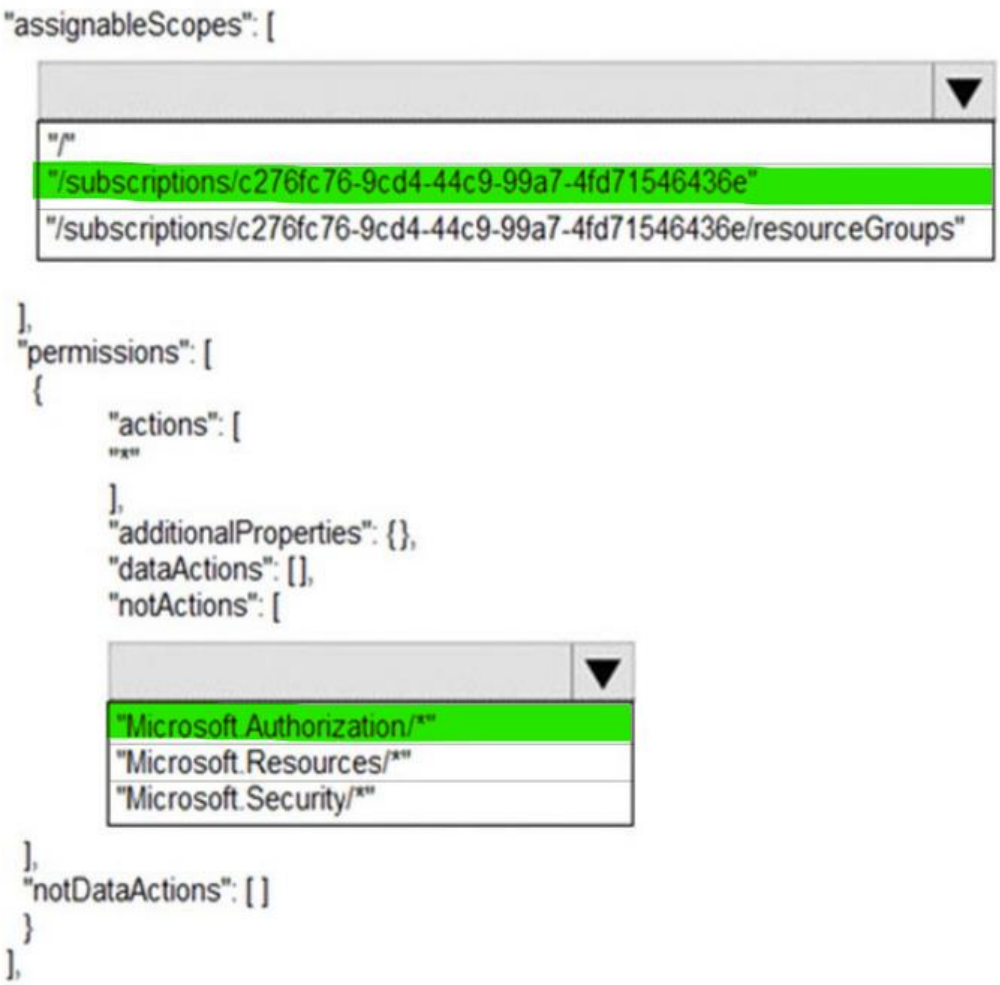
HOTSPOT -
You have an Azure subscription named Subscription1 that has a subscription ID of c276fc76-9cd4-44c9-99a7-4fd71546436e.
You need to create a custom RBAC role named CR1 that meets the following requirements:
- Can be assigned only to the resource groups in Subscription1
- Prevents the management of the access permissions for the resource groups
- Allows the viewing, creating, modifying, and deleting of resources within the resource groups

What should you specify in the assignable scopes and the permission elements of the definition of CR1? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Hot Area:

