Hi,

QUESTION: 182 **Exam Topic: Manage Azure identities and governance questions**

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

A Device settings from the Devices blade

B Providers from the MFA Server blade

C User settings from the Users blade

D General settings from the Groups blade

Answer(s): A

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

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

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

QUESTION: 183 **Exam Topic: Manage Azure identities and governance questions**

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(s): C

Explanation:
The IT Service Management Connector (ITSMC) allows you to connect Azure and a supported IT Service Management (ITSM) product/service, such as the Microsoft System Center Service Manager.

With ITSMC, you can create work items in ITSM tool, based on your Azure alerts (metric alerts, Activity Log alerts and Log Analytics alerts).

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

QUESTION: 184 **Exam Topic: Manage Azure identities and governance questions**

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(s): A

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

QUESTION: 185 **Exam Topic: Manage Azure identities and governance questions**

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

A From the Licenses blade, assign a new license

B From the Directory role blade, modify the directory role

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

Answer(s): B

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

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

QUESTION: 186 **Exam Topic: Manage Azure identities and governance questions**

You recently created a new Azure subscription that contains a user named Admin1.

Admin1 attempts to deploy an Azure Marketplace resource by using an Azure Resource Manager template. Admin1 deploys the template by using Azure PowerShell and receives the following error message: "User failed validation to purchase resources. Error message: "Legal terms have not been accepted for this item on this subscription. To accept legal terms, please go to the Azure portal (http://go.microsoft.com/fwlink/?LinkId=534873) and configure programmatic deployment for the Marketplace item or create it there for the first time."

You need to ensure that Admin1 can deploy the Marketplace resource successfully. What should you do?

A From Azure PowerShell, run the Set-AzApiManagementSubscriptioncmdlet

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

C From Azure PowerShell, run the Set-AzMarketplaceTermscmdlet

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

Answer(s): C

Reference:
https://docs.microsoft.com/en-us/powershell/module/az.marketplaceordering/set-azmarketplaceterms?view=azps-4.1.0

QUESTION: 187 **Exam Topic: Manage Azure identities and governance questions**

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

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

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

A VM1, storage1, VNET1, and VM1Managed only

B VM1 and VM1Managed only

C VM1, storage1, VNET1, VM1Managed, and RVAULT1

D RVAULT1 only

Answer(s): C

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

Reference:
https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/move-resource-group-and-subscription
https://docs.microsoft.com/en-us/azure/key-vault/general/keyvault-move-subscription

QUESTION: 188 **Exam Topic: Manage Azure identities and governance questions**

HOTSPOT

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

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

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

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

To RG6, you apply the tag: RGroup: RG6.
You deploy a virtual network named VNET2 to RG6.

Which tags apply to VNET1 and VNET2? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Hot Area:

Answer Area

VNET1:

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

VNET2:

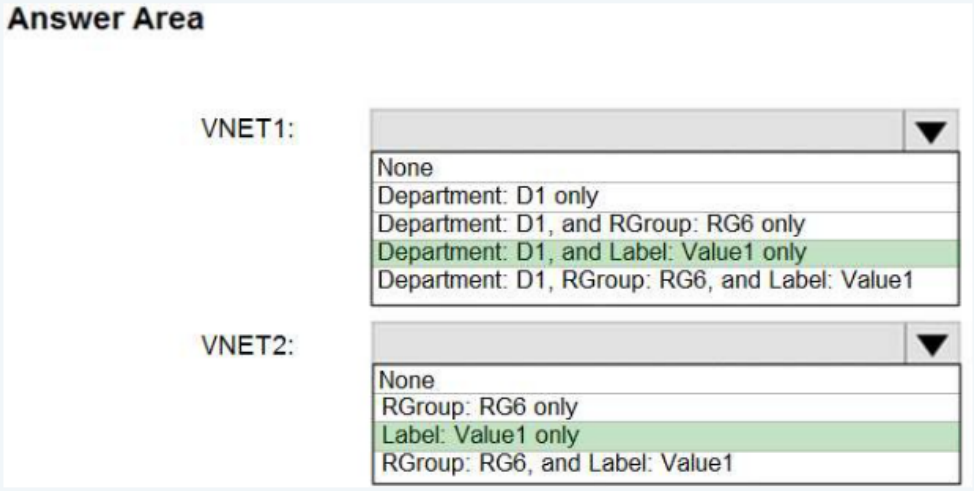
- None
- RGroup: RG6 only
- Label: Value1 only
- RGroup: RG6, and Label: Value1

A See Explanation section for answer.

