Microsoft AZ-104 Exam Questions

Total Questions: 530+
Demo Questions: 35
Version: Updated for 2025

Prepared and Verified by Cert Empire – Your Trusted IT Certification Partner

For Access to the full set of Updated Questions – Visit:
AZ-104 Exam Dumps by Cert Empire

Question: 1

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

Answer:

A

Explanation:

To enable Azure AD Premium P2 features for specific users, you must assign the purchased licenses directly to those user accounts or to a group containing those users. The Licenses blade in Azure Active Directory provides the interface for managing and assigning available licenses to individual users or groups.

Why Incorrect Options Are Wrong:

B: Inviting users to a group does not automatically assign licenses; the group itself must have licenses assigned to it (group-based licensing), and then users become licensed by being members. The question implies direct assignment to 10 users.
C: Adding an enterprise application is related to application integration and single sign-on, not to assigning Azure AD Premium feature licenses to users.
D: Modifying directory roles grants administrative permissions within Azure AD; it does not assign licenses for premium features.

References:

Microsoft Entra ID documentation (formerly Azure AD): "Assign licenses to users by group in Microsoft Entra ID" - This document explains group-based licensing but also implicitly covers individual assignment as the foundational concept. The Licenses blade is central to both.
URL: https://learn.microsoft.com/en-us/entra/identity/users/licensing-groups-assign (Refer to sections on assigning licenses)
Microsoft Entra ID documentation: "Assign or remove licenses in the Microsoft Entra admin center"
URL: https://learn.microsoft.com/en-us/entra/identity/users/licensing-assign-licenses (This

page directly describes assigning licenses to users.)

Question: 2

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

Answer:

C

Explanation:

To integrate Azure Monitor alerts with an on-premises System Center Service Manager (SCSM) and ensure alerts are created in SCSM, the IT Service Management Connector (ITSMC) must be deployed first. ITSMC provides a bi-directional connection between Azure monitoring services and supported ITSM tools, including System Center Service Manager. This connector enables Azure alerts to automatically create incidents or events in SCSM.

Why Incorrect Options are Wrong:

A. Create an automation runbook: While a runbook could be part of a custom solution, deploying the ITSMC is the standard and prerequisite step for direct integration with SCSM.
B. Deploy a function app: Similar to runbooks, a function app could be used for custom integration, but ITSMC is the dedicated Azure solution for this scenario and should be established first.
D. Create a notification: Creating a notification is part of an alert rule. However, to send this notification to Service Manager, the ITSM Connector must first be in place to facilitate this specific action type.

References:

Microsoft Learn: "IT Service Management Connector overview" - This document explains that ITSMC connects Azure to ITSM tools like System Center Service Manager to forward alerts. (URL: https://learn.microsoft.com/en-us/azure/azure-monitor/alerts/itsmc-overview)
Microsoft Learn: "Connect Azure to ITSM tools" - This page details the process, starting with adding the ITSM Connector solution. (URL: https://learn.microsoft.com/enus/azure/azure-monitor/alerts/itsmc-connections?tabs=isc)
Specifically, the steps to connect involve adding the "IT Service Management Connector"

solution from the Azure Marketplace. This is the deployment step.
Microsoft Learn: "Create ITSM work items from Azure alerts" - This document outlines how, after setting up ITSMC, you create an ITSM action in an action group to send alerts. (URL: https://learn.microsoft.com/en-us/azure/azure-monitor/alerts/itsmc-definition#create-itsmwork-items-from-azure-alerts) This confirms that ITSMC is a prerequisite.

Question: 3

You sign up for Azure Active Directory (Azure AD) Premium P2. 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

Answer:

A

Explanation:

To add a user as an administrator on all Azure AD joined devices, you configure the "Additional local administrators on all Azure AD joined devices" setting. This setting is located within the Device settings under the Devices blade in the Azure Active Directory portal. This allows specified users or groups to have local administrator privileges on all devices joined to Azure AD.

Why Incorrect Options are Wrong:

B. Providers from the MFA Server blade: This section is for configuring multi-factor authentication providers and settings, not local device administrator rights.
C. User settings from the Users blade: User settings manage general user configurations like self-service password reset or app registrations, not global device administrator assignments.
D. General settings from the Groups blade: Group settings pertain to group creation, naming policies, and expiration, not assigning local administrators to all Azure AD joined devices.

References:

Microsoft Entra ID (formerly Azure AD) Documentation: "How to manage local administrators on Microsoft Entra joined devices" - This document explicitly states: "You can manage this setting from Device settings in the Microsoft Entra admin center." (Microsoft Learn: https://learn.microsoft.com/en-us/entra/identity/devices/assign-local-admin)
Microsoft Entra ID (formerly Azure AD) Documentation: "Configure device settings" - This page details the various settings available under "Device settings," including "Additional local administrators on all Microsoft Entra joined devices." (Microsoft Learn: https://learn.microsoft.com/en-us/entra/identity/devices/manage-device-identities#configuredevice

-settings)

Question: 4

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 and Reader roles for Subscription1.

B. Assign User1 the User Access Administrator role for VNet1.

C. Assign User1 the Network Contributor role for VNet1.

D. Assign User1 the Network Contributor role for RG1.

Answer:

B

Explanation:

To allow User1 to assign the Reader role for VNet1 to other users, User1 needs the Microsoft.Authorization/roleAssignments/write permission for VNet1. The User Access Administrator role grants this permission. Assigning this role at the VNet1 scope ensures User1 has the necessary permissions specifically for VNet1, adhering to the principle of least privilege. The existing roles (Reader, Security Admin, Security Reader) do not grant permissions to assign roles to other users.

Why Incorrect Options are Wrong:

A. Remove User1 from the Security Reader and Reader roles for Subscription1. Removing roles reduces permissions and does not grant the ability to assign roles.
C. Assign User1 the Network Contributor role for VNet1. The Network Contributor role allows management of network resources but does not grant permissions to assign roles.
D. Assign User1 the Network Contributor role for RG1. Similar to option C, Network Contributor does not grant role assignment permissions, regardless of the scope.

References:

Microsoft Learn. (2024). Azure built-in roles. "User Access Administrator" section. Retrieved from https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#useraccess-administrator
Microsoft Learn. (2024). Azure built-in roles. "Security Admin" section. Retrieved from https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#securityadmin
Microsoft Learn. (2024). Azure built-in roles. "Network Contributor" section. Retrieved from https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#networkcontributor

Microsoft Learn. (2024). Understand Azure role definitions. "Permissions" section. Retrieved from https://learn.microsoft.com/en-us/azure/role-based-access-control/roledefinitions#permissions (Illustrates the Microsoft.Authorization/roleAssignments/write permission).

Question: 5

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

Answer:

A

Explanation:

To verify a custom domain name in Azure Active Directory (Azure AD), you must add a specific DNS record to your public DNS zone. Azure AD provides the details for either an MX (Mail Exchange) or a TXT (Text) record. Creating one of these records proves to Azure AD that you own the domain. Since MX is listed as an option and is a valid method, it is the correct choice.

Why Incorrect Options are Wrong:

B. NSEC: NSEC records are part of DNSSEC (DNS Security Extensions) and are used to prove the non-existence of a domain name, not for domain ownership verification in Azure AD.
C. PTR: PTR (Pointer) records are used for reverse DNS lookups (mapping an IP address to a domain name), not for verifying domain ownership for Azure AD.
D. RRSIG: RRSIG (Resource Record Signature) records are also part of DNSSEC, providing digital signatures for DNS records to ensure their authenticity, not for initial domain ownership verification.

References:

Microsoft Entra ID Documentation (formerly Azure Active Directory): "Add your custom domain name to Azure Active Directory." Microsoft Learn. (Specifically, the section on verifying the domain name).
Direct URL: https://learn.microsoft.com/en-us/entra/fundamentals/add-customdomain#verify-your-custom-domain-name
Relevant text: "After you add your custom domain name to Azure AD, you must return to your domain registrar and add the DNS information Azure AD gave you. Adding this DNS

information verifies your ownership of the domain name. The DNS information can be an MX or a TXT record."

Question: 6

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

Answer:

No

Explanation:

The "DevTest Labs User" role grants permissions specific to managing virtual machines and environments within Azure DevTest Labs. It does not include the Microsoft.Logic/workflows/write permission, which is essential for creating Azure Logic Apps. To enable the Developers group to create Logic Apps in the Dev resource group, a role such as "Logic App Contributor" or "Contributor" should be assigned, scoped to either the "Dev" resource group or "Subscription1".

References:

1. Azure built-in roles - DevTest Labs User: Microsoft Learn. Describes the "DevTest Labs User" role and its limited permissions, which do not include creating Logic Apps.
URL: https://learn.microsoft.com/en-us/azure/role-based-access-control/built-inroles#devtest-labs-user
2. Azure built-in roles - Logic App Contributor: Microsoft Learn. Details the "Logic App Contributor" role, which includes permissions like Microsoft.Logic/ necessary for managing Logic Apps.
URL: https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#logicapp-contributor
3. Azure built-in roles - Contributor: Microsoft Learn. Describes the "Contributor" role, which grants broad permissions to create and manage all types of Azure resources, including Logic Apps.
URL: https://learn.microsoft.com/en-us/azure/role-based-access-control/built-inroles#contributor
4. Resource provider operations - Microsoft.Logic: Microsoft Learn. Lists operations for the Microsoft.Logic resource provider, including Microsoft.Logic/workflows/write which is required to create Logic Apps.
URL: https://learn.microsoft.com/en-us/azure/role-based-access-control/resource-provideroperati

ons#microsoftlogic

Question: 7

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

Answer:

B (No)

Explanation:

The "Logic App Operator" role allows users to read, enable, and disable logic apps. However, it does not grant permissions to create, delete, or modify them. To create Azure Logic Apps, the "Logic App Contributor" role or a more general role like "Contributor" is required. Assigning "Logic App Operator" at the subscription level to the Developers group will not provide them with the necessary permissions to create logic apps in the Dev resource group.

References:

Microsoft Learn. (2024). Azure built-in roles - Azure RBAC. "Logic App Operator: Lets you read, enable, and disable logic apps. Does not let you edit or update them." Retrieved from https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#logic-appoperator
Microsoft Learn. (2024). Azure built-in roles - Azure RBAC. "Logic App Contributor: Lets you manage logic apps, but not access to them." (Managing includes creation). Retrieved from https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#logic-appcontributor
Microsoft Learn. (2024). Resource provider operations. The Microsoft.Logic/workflows/write operation is required for creating Logic Apps. Retrieved from https://learn.microsoft.com/enus/azure/role-based-access-control/resource-provider-operations#microsoftlogic

Question: 8

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

Answer:

Yes

Explanation:

The Contributor role in Azure grants full access to manage all resources within the assigned scope, including creating, updating, and deleting them. Assigning the Contributor role to the "Developers" group on the "Dev" resource group provides the necessary permissions (e.g., Microsoft.Logic/workflows/write) for members of this group to create Azure Logic Apps within that specific resource group.

References:

1. Azure built-in roles - Contributor: Microsoft Learn. "The Contributor role 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."
URL: https://learn.microsoft.com/en-us/azure/role-based-access-control/built-inroles#contributor
2. Resource provider operations - Microsoft.Logic: Microsoft Learn. The Microsoft.Logic/workflows/write operation, which is included in the Contributor role's wildcard permissions (/write), allows for the creation of Logic Apps.
URL: https://learn.microsoft.com/en-us/azure/role-based-access-control/resource-provideroperations#microsoftlogic
3. Understand scope for Azure RBAC: Microsoft Learn. Assigning a role at a resource group scope grants permissions only within that resource group.
URL: https://learn.microsoft.com/en-us/azure/role-based-access-control/scope-overview

Question: 9

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.