Answer Area


"assignableScopes": [
"/"
"/subscriptions/c276fc76-9cd4-44c9-99a7-4fd71546436e"
"/subscriptions/c276fc76-9cd4-44c9-99a7-4fd71546436e/resourceGroups"
],
"permissions": [
{
"actions": [
"*"
],
"additionalProperties": {},
"dataActions": [],
"notActions": [
"Microsoft.Authorization/*"
"Microsoft.Resources/*"
"Microsoft.Security/*"
],
"notDataActions": [ ]
}
],

Answer Area



Explanation:

Correct Answer:

"/subscriptions/c276fc76-9cd4-44c9-99a7-4fd71546435e"

"Microsoft.Authorization/"

Question 29

CertyIQ

You have an Azure subscription.
Users access the resources in the subscription from either home or from customer sites. From home, users must establish a point-to-site VPN to access the Azure resources. The users on the customer sites access the Azure resources by using site-to-site VPNs.
You have a line-of-business-app named App1 that runs on several Azure virtual machine. The virtual machines run Windows Server 2016.
You need to ensure that the connections to App1 are spread across all the virtual machines.
What are two possible Azure services that you can use? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

A. an internal load balancer

B. a public load balancer

C. an Azure Content Delivery Network (CDN)

D. Traffic Manager

E. an Azure Application Gateway

Explanation:

Correct Answer: A and E

A: The customer sites are connected through VPNs, so an internal load balancer is enough.

B: The customer sites are connected through VPNs, so there's no need for a public load balancer, an internal load balancer is enough.

C: A CDN does not provide load balancing for applications, so it not relevant for this situation.

D: Traffic manager is a DNS based solution to direct users' requests to the nearest (typically) instance and does not provide load balancing for this situation.

E: Azure Application Gateway is a valid option, as it provides load balancing in addition to routing and security functions

Question 30

CertyIQ

You have an Azure subscription.
You have 100 Azure virtual machines.
You need to quickly identify underutilized virtual machines that can have their service tier changed to a less expensive offering.
Which blade should you use?

A. Monitor

B. Advisor

C. Metrics

D. Customer insights

Explanation:

Correct Answer: B

Advisor helps you optimize and reduce your overall Azure spend by identifying idle and underutilized resources. You can get cost recommendations from the Cost tab on the Advisor dashboard.

Reference:

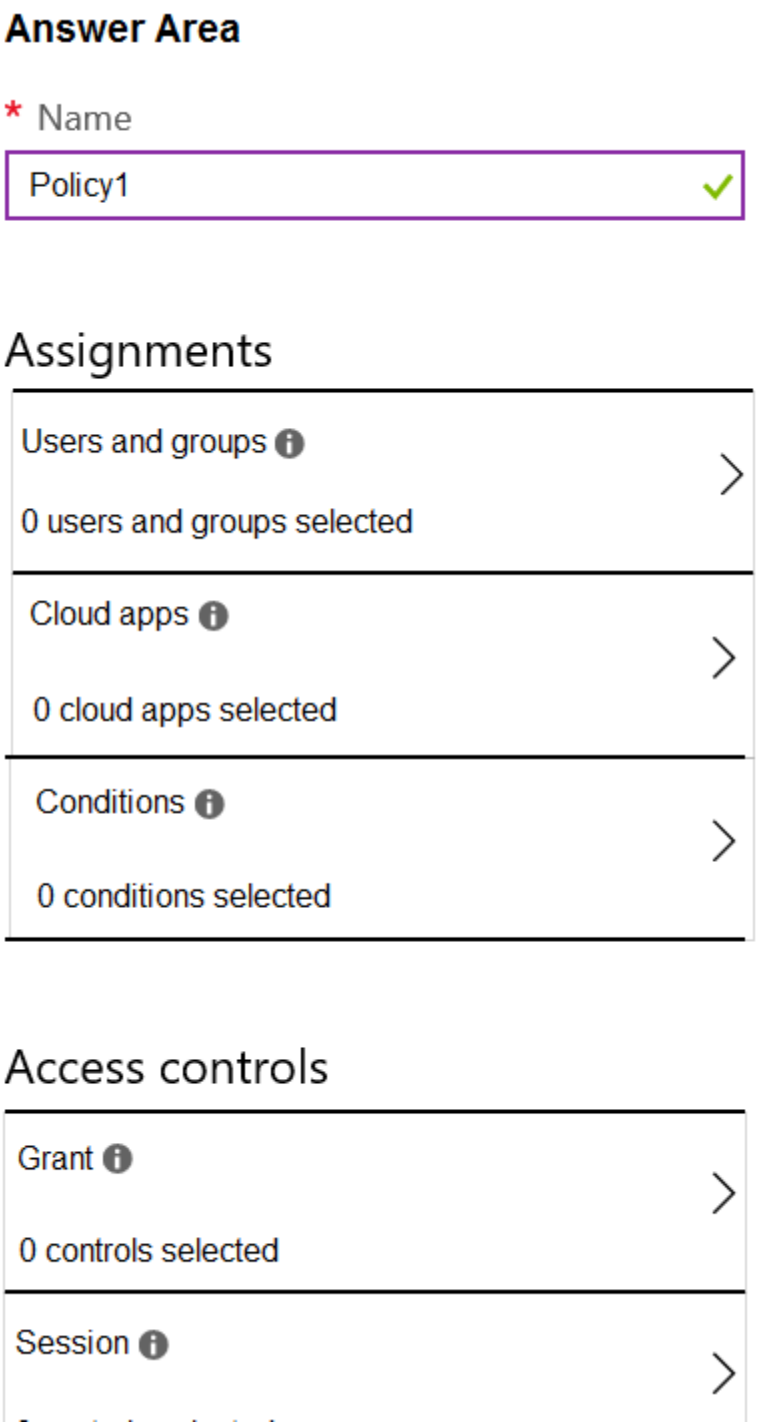
https://docs.microsoft.com/en-us/azure/advisor/advisor-cost-recommendations