Answer(s): A

Answer(s): A

Explanation:



VNET1: Department: D1, and Label:Value1 only.
Tags applied to the resource group or subscription are not inherited by the resources.

Note: Azure Policy allows you to use either built-in or custom-defined policy definitions and assign them to either a specific resource group or across a whole Azure subscription.

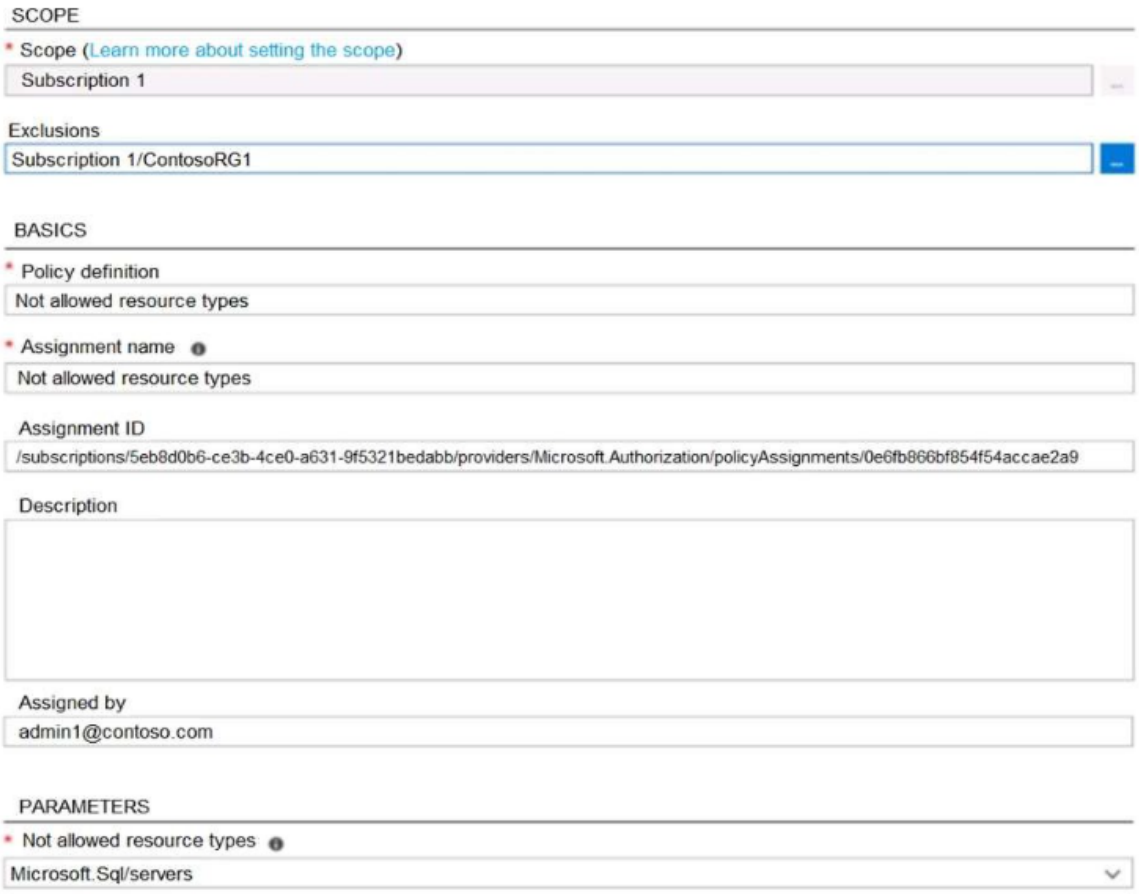
VNET2: Label:Value1 only.

Incorrect Answers:
RGROUP: RG6
Tags applied to the resource group or subscription are not inherited by the resources.

Reference:
https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/tag-policies

QUESTION: 189 **Exam Topic: Manage Azure identities and governance questions**

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



What is the effect of the policy?

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

B You can create Azure SQL servers in ContosoRG1 only.

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

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

Answer(s): B

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

QUESTION: 190 **Exam Topic: Manage Azure identities and governance questions**

HOTSPOT

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

Name	In management group
Tenant Root Group	*Not applicable*
ManagementGroup11	Tenant Root Group
ManagementGroup12	Tenant Root Group
ManagementGroup21	ManagementGroup11

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

Name	Management group
Subscription1	ManagementGroup21
Subscription2	ManagementGroup12

You create the Azure policies shown in the following table:

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

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

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

A See Explanation section for answer.