Hot Area:

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

Answer:

Statement 1: User1 can add Device2 to Group1.

Answer: No

Statement 2: User2 can add Device1 to Group1.

Answer: Yes
Statement 3: User2 can add Device2 to Group2.
Answer: No

Explanation:

Statement 1 is No. User1 has the Cloud Device Administrator role, which grants permissions to manage device objects but does not grant permissions to manage group memberships. Group membership for an "Assigned" group can only be modified by the group's owner (User2) or administrators with specific group management privileges (like User Administrator or Global Administrator).
Statement 2 is Yes. User2 is the designated owner of Group1. The owner of a group with "Assigned" membership has the explicit right to add or remove members. Therefore, User2 can add any device, including Device1, to Group1.
Statement 3 is No. Group2 has a "Dynamic Device" membership type. Membership in dynamic groups is not managed manually but is determined automatically based on a membership rule. It is not possible for any user, including the owner (User2) or even a Global Administrator, to manually add or remove members from a dynamic group.

References:

Microsoft Entra ID (formerly Azure AD) built-in roles:

Cloud Device Administrator: "Users with this role can enable, disable, and delete devices in Microsoft Entra ID and manage Windows 10 BitLocker keys... This role does not grant permissions to manage any other properties on the device."
o Source: Microsoft Learn, "Microsoft Entra built-in roles," Section: "Cloud Device Administrator."

User Administrator: "Users with this role can... create and manage all aspects of users and groups..."
o Source: Microsoft Learn, "Microsoft Entra built-in roles," Section: "User Administrator."

Group Ownership and Management:
o "The owner of the group can be a user or a service principal and can manage the group (for example, change the name or manage membership)."
Section
Source: Microsoft Learn, "Manage group membership for

Microsoft Entra groups."

Dynamic Group Membership:
o "You can't manually add or remove a member from a dynamic group. Microsoft Entra ID automatically adds or removes members based on the rule."
Section
Source: Microsoft Learn, "Create or update a dynamic group in Microsoft Entra ID."

Question: 10

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	SQL server in Azure VM	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

Answer:

C

Explanation:

The deletion of resource group RG26 is failing, likely because SQLDB01 cannot be deleted due to its backup configuration. SQLDB01 is backed up to RGV1, implying it's protected by Azure Backup (e.g., via a Recovery Services vault). Such protection creates a dependency that prevents the deletion of the protected resource and, consequently, its containing resource group. The first step to resolve this is to stop the backup for SQLDB01, which typically involves stopping protection and deleting backup data. This removes the dependency, allowing SQLDB01 to be deleted, and subsequently RG26.

Why Incorrect Options are Wrong:

A. Delete VM1: While necessary for RG deletion, it's not the first step if the SQL DB backup is the primary blocker for the RG deletion failure.
B. Stop VM1: Stopping a VM is insufficient; the VM must be deleted. This also doesn't address the likely backup-related blocker.
D. Delete sa001: Similar to deleting VM1, this is a necessary step but not the first one if the

SQL DB backup is causing the RG deletion to fail.

References:

1. Azure Backup - Delete a Recovery Services vault: "You can't delete a Recovery Services vault if it's registered to a server and contains backup data. If you try to delete a vault that contains dependencies, you'll receive an error... To delete backup items in the cloud... For Azure SQL Database... Right-click the backup item - Stop backup. Then select Delete Backup Data."
URL: https://docs.microsoft.com/en-us/azure/backup/backup-azure-deletevault?tabs=portal#delete-protected-items-in-the-cloud (The specific section details stopping backup for protected items like SQL databases).
2. Azure Resource Manager resource group and resource deletion: "Resource Manager only deletes the resource group when all resources have been deleted... If a resource depends on a resource in a different resource group, Resource Manager can't determine the correct order. You'll receive an error indicating that you must delete the dependent resource."
URL: https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/deleteresource-group?tabs=azure-portal#how-resources-are-deleted
3. Troubleshoot issues when you delete Azure resources: This document often lists common reasons for deletion failures, including locks and dependencies from services like Azure Backup.
URL: https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/deletecommon-errors (While a general troubleshooting guide, it reinforces the concept of dependencies blocking deletion).

Question: 11

You have an Azure subscription named Subscription1 that contains an Azure Log Analytics workspace named Workspace1. You need to view the error events 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. search in (Event) * where EventType -eq "error"

Answer:

B

Explanation:

Azure Monitor and Log Analytics use the Kusto Query Language (KQL).
To examine only rows in the Event table that contain the term error, the supported syntax is: search in (Event) "error"
The search operator scopes the free-text search to the specified table list in this case, the single table Event returning every record whose any column includes the string error. This satisfies the requirement to view the error events from a table named Event, and the syntax exactly matches what Microsoft KQL documentation prescribes.

Why Incorrect Options are Wrong:

A. PowerShell cmdlet, not KQL; cannot run inside Log Analytics workspace.
C. KQL uses project/project-away, not SQL SELECT; statement is invalid.
D. Combines a useless wildcard with an invalid comparison operator (-eq). KQL equality is ==.

References:

1. Microsoft Docs search operator (Kusto Query Language): Example syntax search in (Event) "Error"
https://learn.microsoft.com/azure/data-explorer/kusto/query/searchoperator
2. Microsoft Docs Kusto query language quick reference: Equality operator is ==, not -eq.
https://learn.microsoft.com/azure/data-explorer/kusto/query/quick-reference

Question: 12

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 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:

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:

Statement 1: A network security group (NSG) named NSG1 will be created.
Correct Answer: No
Explanation: The ARM template defines a resource of type Microsoft.Network/networkSecurityGroups/securityRules. The name NSG1/AllowWeb specifies that a security rule named AllowWeb is to be created or updated within an existing Network Security Group (NSG) named NSG1. The template does not contain a resource definition for creating the NSG NSG1 itself; it assumes NSG1 already exists.

References:

Microsoft Learn. (2023). Microsoft.Network/networkSecurityGroups/securityRules. Retrieved from https://learn.microsoft.com/enus/azure/templates/microsoft.network/networksecuritygroups/securityrules?pivots=deployment-language-arm-template (This page shows the structure for defining security rules, where the name format is /, indicating the rule is a child resource of an NSG).
Microsoft Learn. (2023). Quickstart: Create a network security group using an ARM template. Retrieved from https://learn.microsoft.com/en-us/azure/virtual-network/templatedeploy-nsg (This shows that creating an NSG requires a resource of type Microsoft.Network/networkSecurityGroups).
Statement 2: The AllowWeb inbound security rule will be created.
Correct Answer: Yes
Explanation: The ARM template's primary purpose is to deploy the resource defined within it. The resource is of type Microsoft.Network/networkSecurityGroups/securityRules with the name component AllowWeb. The properties specify "direction": "Inbound", "access": "Allow", and other parameters for an inbound security rule. Successful deployment of this template means this rule will be created (or updated if it already exists) in the NSG named

NSG1.
References:
Microsoft Learn. (2023). Microsoft.Network/networkSecurityGroups/securityRules. Retrieved from https://learn.microsoft.com/enus/azure/templates/microsoft.network/networksecuritygroups/securityrules?pivots=deploym
ent-language-arm-template (The template directly matches the schema for creating a security rule).
Microsoft Learn. (2024). Understand the structure and syntax of ARM templates. Retrieved from https://learn.microsoft.com/en-us/azure/azure-resourcemanager/templates/syntax#resources (The resources section defines the Azure resources
to deploy).
Statement 3: VM1-NI will allow inbound connections on TCP port 80 from the internet.
Correct Answer: No
Explanation: The ARM template creates the AllowWeb security rule within an NSG named NSG1. This rule is configured to allow inbound TCP port 80 from the internet. However, for this rule to affect VM1-NI, the NSG NSG1 must be associated with either the network interface VM1-NI itself or the subnet to which VM1-NI is connected. The problem states the template is successfully deployed but does not provide information that NSG1 is associated with VM1-NI or its subnet. The template deployment alone does not establish this association.

References:
Microsoft Learn. (2024). Network security groups. Retrieved from https://learn.microsoft.com/en-us/azure/virtual-network/network-security-groupsoverview#how-network-security-groups-filter-network-traffic (This document explains that
"To filter network traffic to or from a resource, you need to associate a network security group to the network interface or subnet that the resource is in.").
Microsoft Learn. (2024). Associate or dissociate a network security group. Retrieved from https://learn.microsoft.com/en-us/azure/virtual-network/manage-network-securitygroup?tabs=network-security-group-portal#associate-or-dissociate-a-network-security-
group (This details the separate step of associating an NSG with a NIC or subnet).
References:

Question: 13

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.

Answer:

A

Explanation:

When an Azure resource like a Web App is moved to a new resource group, its physical location (region) does not change. WebApp1 is located in West Europe, meaning its App Service plan is also in West Europe. Moving WebApp1 to RG2 will not change the App Service plan's region; it will remain in West Europe.
Azure Policy assignments are scoped. When WebApp1 is moved from RG1 to RG2, it will no longer be subject to policies scoped directly to RG1 (Policy1) but will become subject to policies scoped to RG2 (Policy2).

Why Incorrect Options are Wrong:

B: The App Service plan's location (region) does not change when its managing resource group changes; it remains in West Europe, not North Europe.
C: After moving to RG2, WebApp1 will be subject to Policy2 (assigned to RG2), not Policy1 (assigned to RG1).
D: Both the App Service plan's location change and the policy application are incorrect for