Question 31

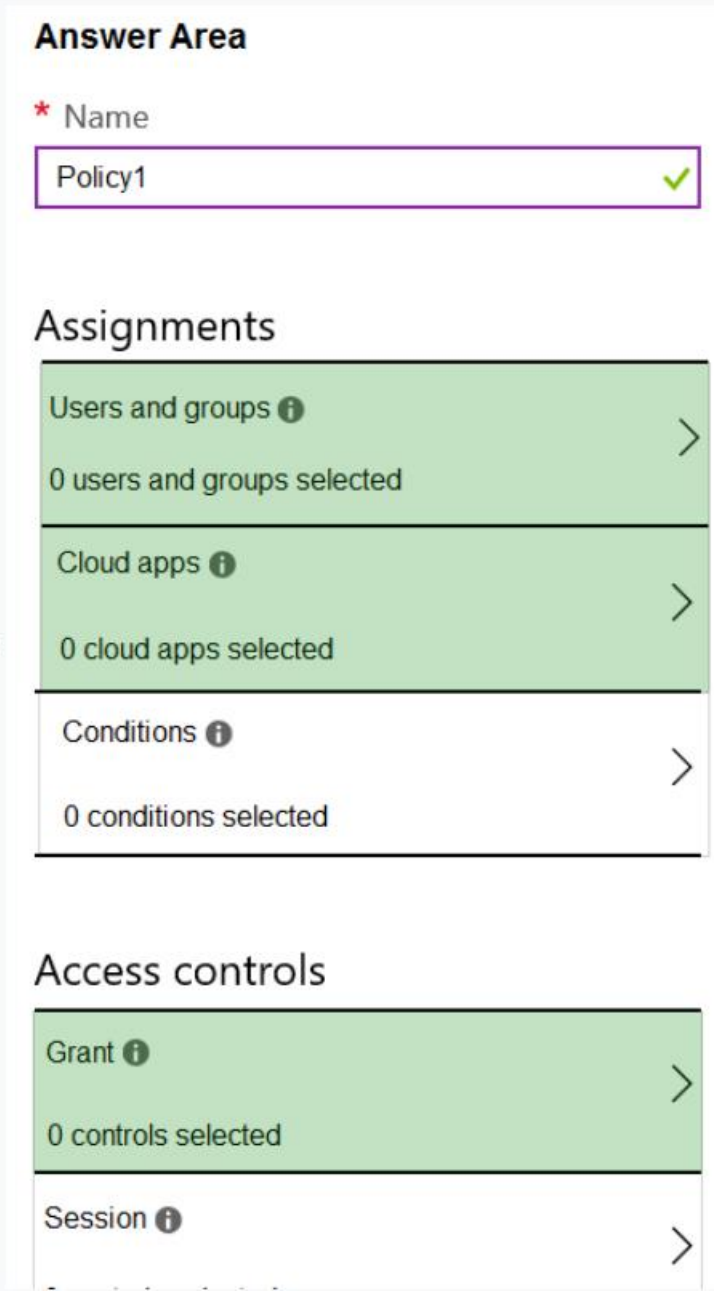
CertyIQ

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



Correct Answer:



Explanation:

- Select Users & Groups : Where you have to choose all users.

- Select Cloud apps or actions: to specify the Azure portal

- Grant: to grant the MFA.

Those are the minimum requirements to create MFA policy. No conditions are required in the question.

Also check this link beside the one provided in the answer

https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-policies

Question 32

CertyIQ

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.

Explanation:

You can adjust the guest user settings, their access, who can invite them from "External collaboration settings"

check this link https://docs.microsoft.com/en-us/azure/active-directory/external-identities/delegate-invitations

Question 33

CertyIQ

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.

Explanation:

Correct Answer: C

No one is given default access to the root management group. Azure AD Global Administrators are the only users that can elevate themselves to gain access. Once they have access to the root management group, the global administrators can assign any Azure role to other users to manage it.

Reference:

https://docs.microsoft.com/en-us/azure/governance/management-groups/overview#important-facts-about-the-root-management-group

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

Question 34

CertyIQ

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

Explanation:

Group 3 is a statically assigned group. Unless the question states "user x has been added to group 3" then they WON'T be in group 3. Group 3 can be removed from the equation for both users.

User 1 - Group 1 ONLY (city starts with M, but their department is excluded for group 2.

User 2 - Group 1 and 2 (city starts with M, no restrictions for group 2)

Question 35

CertyIQ

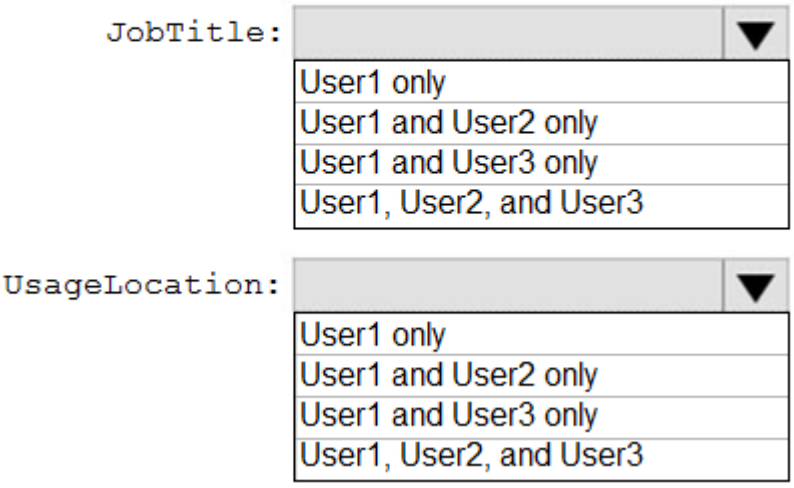
HOTSPOT -
You have a hybrid deployment of Azure Active Directory (Azure AD) that contains the users shown in the following table.

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.