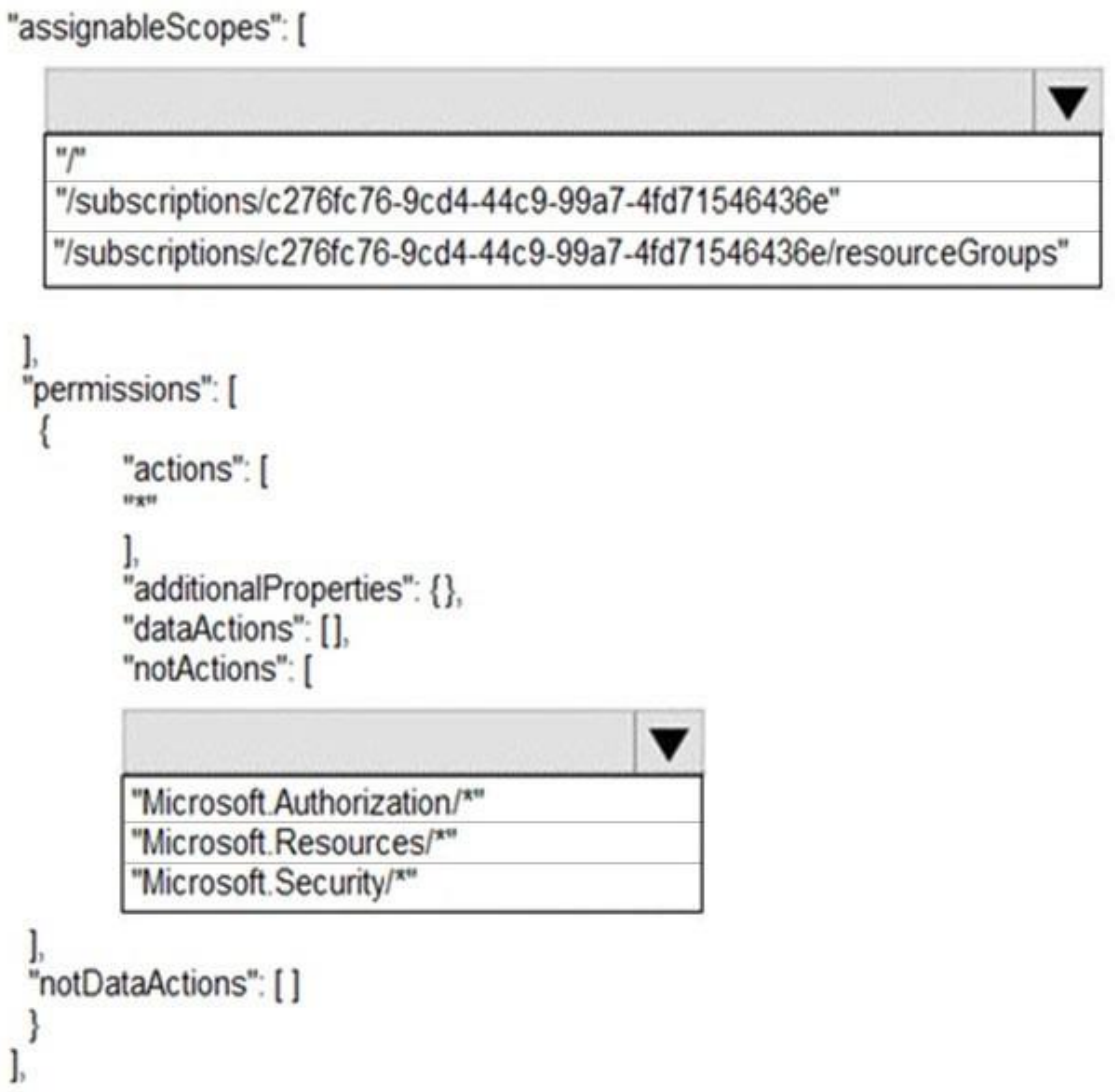
the reasons stated above.

References:

1. Move resources to a new resource group or subscription - Azure Resource Manager Microsoft Learn:
"When you move a resource, it only moves to a new resource group or subscription. It doesn't change the location of the resource."
Direct URL: https://learn.microsoft.com/en-us/azure/azure-resourcemanager/management/move-resource-group-and-subscription (Refer to the section "Checklist before moving resources" or similar introductory paragraphs about resource location).
2. Overview of Azure App Service plans - Azure App Service Microsoft Learn:
"When you create an App Service plan in a certain region (for example, West Europe), a set of compute resources is created for that plan in that region. Whatever apps you put into this App Service plan run on these compute resources as defined by your App Service plan."
This indicates the plan's location is fixed at creation.
Direct URL: https://learn.microsoft.com/en-us/azure/app-service/overview-hosting-plans (Refer to the section "How does an App Service plan work?").
3. Overview of Azure Policy - Azure Policy Microsoft Learn:
"A policy assignment is a policy definition that has been assigned to take place within a specific scope. This scope could range from a management group to a resource group."
When a resource moves to a new resource group, it falls under the policy assignments of that new scope.
Direct URL: https://learn.microsoft.com/en-us/azure/governance/policy/overview (Refer to the section "Policy assignment").

Question: 14

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:

AssignableScopes: /subscriptions/c276fc76-9cd4-44c9-99a7-4fd71546436e Actions: NotActions: Microsoft.Authorization/

Explanation:

For the custom RBAC role CR1:

1. AssignableScopes: To ensure the role "Can be assigned only to the resource groups in Subscription1", the AssignableScopes for the role definition should be set to the subscription ID: /subscriptions/c276fc76-9cd4-44c9-99a7-4fd71546436e. This makes the role definition available for assignment at this subscription scope or any resource group within it. The actual role assignment would then be made to a resource group.
2. Permissions:

To "Allow the viewing, creating, modifying, and deleting of resources within the resource groups", the Actions property should be set to . This grants all permissions by default.

To "Prevent the management of the access permissions for the resource groups", the NotActions property should include Microsoft.Authorization/. This explicitly denies permissions to manage role assignments, role definitions, and other access control settings.

This configuration allows full control over resources within the assigned scope (resource groups in Subscription1) but explicitly denies the ability to manage RBAC permissions.

References:

1. Azure custom roles - AssignableScopes:

Microsoft Learn: "Understand Azure role definitions - AssignableScopes"

URL:

https://learn.microsoft.com/en-us/azure/role-based-access-control/customroles#assignablescopes

Specific section: The assignableScopes property of a role specifies the scopes (subscriptions, resource groups, or resources) within which the role is available for assignment. You can make the custom role available for assignment in only the subscriptions or resource groups that require it.

2. Azure custom roles - Permissions (Actions and NotActions):

Microsoft Learn: "Understand Azure role definitions - Permissions"

URL: https://learn.microsoft.com/en-us/azure/role-based-access-control/customroles#permissions

Specific section: The permissions property of a role specifies the operations that the role allows or denies. Permissions are defined with Actions (allowed operations) and NotActions (denied operations). Actions = "" grants all actions. NotActions = "Microsoft.Authorization/" denies all actions under Microsoft.Authorization.

3. Tutorial: Create an Azure custom role using Azure PowerShell - Step 4: Define permissions:

Microsoft Learn: "Tutorial: Create an Azure custom role using Azure PowerShell - Example role definition"

URL: https://learn.microsoft.com/en-us/azure/role-based-access-control/tutorial-customrole-powershell#step-4-define-permissions

Specific section: Shows examples where Actions: "" is used with NotActions to exclude

specific permissions like Microsoft.Authorization//Delete. The principle is the same: grant broadly with in Actions, then restrict with NotActions.

Question: 15

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

Answer:

A, E

Explanation:

To spread connections across multiple Azure virtual machines for an application (App1) accessed via VPNs (Point-to-Site and Site-to-Site), both an Azure Internal Load Balancer and an Azure Application Gateway (configured with a private frontend IP) are suitable solutions.
An Azure Internal Load Balancer (Option A) operates at Layer 4 (TCP/UDP) and distributes network traffic to VMs within a virtual network using a private IP address. This is ideal for distributing traffic from VPN-connected users to backend VMs.
An Azure Application Gateway (Option E), when configured with a private frontend IP address, acts as an internal Layer 7 load balancer for HTTP/S traffic. It can distribute web traffic to backend VMs and offers features like SSL termination and URL-based routing.
These services ensure that connections are distributed across the VMs hosting App1 within the private network.

References:

Azure Load Balancer (Internal):
Microsoft Learn: "What is Azure Load Balancer?" - "Azure Load Balancer operates at layer 4 of the Open Systems Interconnection (OSI) model... An internal (or private) load balancer is used only for private IP addresses at the front end."
URL: https://learn.microsoft.com/en-us/azure/load-balancer/load-balancer-overview
Microsoft Learn: "Quickstart: Create an internal load balancer - Azure portal" - "An Azure internal load balancer distributes network traffic to resources that are inside a virtual network."
URL: https://learn.microsoft.com/en-us/azure/load-balancer/quickstart-load-balancerinternal-portal
Azure Application Gateway (Internal):
Microsoft Learn: "What is Azure Application Gateway?" - "Azure Application Gateway is a web traffic load balancer that enables you to manage traffic to your web applications... Application Gateway can be configured with a private IP address, a public IP address, or both."
URL: https://learn.microsoft.com/en-us/azure/application-gateway/overview
Microsoft Learn: "Create an application gateway with an internal load balancer (ILB)" - This documentation explicitly describes using Application Gateway for internal load balancing scenarios.
URL: https://learn.microsoft.com/en-us/azure/application-gateway/application-gateway-ilbarm

(Conceptual link, specific steps may vary) or related sections in the overview.
Traffic Manager (for differentiation):
Microsoft Learn: "What is Traffic Manager?" - "Azure Traffic Manager is a DNS-based traffic load balancer. This service allows you to distribute traffic to your public facing applications across the global Azure regions."
URL: https://learn.microsoft.com/en-us/azure/traffic-manager/traffic-manager-overview

Question: 16

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

Answer:

B

Explanation:

Azure Advisor provides personalized recommendations to optimize Azure resources. One of its key recommendation categories is "Cost," which includes identifying underutilized virtual machines and suggesting changes like resizing or shutting them down to save money. This directly addresses the need to quickly identify VMs for less expensive offerings.

Why Incorrect Options are Wrong:

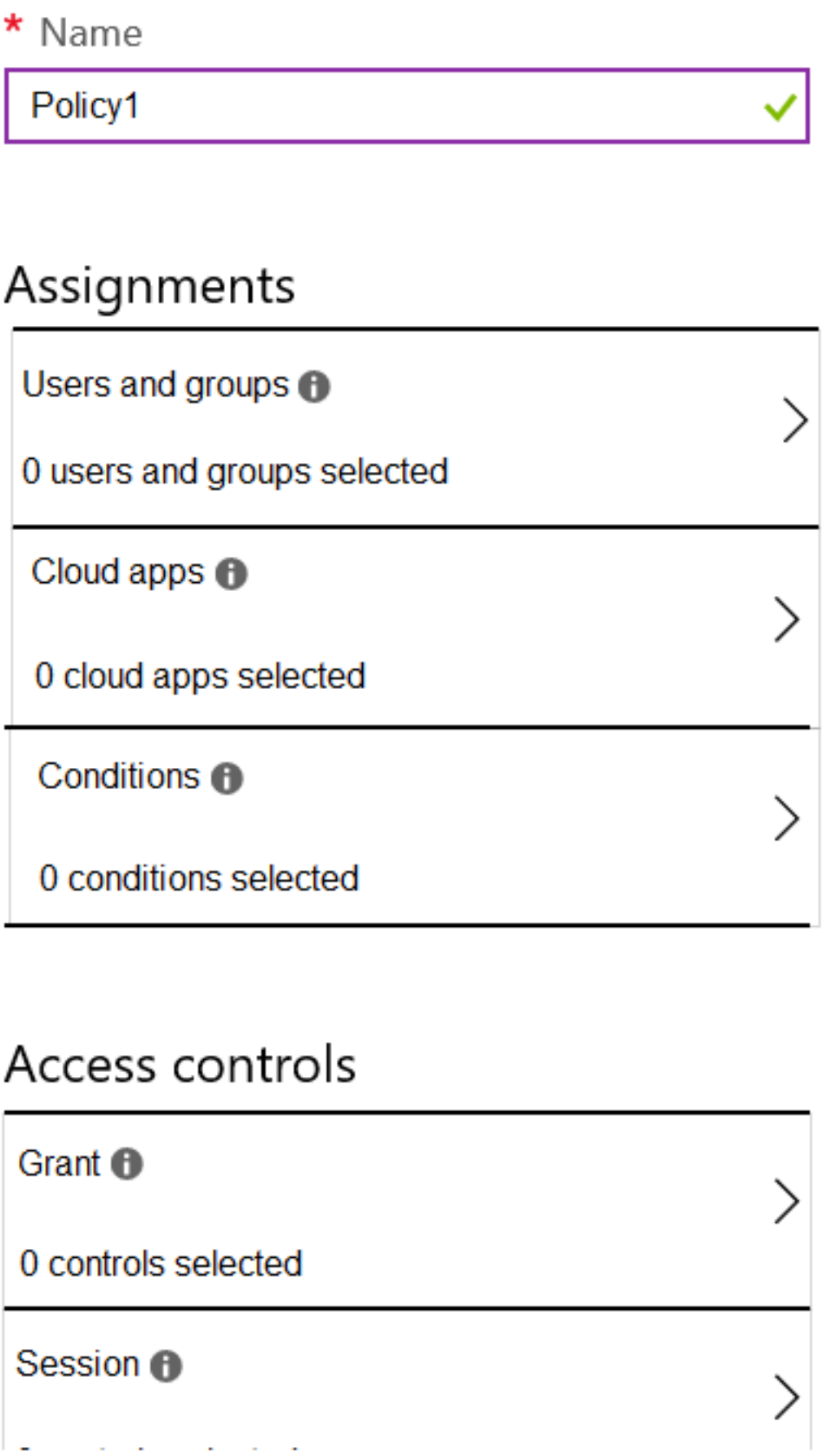
A. Monitor: Azure Monitor collects and analyzes telemetry data, including VM performance, but it doesn't proactively provide cost optimization recommendations for service tiers in the same direct way Advisor does.
C. Metrics: Metrics are raw performance data points (e.g., CPU, memory usage) available within Azure Monitor. While useful for analysis, they don't offer direct, consolidated recommendations for cost optimization.
D. Customer insights: Azure Customer Insights is a customer data platform (CDP) and is unrelated to Azure infrastructure optimization or virtual machine cost management.