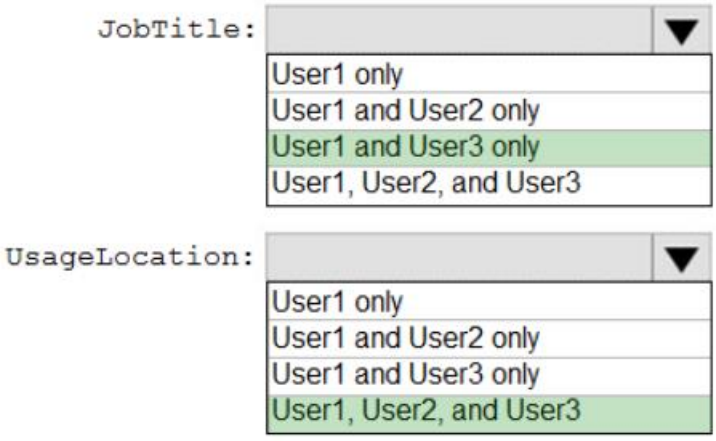
Hot Area:

Answer Area



Correct Answer:

Answer Area



Explanation:

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

Question 36

CertyIQ

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

Explanation:

Correct Answer: A - Yes

Your account must have any one of the following Azure roles at the subscription scope: Owner, Contributor, Reader, or Network Contributor.

Network Contributor role - Lets you manage networks, but not access to them.

Traffic Analytics is a cloud-based solution that provides visibility into user and application activity in cloud networks. Traffic analytics analyzes Network Watcher network security group (NSG) flow logs to provide insights into traffic flow in your Azure cloud.

Reference:

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

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

https://docs.microsoft.com/en-us/azure/network-watcher/traffic-analytics#user-access-requirements

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

Question 37 CertyIQ

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

Explanation:

Correct Answer: A

Your account must have any one of the following Azure roles at the subscription scope: Owner, Contributor, Reader, or Network Contributor.

Network Contributor role - Lets you manage networks, but not access to them.

Traffic Analytics is a cloud-based solution that provides visibility into user and application activity in cloud networks. Traffic analytics analyzes Network Watcher network security group (NSG) flow logs to provide insights into traffic flow in your Azure cloud.

Reference:

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

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

https://docs.microsoft.com/en-us/azure/network-watcher/traffic-analytics#user-access-requirements

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

Question 38

CertyIQ

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

Explanation:

Correct Answer: A - Yes

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

Reader role - View all resources, but does not allow you to make any changes.

Traffic Analytics is a cloud-based solution that provides visibility into user and application activity in cloud networks. Traffic analytics analyzes Network Watcher network security group (NSG) flow logs to provide insights into traffic flow in your Azure cloud.

Reference:

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

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

https://docs.microsoft.com/en-us/azure/network-watcher/traffic-analytics#user-access-requirements

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

Question 39

CertyIQ

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

Explanation:

Correct Answer: C

Only Owner and Contributor can perform the actions, but we need to follow the least privilege principal, so Contributor.

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

B: Virtual Machine Contributor - Create and manage virtual machines, manage disks and disk snapshots, install and run software, reset password of the root user of the virtual machine using VM extensions, and manage local user accounts using VM extensions. This role does not grant you management access to the virtual network or storage account the virtual machines are connected to. This role does not allow you 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, manage assignments in Azure Blueprints, or share image galleries.