References:

Microsoft Azure. (n.d.). Introduction to Azure Advisor. Microsoft Learn. Retrieved from https://learn.microsoft.com/en-us/azure/advisor/advisor-overview (Focus on "Cost optimization" section)
Microsoft Azure. (n.d.). Optimize costs with Azure Advisor. Microsoft Learn. Retrieved from https://learn.microsoft.com/en-us/azure/advisor/advisor-cost-recommendations (Specifically mentions "Optimize virtual machine (VM) or virtual machine scale set (VMSS) spend by resizing or shutting down underutilized instances")

Question: 17

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:


* 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:

1. Users and groups 2. Cloud apps or actions 3. Grant

Explanation:

To create a Conditional Access policy that requires all users to use multi-factor authentication (MFA) when accessing the Azure portal, you must configure three primary settings:

1. Users and groups: This setting defines the scope of users the policy will apply to. For this requirement, it should be configured to "All users."
2. Cloud apps or actions: This setting specifies the target cloud application. For the Azure portal, you select "Microsoft Azure Management."
3. Grant: This setting defines the access controls to be enforced. To require MFA, you configure this to "Grant access" and select "Require multi-factor authentication."

These three settings collectively define who the policy applies to, what resource it protects, and what conditions must be met for access.

References:

Microsoft Learn: "Conditional Access: Users and groups." (Specifies how to assign the policy to users, including "All users").
URL: https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/conceptconditional-access-users-groups

Microsoft Learn: "Conditional Access: Cloud apps or actions." (States that "Microsoft Azure Management" includes the Azure portal (portal.azure.com)).
URL: https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/conceptconditional-access-cloud-apps
Microsoft Learn: "Conditional Access: Grant." (Details the grant controls, including "Require multi-factor authentication").
URL: https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/conceptconditional-access-grant
Microsoft Learn: "Tutorial: Secure user sign-in events with Azure AD Multi-Factor Authentication." (Provides a step-by-step guide that involves configuring these three settings for MFA).
URL:
https://learn.microsoft.com/en-us/azure/active-directory/authentication/tutorial-enableazure-mfa
(This tutorial often leads to creating a Conditional Access policy which would use these settings). A more direct CA policy creation example: https://learn.microsoft.com/enus/azure/active-directory/conditional-access/howto-conditional-access-policy-all-users-mfa

Question: 18

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 settings 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.

Answer:

A

Explanation:

The "Generic authorization exception" error, when an administrator like Admin1 (with the User administrator role) attempts to invite an external user, typically indicates that the organization-wide external collaboration settings are configured to restrict guest invitations. The User administrator role inherently includes permissions to invite guest users. However, these permissions can be overridden by more restrictive settings in the "External collaboration settings" blade. Modifying these settings to allow invitations by administrators or members is the direct way to resolve this issue.

Why Incorrect Options are Wrong:

B. From the Custom domain names blade, add a custom domain. Adding a custom domain is for branding and using your organization's domain for user sign-ins; it does not affect the ability to invite external users with existing Microsoft accounts like outlook.com.
C. From the Organizational relationships blade, add an identity provider. Adding an identity provider is for setting up federation with other identity systems (e.g., SAML/WS-Fed IdPs, other Azure AD tenants, social IdPs). Microsoft accounts (outlook.com) are natively supported for B2B collaboration and do not require adding a specific identity provider in this context.
D. From the Roles and administrators blade, assign the Security administrator role to Admin1. The User administrator role already has the necessary permissions to invite guest users. The issue is likely a restrictive policy, not a lack of role-based permissions for

Admin1. Escalating privileges is not the correct first step.

References:

Microsoft Entra ID (formerly Azure AD) Documentation: "Delegate guest inviter role" - This page discusses the Guest Inviter role, but the broader context is within External collaboration settings. The User Administrator role has more privileges.
Reference: Microsoft Learn. (2023). Delegate invitations for Microsoft Entra B2B collaboration. "By default, Global Administrator role can invite guests. The User Administrator role can also invite guests." Available at: https://learn.microsoft.com/enus/entra/external-id/delegate-invitations
Microsoft Entra ID Documentation: "Configure external collaboration settings" - This page details the settings that control guest invitations.
Reference: Microsoft Learn. (2023). Configure external collaboration settings. "External collaboration settings let you specify what roles in your organization can invite external users for B2B collaboration." Available at: https://learn.microsoft.com/en-us/entra/externalid/external-collaboration-settings-configure (Specifically, the "Guest invite settings" section).
Microsoft Entra ID Documentation: "User administrator" role.
Reference: Microsoft Learn. (2023). Microsoft Entra built-in roles - User Administrator. "Users with this role can... invite guest users." Available at: https://learn.microsoft.com/enus/entra/identity/role-based-access-control/permissions-reference#user-administrator

Question: 19

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.

Answer:

C

Explanation:

To assign policies at the tenant root management group, User1 needs a role like "Resource Policy Contributor" or "Owner" at that scope. Assigning User1 the "Global Administrator" role allows User1 to then elevate their access to manage all Azure subscriptions and management groups. This elevation grants User1 the "User Access Administrator" role at the root scope. User1 can then use this role to assign themselves the necessary "Resource Policy Contributor" or "Owner" role at the tenant root management group, enabling them to assign policies.

Why Incorrect Options are Wrong:

A: Assigning "Owner" at the subscription level does not grant permissions at the tenant root management group. Conditional access policies are for user access control, not Azure resource policy assignment.
B: Assigning "Owner" at the subscription level is insufficient for managing the tenant root management group. The instruction is too vague without the initial elevation step.
D: Creating a new management group and making User1 its owner does not grant permissions to the tenant root management group.

References:

Microsoft Learn. (2023). Elevate access to manage all Azure subscriptions and management groups. "As a Global Administrator in Azure Active Directory (Azure AD), you might not have access to all subscriptions and management groups in your directory. However, you can elevate your access to get access to all subscriptions and management groups... When you elevate your access, you will be assigned the User Access Administrator role in Azure at the root scope (/). This allows you to view all resources and assign access in any subscription or management group in the directory."
URL: https://learn.microsoft.com/en-us/azure/role-based-access-control/elevate-accessglobal-admin

Microsoft Learn. (2023). Azure built-in roles - Resource Policy Contributor. "Lets you manage policy assignments, but not access to them." Includes Microsoft.Authorization/policyAssignments/write.
URL: https://learn.microsoft.com/en-us/azure/role-based-access-control/built-inroles#resource-policy-contributor

Microsoft Learn. (2023). What are Azure management groups? "The root management group contains all subscriptions and management groups... All users in the Azure AD tenant can view the hierarchy, but to manage resources, they need Azure role assignments."
URL: https://learn.microsoft.com/en-us/azure/governance/management-groups/overview (Section: Root management group for each directory)

Question: 20

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 365	Dynamic user	(user.department -notIn ["human resources"])
Group3	Microsoft 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

Of which groups are User1 and User2 members? To answer, select the appropriate options in the [illegible]t. Hot 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

Answer:

User1: Group1 only

User2: Group1 and Group2 only

Explanation:

The group memberships are determined by evaluating each user's attributes against the dynamic membership rules of the groups.

User1 Analysis:

• Group1: User1's city, "Montreal," starts with "m," so the condition (user.city -startsWith "m") is met.

• Group2: User1's department is "Human resources." The rule (user.department -notIn "human resources") requires the department not to be in the specified list. Therefore, this condition is not met.

• Group3: This group has an "Assigned" membership type, meaning users must be added manually. Since no assignment is mentioned, User1 is not a member.

• Conclusion: User1 is a member of Group1 only.

User2 Analysis:

• Group1: User2's city, "Melbourne," starts with "m," so the condition (user.city -startsWith "m") is met.

• Group2: User2's department, "Marketing," is not "Human resources," so the condition (user.department -notIn "human resources") is met.

• Group3: This is an "Assigned" group, and no assignment is mentioned for User2.

• Conclusion: User2 is a member of Group1 and Group2 only.

The "Office 365 license assigned" attribute is irrelevant for these specific group membership rules.

References:

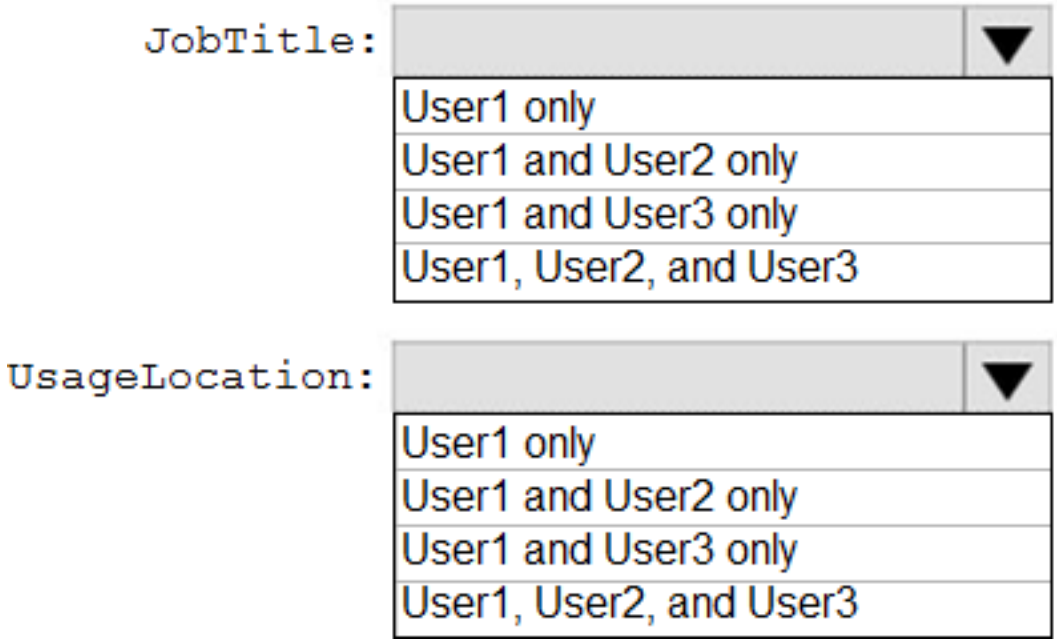
Microsoft Entra ID Documentation (formerly Azure AD): The rules for dynamic group membership are based on user or device properties. The evaluation logic used in this question directly applies the supported rule syntax.
Source: Microsoft Learn, "Rules for dynamically populated groups membership in Microsoft Entra ID."
Reference: The document details supported operators, including -startsWith for string comparisons and -notIn for matching against a collection of string values. The evaluation follows the logic described under the "Rule syntax" and "Supported expression rule operators" sections.

Question: 21

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:

User Attribute Can be modified from Azure AD? ---------- ------ User1 JobTitle No User1 UsageLocation Yes User2 JobTitle Yes User2 UsageLocation Yes User3 JobTitle Yes User3 UsageLocation Yes

Explanation:

User1 (Source: Windows Server AD): This user is synchronized from an on-premises Active Directory. Attributes like JobTitle are typically mastered on-premises and cannot be modified directly in Azure AD; changes must be made in the on-premises AD and then synchronized. However, UsageLocation can be modified in Azure AD if it's not set in or

synchronized from the on-premises AD, as it's crucial for licensing.
User2 (Source: Azure Active Directory): This is a cloud-only user. All attributes, including JobTitle and UsageLocation, are managed directly within Azure AD and can be modified there.
User3 (Source: External Azure Active Directory): This is a B2B guest user. Once the guest user accepts the invitation, their user object in the resource tenant's Azure AD can be updated. Attributes such as JobTitle and UsageLocation can be modified from Azure AD in the resource tenant.

References:

1. For User1 (Synchronized User - JobTitle):
Microsoft Learn: "Add or update a user's profile information and settings".
URL: https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/active-directoryusers-profile-azure-portal
Relevant section: "For users whose source of authority is Windows Server Active Directory, you must manage their information using your on-premises Windows Server Active Directory."
Microsoft Learn: "Attributes synchronized to Azure Active Directory" (Implies title is synced and mastered on-prem).
URL: https://learn.microsoft.com/en-us/azure/active-directory/hybrid/connect/referenceconnect-sync-attributes-synchronized

2. For User1 (Synchronized User - UsageLocation):
Microsoft Learn: "Set UsageLocation for Microsoft 365 users".
URL: https://learn.microsoft.com/en-us/microsoft-365/enterprise/set-usage-location-forusers?view=o365-worldwide
Relevant section: "For users that are synchronized from On-Premises Active Directory... If the UsageLocation value is not set in On-Premises Active Directory, you can set it directly in Azure AD or the Microsoft 365 admin center."
3. For User2 (Cloud-only User):
Microsoft Learn: "Add or update a user's profile information and settings".
URL: https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/active-directoryusers-profile-azure-portal
Relevant section: General principles for managing cloud-only user attributes.
4. For User3 (B2B Guest User):
Microsoft Learn: "Properties of an Azure Active Directory B2B collaboration user".
URL: https://learn.microsoft.com/en-us/azure/active-directory/external-identities/userproperties
Relevant section: "What user properties can I edit for B2B guest users? Once the guest user has accepted the invitation, their user object in Azure AD can be updated with any other user attributes like any other user object. For example, you can update their job title, department, or usage location."

Question: 22

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

Answer:

A (Yes)

Explanation:

To enable Traffic Analytics, a user needs permissions to create and manage Network Watcher, Log Analytics workspaces, and configure NSG flow logs. The Network Contributor role grants permissions to manage networking resources, including Network Watcher and NSGs. When assigned at the subscription level, this role provides sufficient permissions to configure Traffic Analytics, which involves reading NSG flow logs and writing data to a Log Analytics workspace.

References:

Microsoft Learn. (2023). Azure built-in roles - Network Contributor. "Grants permissions to manage networking resources." This includes Network Watcher and NSGs. Retrieved from https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#networkcontributor

Microsoft Learn. (2023). Traffic analytics - Prerequisites. "To configure traffic analytics, you need the following prerequisites: ... An Azure account with an active subscription. ... Appropriate permissions for Network Watcher, Log Analytics workspace, and NSGs." The Network Contributor role at the subscription scope covers these. Retrieved from https://learn.microsoft.com/en-us/azure/network-watcher/traffic-analytics-prerequisites

Microsoft Learn. (2023). Tutorial: Enable Traffic Analytics. "You need one of the following Azure roles assigned to your account: owner, contributor, reader, or network contributor." This explicitly lists Network Contributor. Retrieved from https://learn.microsoft.com/enus/azure/network-watcher/traffic-analytics-tutorial#prerequisites

Question: 23

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

Answer:

A

Explanation:

The Owner role at the subscription level grants full access to all resources within that subscription, including the ability to manage Network Watcher, NSG Flow Logs, and Log Analytics workspaces. These are all necessary components for enabling and configuring Traffic Analytics. The Owner role inherently includes all permissions required to perform these actions, such as Microsoft.Network/networkWatchers/configureFlowLog/action and Microsoft.OperationalInsights/workspaces/.

References:

1. Microsoft Learn. (2024). Azure built-in roles. "Owner: Has full access to all resources, including the right to delegate access to others." Retrieved from https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#owner
2. Microsoft Learn. (2023). Traffic analytics. "Prerequisites... One of the following Azure built-in roles needs to be assigned to your account: Owner, Contributor, Network Contributor, or a custom role that contains the necessary actions..." Retrieved from https://learn.microsoft.com/en-us/azure/network-watcher/traffic-analytics#prerequisites
3. Microsoft Learn. (2023). Tutorial: Log network traffic to and from a virtual machine using the Azure portal. "To enable traffic analytics, you must have the necessary permissions. Your account must be a member of one of the following Azure built-in roles: Owner, Contributor, Network contributor..." Retrieved from https://learn.microsoft.com/enus/azure/network-watcher/traffic-analytics-tutorial#prerequisites

Question: 24

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

Answer:

B (No)

Explanation:

To enable Traffic Analytics, the user requires permissions to write data to the Log Analytics workspace and modify Network Watcher resources. The Reader role only grants read-only access to Azure resources. The minimum required built-in roles at the subscription level to enable Traffic Analytics are Owner, Contributor, Network Contributor, or Monitoring Contributor.

References:

Microsoft Learn. (2024). Traffic analytics. "Prerequisites" section, "Permissions" subsection. Retrieved from https://learn.microsoft.com/en-us/azure/network-watcher/trafficanalytics#prerequisites
Microsoft Learn. (2024). Azure built-in roles. "Reader" role description. Retrieved from https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#reader

Question: 25

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

Answer:

C

Explanation:

User1 needs to deploy virtual machines and manage virtual networks.
The Virtual Machine Contributor role allows managing virtual machines (including deployment) but does not grant permissions to manage virtual networks themselves (it only allows reading network resources and joining VMs to existing networks).
The Contributor role grants permissions to manage all Azure resources, including virtual machines and virtual networks, but does not allow managing access (assigning roles). This fulfills both requirements.

While "Contributor" is a broad role, among the given options, it's the most appropriate single role that satisfies all specified requirements while being less permissive than "Owner". The principle of least privilege guides us to choose it over "Owner".

Why Incorrect Options are Wrong:

A. Owner: This role grants full access to all resources, including managing access, which is more than required and violates the principle of least privilege.
B. Virtual Machine Contributor: This role allows managing virtual machines but not virtual networks. The requirement is to manage both.
D. Virtual Machine Administrator Login: This role only grants permissions to log in to a virtual machine as an administrator, not to deploy or manage Azure infrastructure resources like VMs or VNets.

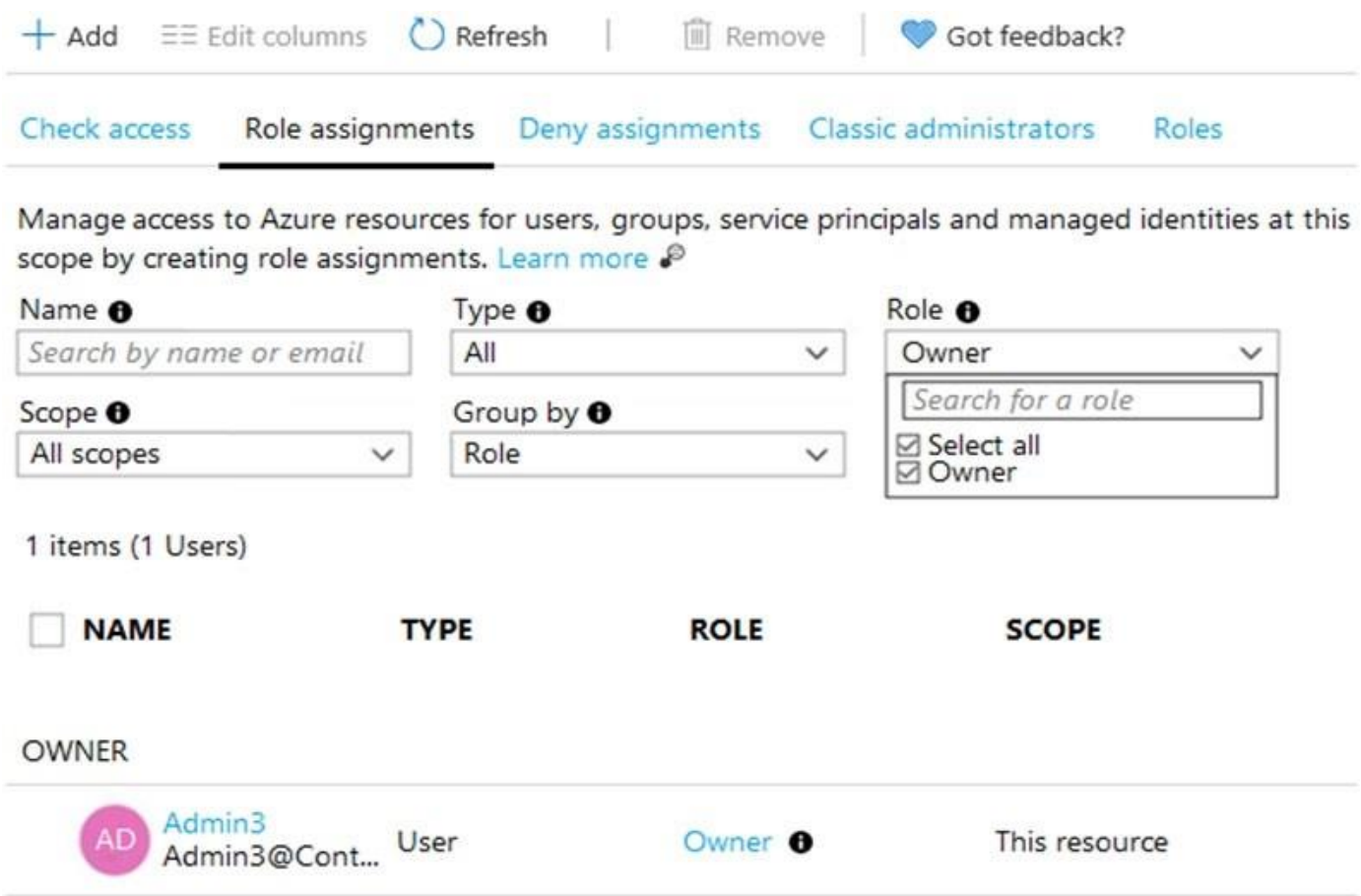
References:

Microsoft Learn: Azure built-in roles. (Covers descriptions of Owner, Contributor, Virtual Machine Contributor).
URL: https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles
Specific Sections: "Owner", "Contributor", "Virtual Machine Contributor", "Virtual Machine