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

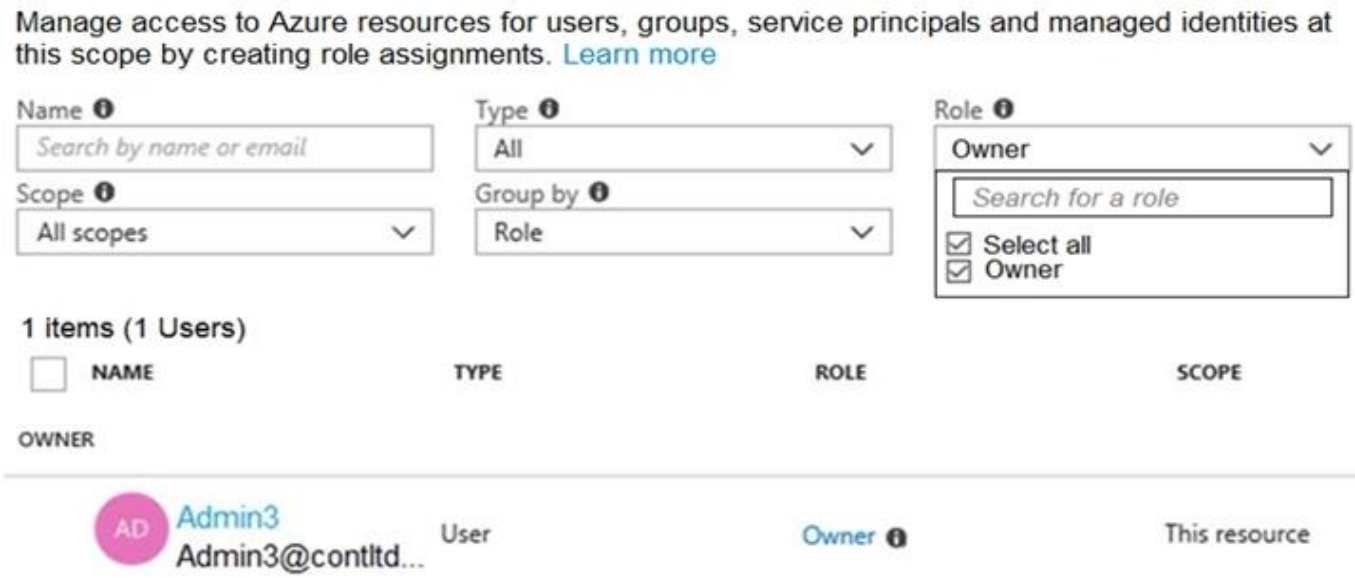
Reference:

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

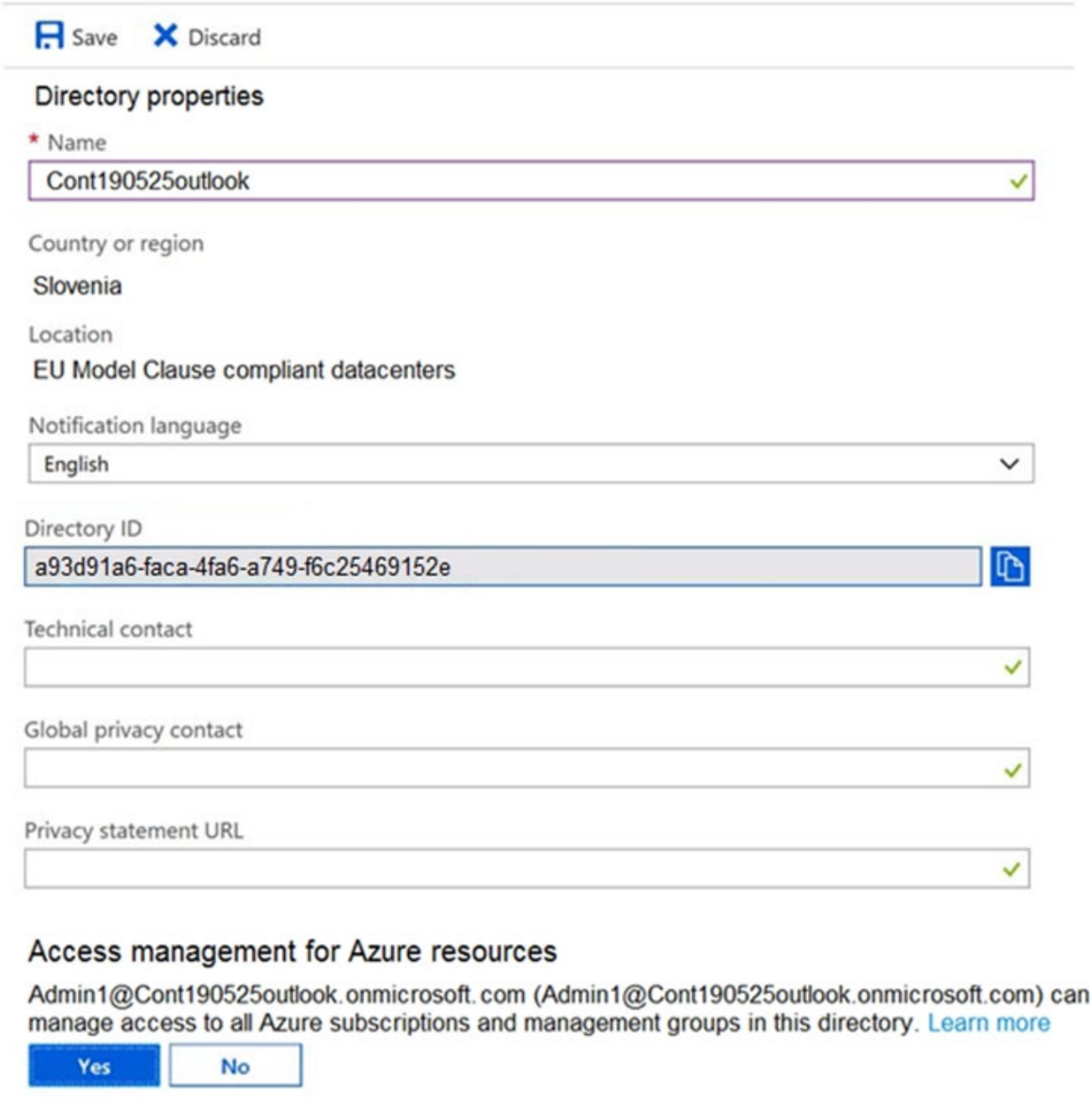
Question 40

CertyIQ

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.)



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



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.	○	○
Admin3 can add Admin 2 as an owner of the subscription.	○	○
Admin2 can create a resource group in the subscription.	○	○

Correct Answer:

Answer Area

Statements	Yes	No
Admin1 can add Admin 2 as an owner of the subscription.	○	○
Admin3 can add Admin 2 as an owner of the subscription.	○	○
Admin2 can create a resource group in the subscription.	○	○

Explanation:

Azure (RBAC) and Azure AD roles are independent. AD roles do not grant access to resources and Azure roles do not grant access to Azure AD. However, a Global Administrator in AD can elevate access to all subscriptions and will be User Access Administrator in Azure root scope.

All 3 users are GA (AD) and Admin3 is owner of the subscription (RBAC).

Admin1 has elevated access, so he is also User Access Admin (RBAC).

To assign a user the owner role at the Subscription scope, you require permissions, such as User Access Admin or Owner.

Box 1: Yes

Admin1 has elevated access, so he is User Access Admin. This is valid.

Box 2: Yes

Admi3 is Owner of the Subscription. This is valid.

Box 3: No

Admin2 is just a GA in Azure AD scope. He doesn't have permission in the Subscription.

Reference:

https://docs.microsoft.com/en-us/azure/role-based-access-control/elevate-access-global-admin

https://docs.microsoft.com/en-us/azure/role-based-access-control/role-assignments-portal-subscription-admin

End of Part 1

Want all 10 PDFs of AZ-104?

Please drop us mail at: - certyiqofficial@gmail.com

Please find the videos of this **AZ-900/AI-900/AZ-305/ AZ-104 /DP-900/ SC-900 and other Microsoft exam** series on

CertyIQ Official YouTube channel (**FREE PDFs**): -

Please Subscribe to CertyIQ YouTube Channel to get notified for latest exam dumps by clicking on the below image, it will redirect to the CertyIQ YouTube page.

Connect with us @ LinkedIn Telegram

Contact us for other dumps: -

contact.certyiqofficial@gmail.com

For any other enquiry, please drop us a mail at

enquiry.certyiqofficial@gmail.com