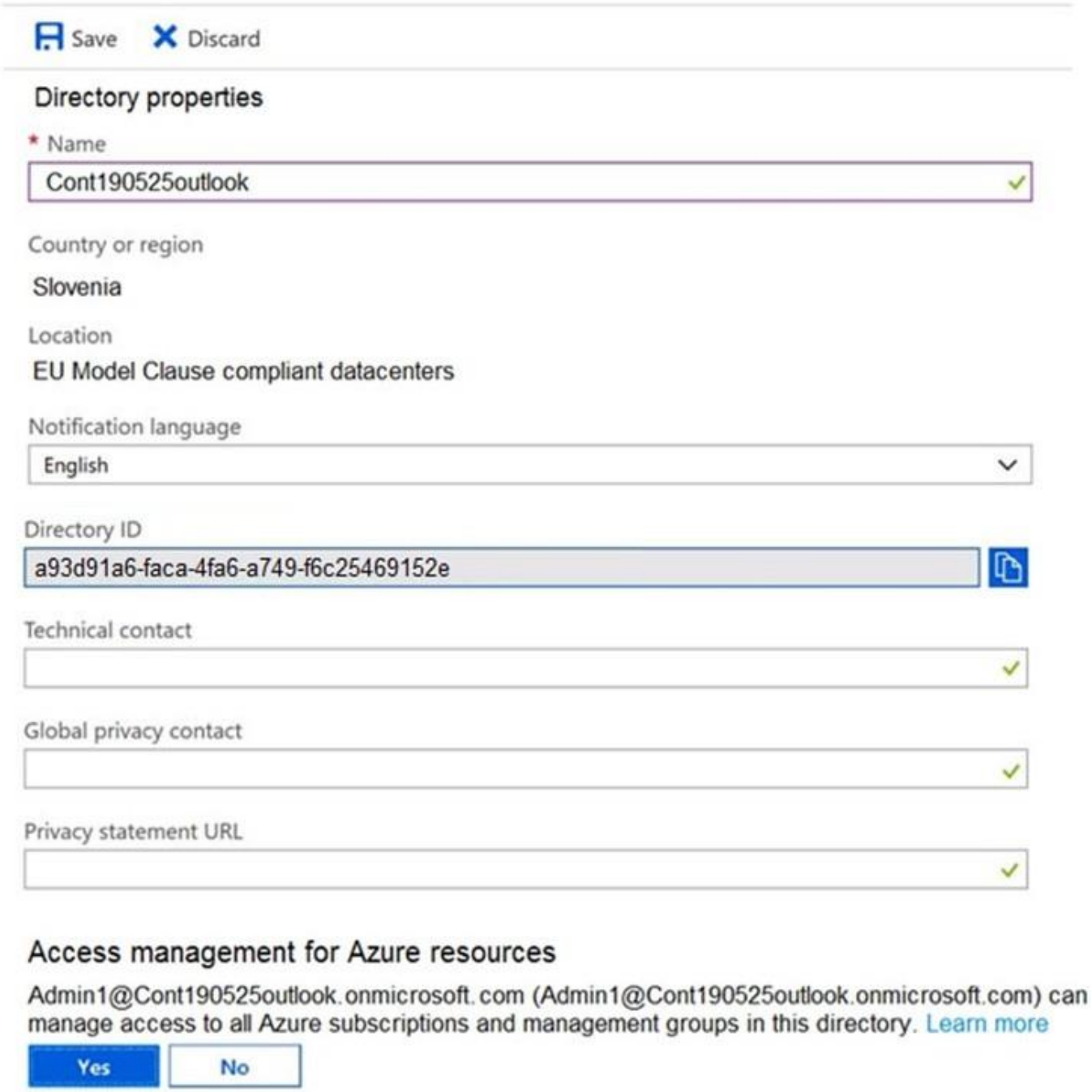
Administrator Login".
The "Virtual Machine Contributor" description explicitly states: "Lets you manage virtual machines, but not access to them, and not the virtual network or storage account they're connected to." This confirms it cannot manage virtual networks.
The "Contributor" role description states: "Lets you manage everything except access to resources." This includes managing VMs and VNets.
Microsoft Learn: Principle of least privilege.
URL: https://learn.microsoft.com/en-us/azure/role-based-access-control/bestpractices#apply-the-principle-of-least-privilege
This principle advocates granting only the permissions necessary to perform a task.
"Contributor" is chosen over "Owner" based on this. While more granular roles (like Virtual Machine Contributor + Network Contributor) would be ideal, "Contributor" is the best single option provided.

Question: 26

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. Hot 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:

Statement 1: Admin1 can assign users the Owner role for the Azure subscription.
Correct Answer: Yes
Explanation: Admin1 is assigned the Owner role on the Azure subscription as per the "Access control exhibit." The Owner role grants full access to manage all resources, including the ability to assign roles in Azure RBAC. Therefore, Admin1 can assign the Owner role to other users for this subscription.

References:

Microsoft Learn: "Azure built-in roles - Owner". States "Grants full access to manage all resources, including the ability to assign roles in Azure RBAC." (URL: https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#owner)

Microsoft Learn: "Classic subscription administrator roles, Azure roles, and Azure AD roles". Section "Azure roles". (URL: https://learn.microsoft.com/en-us/azure/role-based-accesscontrol/rbac-and-directory-admin-roles#azure-roles)
Statement 2: Admin2 can assign users the Reader role for the Azure subscription.
Correct Answer: Yes
Explanation: Admin2 is a Global Administrator. The "Tenant exhibit" shows that "Access management for Azure resources" is set to "Yes." This setting elevates the access of Global Administrators, granting them the User Access Administrator role at the root scope (/). The User Access Administrator role allows managing user access to Azure resources, which includes assigning roles like the Reader role.
References:
Microsoft Learn: "Elevate access to manage all Azure subscriptions and management groups". States "When you elevate your access, you will be assigned the User Access Administrator role in Azure at root scope (/). This allows you to view all resources and assign access in any subscription or management group in the directory." (URL: https://learn.microsoft.com/en-us/azure/role-based-access-control/elevate-access-globaladmin)
Microsoft Learn: "Azure built-in roles - User Access Administrator". States "Lets you manage user access to Azure resources." This role includes the

Microsoft.Authorization/roleAssignments/write permission. (URL: https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#useraccess-administrator)

Statement 3: Admin3 can create Azure resources in the Azure subscription.

Correct Answer: No

Explanation: Admin3 is a Global Administrator, and "Access management for Azure resources" is enabled. This grants Admin3 the User Access Administrator role at the root scope (/). The User Access Administrator role allows managing user access (i.e., assigning roles to users, including themselves) but does not inherently grant permissions to create or manage Azure resources like virtual machines or storage accounts. To create resources, Admin3 would first need to use their User Access Administrator privilege to assign themselves a role with resource creation permissions (e.g., Contributor or Owner) on the subscription. The User Access Administrator role itself does not provide these permissions directly.

References:

Microsoft Learn: "Azure built-in roles - User Access Administrator". The permissions listed for this role (e.g., Microsoft.Authorization/, Microsoft.Support/) do not include actions for creating or modifying resources under providers like Microsoft.Compute or Microsoft.Storage. (URL: https://learn.microsoft.com/en-us/azure/role-based-accesscontrol/built-in-roles#user-access-administrator)

Microsoft Learn: "Elevate access to manage all Azure subscriptions and management groups". This document clarifies that elevation grants the User Access Administrator role, whose purpose is to "assign access". (URL: https://learn.microsoft.com/en-us/azure/rolebased-access-control/elevate-access-global-admin)

References:

Question: 27

You have an Azure subscription named Subscription1 that contains an Azure virtual machine named VM1. VM1 is in a resource group named RG1. VM1 runs services that will be used to deploy resources to RG1. You need to ensure that a service running on VM1 can manage the resources in RG1 by using the identity of VM1. What should you do first?

A. From the Azure portal, modify the Managed Identity settings of VM1

B. From the Azure portal, modify the Access control (IAM) settings of RG1

C. From the Azure portal, modify the Access control (IAM) settings of VM1

D. From the Azure portal, modify the Policies settings of RG1

Answer:

A

Explanation:

To allow a service on VM1 to manage resources in RG1 using VM1's identity, you must first enable a managed identity (either system-assigned or user-assigned) for VM1. This creates a service principal in Azure Active Directory that represents VM1. Once the identity is enabled, you can then grant this identity the necessary permissions (e.g., Contributor role) on the resource group RG1 via its Access control (IAM) settings. Enabling the managed identity on VM1 is the prerequisite.

Why Incorrect Options are Wrong:

B: Modifying IAM settings of RG1 is the second step, done after VM1 has an identity to assign permissions to.
C: Modifying IAM settings of VM1 grants permissions to VM1, not from VM1 to manage other resources.
D: Azure Policy enforces organizational standards and compliance; it's not used for granting direct management permissions to a VM's identity.

References:

Microsoft Learn. (2023). Managed identities for Azure resources. "To allow an Azure resource to use managed identities, you first enable a managed identity on the resource." https://learn.microsoft.com/en-us/azure/active-directory/managed-identities-azureresources/overview
Microsoft Learn. (2023). Configure managed identities for Azure resources on a VM using the Azure portal. "Azure resources that support managed identities always have an option to enable managed identities." https://learn.microsoft.com/en-us/azure/activedirectory/managed-identities-azure-resources/qs-configure-portal-windows-vm#enable-

system-assigned-managed-identity-on-an-existing-vm
Microsoft Learn. (2023). Assign an Azure role to a managed identity. "After you configure an Azure resource with a managed identity, you can give the managed identity access to another resource, just like any security principal." https://learn.microsoft.com/enus/azure/active-directory/managed-identities-azure-resources/howto-assign-managed-identity-access-portal

Question: 28

You have an Azure subscription that contains a resource group named TestRG. You use TestRG to validate an Azure deployment. TestRG contains the following resources:

Name	Type	Description
VM1	Virtual Machine	VM1 is running and configured to back up to Vault1 daily
Vault1	Recovery Services Vault	Vault1 includes all backups of VM1
VNET1	Virtual Network	VNET1 has a resource lock of type Delete

You need to delete TestRG. What should you do first?

A. Modify the backup configurations of VM1 and modify the resource lock type of VNET1

B. Remove the resource lock from VNET1 and delete all data in Vault1

C. Turn off VM1 and remove the resource lock from VNET1

D. Turn off VM1 and delete all data in Vault1

Answer:

B

Explanation:

To delete the resource group TestRG, you must first address any impediments to deleting its constituent resources. VNET1 has a Delete lock, which prevents its deletion; this lock must be removed. Vault1 is a Recovery Services vault likely protecting VM1. A Recovery Services vault cannot be deleted if it contains backup items. Therefore, you must stop the backup for VM1 and delete the backup data from Vault1. Option B covers both these necessary prerequisite actions.

Why Incorrect Options are Wrong:

A: Modifying the lock type (unless to 'None' or removed) is insufficient; the lock must be removed.
C: Turning off VM1 does not resolve the backup dependency with Vault1, which prevents Vault1's deletion.
D: Turning off VM1 is not the primary blocker, and this option fails to address the resource lock on VNET1.

References:

Resource Locks: Microsoft Learn. (2023). Lock resources to prevent unexpected changes. "Before you can delete a locked resource, you must first remove the lock."
Direct URL: https://learn.microsoft.com/en-us/azure/azure-resourcemanager/management/lock-resources?tabs=json#delete
Deleting Recovery Services Vault: Microsoft Learn. (2023). Delete an Azure Backup Recovery Services vault. "You can't delete a Recovery Services vault if there are any dependencies, such as backup items or recovery points... To delete a vault with dependencies: ... In the item's dashboard, select Stop backup. In the Stop Backup page, select Delete Backup Data from the dropdown menu."
Direct URL: https://learn.microsoft.com/en-us/azure/backup/backup-azure-deletevault?tabs=portal#delete-a-recovery-services-vault-with-dependencies
Deleting Resource Groups: Microsoft Learn. (2023). Azure Resource Manager resource group and resource deletion. "When you delete a resource group, Resource Manager determines the order to delete resources... It waits for dependencies to be finished before deleting a dependent resource... If you have a lock on a resource group or a resource, you must remove the lock before you can delete the resource group or resource."
Direct URL: https://learn.microsoft.com/en-us/azure/azure-resourcemanager/management/delete-resource-group?tabs=azure-powershell#how-resources-are-deleted

Question: 29

You have an Azure DNS zone named adatum.com. You need to delegate a subdomain named research.adatum.com to a different DNS server in Azure. What should you do?

A. Create an NS record named research in the adatum.com zone.

B. Create a PTR record named research in the adatum.com zone.

C. Modify the SOA record of adatum.com.

D. Create an A record named *.research in the adatum.com zone.

Answer:

A

Explanation:

To delegate a subdomain like research.adatum.com to different DNS servers, you must create a Name Server (NS) record in the parent zone (adatum.com). This NS record, named research, will specify the authoritative name servers for the research.adatum.com subdomain. This action effectively transfers DNS resolution authority for the subdomain to the designated servers.

Why Incorrect Options are Wrong:

B. Create a PTR record named research in the adatum.com zone. PTR records are for reverse DNS lookups (IP to name), not subdomain delegation.
C. Modify the SOA record of adatum.com. The SOA record defines authoritative information for the zone itself, not for delegating subdomains.
D. Create an A record named .research in the adatum.com zone. An A record maps a hostname to an IP address; a wildcard A record resolves undefined hosts but doesn't delegate authority.

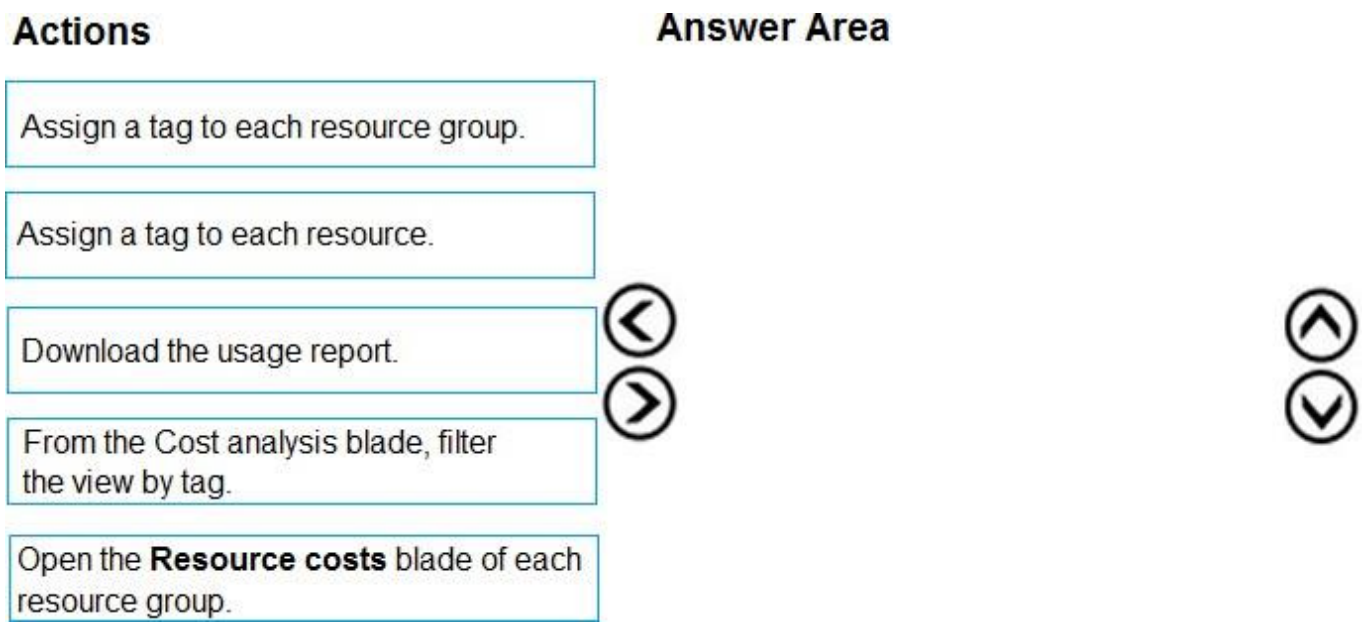
References:

Microsoft Learn. (2023). Delegate an Azure DNS subdomain - Azure portal. "To delegate a DNS subdomain... you delegate this subdomain by creating a name server (NS) record set in the parent zone." Retrieved from https://learn.microsoft.com/en-us/azure/dns/delegatesubdomain-azure-dns
Microsoft Learn. (2023). Azure DNS FAQ. "How do I delegate a subdomain? You create a child DNS zone, then delegate it from the parent by creating an NS record set in the parent zone." Retrieved from https://learn.microsoft.com/en-us/azure/dns/dns-faq#how-do-idelegate-a-subdomain--
Mockapetris, P. (1987). RFC 1035: Domain Names - Implementation and Specification. IETF. Section 3.3.11. NS RDATA format. Retrieved from

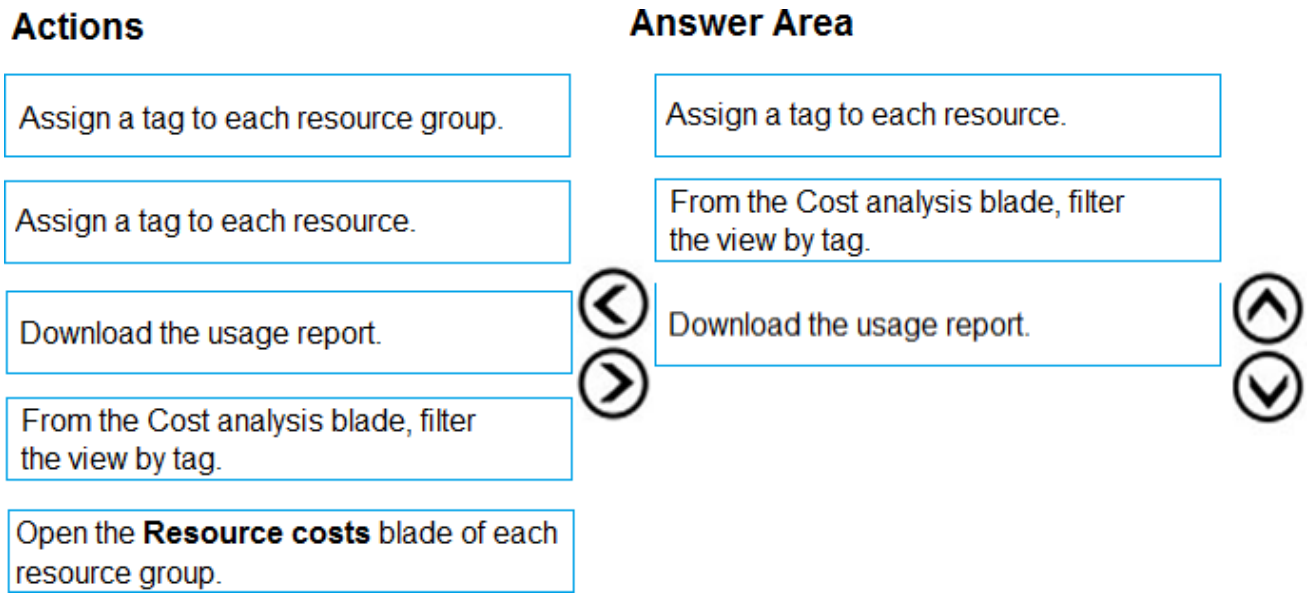
https://datatracker.ietf.org/doc/html/rfc1035#section-3.3.11 (General DNS principles)

Question: 30

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:



Answer:



Explanation:

To accurately report costs by department when departments use resources across multiple resource groups, you must first apply a consistent metadata tag (e.g., a "Department" tag) to each individual resource. This creates a logical grouping for cost allocation that is independent of the resource group structure.

Next, you use the Cost Analysis tool within Azure Cost Management. This tool allows you to group and filter cost data based on various properties, including the tags you applied. By filtering by the "Department" tag, you can aggregate all costs associated with a specific department.

Finally, after the view is correctly filtered to show the departmental cost breakdown, you can download this data as a usage report to be shared with the finance department.

References:

Microsoft Learn, Azure Documentation: Group and allocate costs using tags. This official document explicitly states, "Tags are a key part of organizing your Azure resources... Tags are useful for rolling up billing information. For example, you can tag resources with the department they belong to and then use Azure Cost Management + Billing to see the costs for that department." This supports the first action.

o URL: https://learn.microsoft.com/en-us/azure/cost-managementbilling/costs/cost-mgt-best-practices#group-and-allocate-costs-using-tags

Microsoft Learn, Azure Documentation: Use cost analysis for common tasks. This guide details how to use the Cost Analysis tool. It includes sections on "View costs

for a specific tag" and "Download your usage data," which directly correspond to the second and third steps in the correct sequence.

o URL: https://learn.microsoft.com/en-us/azure/cost-managementbilling/costs/cost-analysis-common-uses (Refer to sections: "View costs for a specific tag" and "Download usage data").

Question: 31

You have a registered DNS domain named contoso.com. You create a public Azure DNS zone named contoso.com. You need to ensure that records created in the contoso.com zone are resolvable from the internet. What should you do?

A. Create NS records in contoso.com.

B. Modify the SOA record in the DNS domain registrar.

C. Create the SOA record in contoso.com.

D. Modify the NS records in the DNS domain registrar.

Answer:

D

Explanation:

To make records in an Azure DNS public zone resolvable from the internet, you must delegate your domain to Azure DNS. This involves updating the Name Server (NS) records at your domain registrar (where you purchased the domain name) to point to the Azure DNS name servers assigned to your zone. This tells the internet's DNS system where to find the authoritative DNS records for your domain.

Why Incorrect Options are Wrong:

A. Create NS records in contoso.com: Azure DNS automatically creates NS records within the zone. This action doesn't delegate the domain.
B. Modify the SOA record in the DNS domain registrar: SOA records are managed within the authoritative DNS zone (Azure DNS), not typically modified at the registrar for delegation.
C. Create the SOA record in contoso.com: Azure DNS automatically creates the SOA record when the zone is created. This doesn't achieve internet resolvability.

References:

Microsoft Learn. (2023). Delegate a domain to Azure DNS. "To delegate your Azure DNS zone, you must update the parent domain by using the name servers from Azure DNS. Each registrar has its own DNS management tools to change the name server records for a domain. In the registrar's DNS management page, edit the NS records and replace the NS records with the Azure DNS name servers." Retrieved from https://learn.microsoft.com/enus/azure/dns/dns-delegate-domain-azure-dns
Microsoft Learn. (2023). Tutorial: Host your domain in Azure DNS. "Before you can delegate your contoso.com DNS zone to Azure DNS, you need to know the name servers for your zone... Once the DNS zone gets created and you have the name servers, you'll

need to update the parent domain with the Azure DNS name servers. Each registrar has its own DNS management tools to change the name server records for a domain." Retrieved from https://learn.microsoft.com/en-us/azure/dns/dns-hosting-manual

Question: 32

HOTSPOT - You have an Azure subscription that contains a storage account named storage1. The subscription is linked to an Azure Active Directory (Azure AD) tenant named contoso.com that syncs to an on-premises Active Directory domain. The domain contains the security principals shown in the following table.

Name	Type
User1	User
Computer1	Computer

In Azure AD, you create a user named User2. The storage1 account contains a file share named share1 and has the following configurations.

```
"kind": "StorageV2",
"properties": {
                "azureFilesIdentityBasedAuthentication": {
                    "directoryServiceOptions": "AD",
                    "activeDirectoryProperties": {
                        "domainName": "Contoso.com",
                        "netBiosDomainName": "Contoso.com",
                        "forestName": "Contoso.com",
-
                    }
            }
```

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:

Statements	Yes	No
You can assign the Storage File Data SMB Share Contributor role to User1 for share1.	○	○
You can assign the Storage File Data SMB Share Reader role to Computer1 for share1.	○	○
You can assign the Storage File Data SMB Share Elevated Contributor role to User2 for share1.	○	○

Answer:

Statement 1: You can assign the Storage File Data SMB Share Contributor role to User1 for share1.

Answer: Yes

Statement 2: You can assign the Storage File Data SMB Share Reader role to

Computer1 for share1.
Answer: No
Statement 3: You can assign the Storage File Data SMB Share Elevated Contributor role to User2 for share1.
Answer: No

Explanation:

Statement 1 (Yes): The storage account is configured for on-premises Active Directory Domain Services (AD DS) authentication (directoryServiceOptions: "AD"). User1 is a hybrid identity, meaning it exists in the on-premises AD DS and is synchronized to Azure AD. This is the required configuration. An Azure RBAC role can be assigned to the Azure AD identity (User1), and authentication will be handled by the on-premises AD DS.
Statement 2 (No): Azure RBAC share-level permissions for Azure Files can be assigned to user, group, or service principal identities in Azure AD. Assigning these data access roles directly to computer identities is not a supported configuration. Access control is managed through user or group principals.
Statement 3 (No): User2 is a cloud-only identity that exists only in Azure AD and not in the on-premises AD DS. Since the storage account is configured to use the on-premises AD DS for authentication, it cannot authenticate User2. For this authentication method to work, the user identity must exist in the on-premises AD DS that the storage account is joined to.

References:

Microsoft Documentation - Overview of Azure Files identity-based authentication options for SMB access:
o URL: https://learn.microsoft.com/en-us/azure/storage/files/storage-filesactive-directory-overview
o Supporting Section: Under the "On-premises Active Directory Domain Services (AD DS)" section, it states: "Identities used for access must be hybrid user identities, which exist in both on-premises AD DS and Azure AD." This directly supports the answers for User1 (a hybrid identity) and User2 (a cloud-only identity).

Microsoft Documentation - Assign share-level permissions:
o URL: https://learn.microsoft.com/en-us/azure/storage/files/storage-filesidentity-ad-ds-assign-permissions
o Supporting Section: The "Assign permissions to an identity" section specifies assigning roles to "a user/group". The documentation consistently refers to assigning roles to users, groups, and service

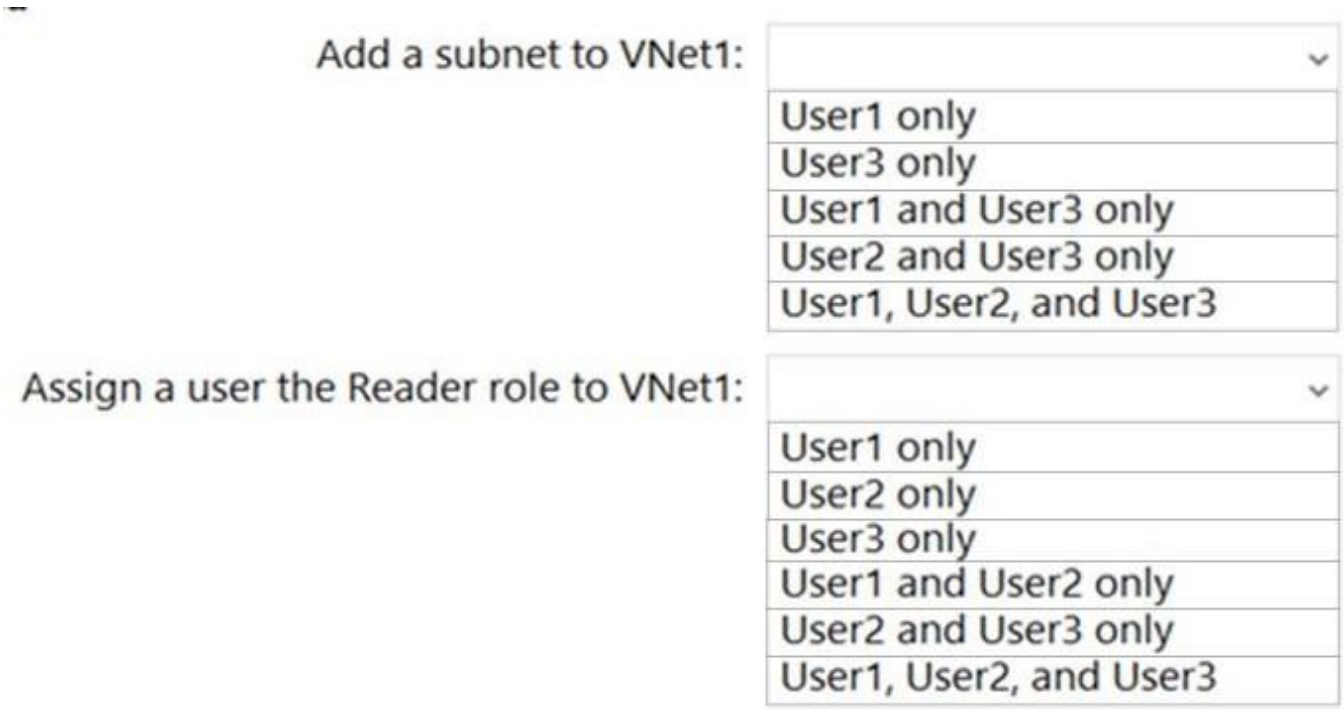
principals, not computer objects, for data-plane access.

Question: 33

HOTSPOT - You have an Azure subscription named Subscription1 that contains a virtual network VNet1. You add the users in the following table.

User	Role
User1	Owner
User2	Security Admin
User3	Network Contributor

Which user can perform each configuration? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point. Hot Area:



Answer:

Add a subnet to VNet1: User1 and User3 only
Assign a user the Reader role to VNet1: User1 only

Explanation:

Azure role-based access control (RBAC) permissions are inherited from parent scopes. In this scenario, all roles are assigned at the subscription level and thus apply to VNet1.
Add a subnet to VNet1: This action requires write permissions for virtual networks, specifically Microsoft.Network/virtualNetworks/subnets/write.

User1 (Owner): Has unrestricted permissions to all resources, including adding a subnet.
User3 (Network Contributor): This role is specifically designed to manage network resources and includes the necessary permissions to create and manage subnets.
User2 (Security Admin): This role lacks the permissions to modify network resources.
Assign a user the Reader role to VNet1: This action requires permission to create role assignments, specifically Microsoft.Authorization/roleAssignments/write.
User1 (Owner): Includes this permission, allowing them to delegate access to other users.
User2 (Security Admin) and User3 (Network Contributor): Neither of these roles includes the permission to assign access roles to other users for resources.

References:

1. Azure built-in roles documentation: This official Microsoft Learn document provides a comprehensive list and description of all built-in roles in Azure.
o URL: https://learn.microsoft.com/en-us/azure/role-based-access-control/builtin-roles
o Specifics: The general table on this page outlines the capabilities of key roles.
2. Owner Role Documentation:
o URL: https://learn.microsoft.com/en-us/azure/role-based-access-control/builtin-roles#owner
o Specifics: "Grants full access to manage all resources, including the ability to assign roles in Azure RBAC." This confirms User1 can perform both tasks.

3. Network Contributor Role Documentation:
o URL: https://learn.microsoft.com/en-us/azure/role-based-access-control/builtin-roles#network-contributor
o Specifics: "Lets you manage networks, but not access to them." This explicitly states the role can modify the network (add a subnet) but cannot assign roles (manage access).
4. Security Admin Role Documentation:
o URL: https://learn.microsoft.com/en-us/azure/role-based-access-control/builtin-roles#security-admin
o Specifics: Details permissions related to security resources (like Microsoft Defender for Cloud), but does not include permissions for general network resource management or role assignments.

Question: 34

HOTSPOT - You have the Azure resources shown on the following exhibit.

You plan to track resource usage and prevent the deletion of resources. To which resources can you apply locks and tags? To answer, select the appropriate options in the answer

Locks:

RG1 and VM1 only
Sub1 and RG1 only
Sub1, RG1, and VM1 only
MG1, Sub1, RG1, and VM1 only
Tenant Root Group, MG1, Sub1, RG1, and VM1

Tags:

RG1 and VM1 only
Sub1 and RG1 only
Sub1, RG1, and VM1 only
MG1, Sub1, RG1, and VM1 only
Tenant Root Group, MG1, Sub1, RG1, and VM1

Answer:

- Subscription: Locks - Yes Tags - Yes
- Resource group: Locks - Yes Tags - Yes
- Individual resource: Locks - Yes Tags - Yes
- Management group (if listed): Locks - No Tags - No

Explanation:

Azure resource locks can be placed at three scopes only: the individual resource, its resource group, or the entire subscription; they are not supported at management-group level.

Azure tags are supported on almost every deployable Azure entity, including subscriptions, resource groups, and individual resources, but tagging is not available at the management-group scope.

References:

1. Microsoft Learn Apply, lock, and remove Azure resource locks (Scopes: subscription, resource group, resource)
https://learn.microsoft.com/azure/azure-resource-manager/management/lock-resources
2. Microsoft Learn Use tags to organize your Azure resources (Subscriptions, resource groups, and resources)

https://learn.microsoft.com/azure/azure-resource-manager/management/tag-resources

Question: 35

You have an Azure Active Directory (Azure AD) tenant. You plan to delete multiple users by using Bulk delete in the Azure Active Directory admin center. You need to create and upload a file for the bulk delete. Which user attributes should you include in the file?

A. The user principal name and usage location of each user only

B. The user principal name of each user only

C. The display name of each user only

D. The display name and usage location of each user only

E. The display name and user principal name of each user only

Answer:

B

Explanation:

When performing a bulk delete of users in Azure Active Directory using a CSV file, the only required attribute for each user is their User Principal Name (UPN). The UPN uniquely identifies each user within the Azure AD tenant. Other attributes like display name or usage location are not necessary for the bulk delete operation.

Why Incorrect Options are Wrong:

A. The user principal name and usage location of each user only: Usage location is not required for bulk deletion.
C. The display name of each user only: The display name is not a unique identifier and is not sufficient for bulk deletion.
D. The display name and usage location of each user only: Neither display name nor usage location are the required unique identifiers for this operation.
E. The display name and user principal name of each user only: While the UPN is correct, the display name is not required for bulk deletion.

References:

Microsoft Entra ID (formerly Azure AD) Documentation. (2023). Bulk delete users in Microsoft Entra ID. Microsoft Learn. Retrieved from https://learn.microsoft.com/enus/entra/identity/users/users-bulk-delete#download-the-csv-template
Specific Section: "Download the CSV template" - "Open the CSV file and add a line for each user you want to delete. The only required value is User principal name. Save the file."