Answer(s): A

Answer(s): A

Explanation:

Answer Area

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

Box 1: No
Virtual networks are not allowed at the root and is inherited. Deny overrides allowed.

Box 2: Yes
Virtual Machines can be created on a Management Group provided the user has the required RBAC permissions.

Box 3: Yes
Subscriptions can be moved between Management Groups provided the user has the required RBAC permissions.

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

QUESTION: 191 **Exam Topic: Manage Azure identities and governance questions**

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

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

B Event | search "error"

C select * from Event where EnventType == "error"

D Event | where EventType is "error"

Answer(s): B

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

QUESTION: 192 **Exam Topic: Manage Azure identities and governance questions**

HOTSPOT

You have an Azure subscription that contains a virtual network named VNET1 in the East US 2 region. You have the following resources in an Azure Resource Manager template.

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

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

For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.
Hot Area:

Answer Area

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

A See Explanation section for answer.

Answer(s): A

Answer(s): A

Explanation:

Answer Area

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

Box 1: Yes

Box 2: Yes

VM1 is in Zone1, while VM2 is on Zone2.

Box 3: No

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

QUESTION: 193 **Exam Topic: Manage Azure identities and governance questions**

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(s): A

Explanation:
You can move an app to another App Service plan, as long as the source plan and the target plan are in the same resource group and geographical region.
The region in which your app runs is the region of the App Service plan it's in. However, you cannot change an App Service plan's region.

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

QUESTION: 194 **Exam Topic: Manage Azure identities and governance questions**

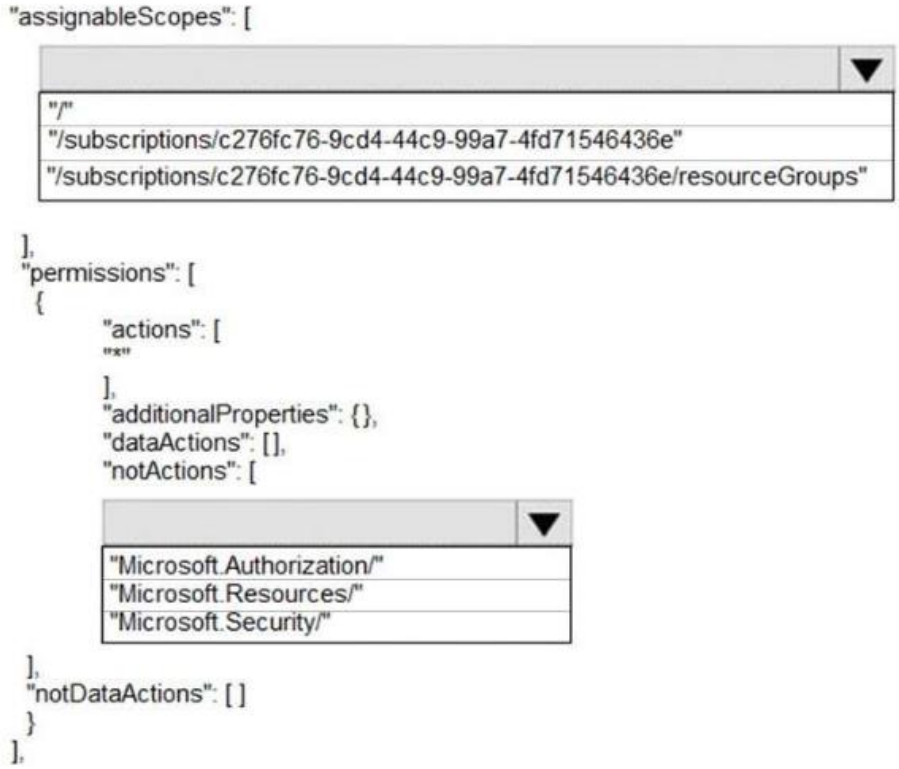
HOTSPOT
You have an Azure subscription named Subscription1 that has a subscription ID of c276fc76-9cd4-44c9-99a7- 4fd71546436e.
You need to create a custom RBAC role named CR1 that meets the following requirements:

□Can be assigned only to the resource groups in Subscription1
□Prevents the management of the access permissions for the resource groups
□Allows the viewing, creating, modifying, and deleting of resources within the resource groups

What should you specify in the assignable scopes and the permission elements of the definition of CR1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.
Hot Area:

Answer Area



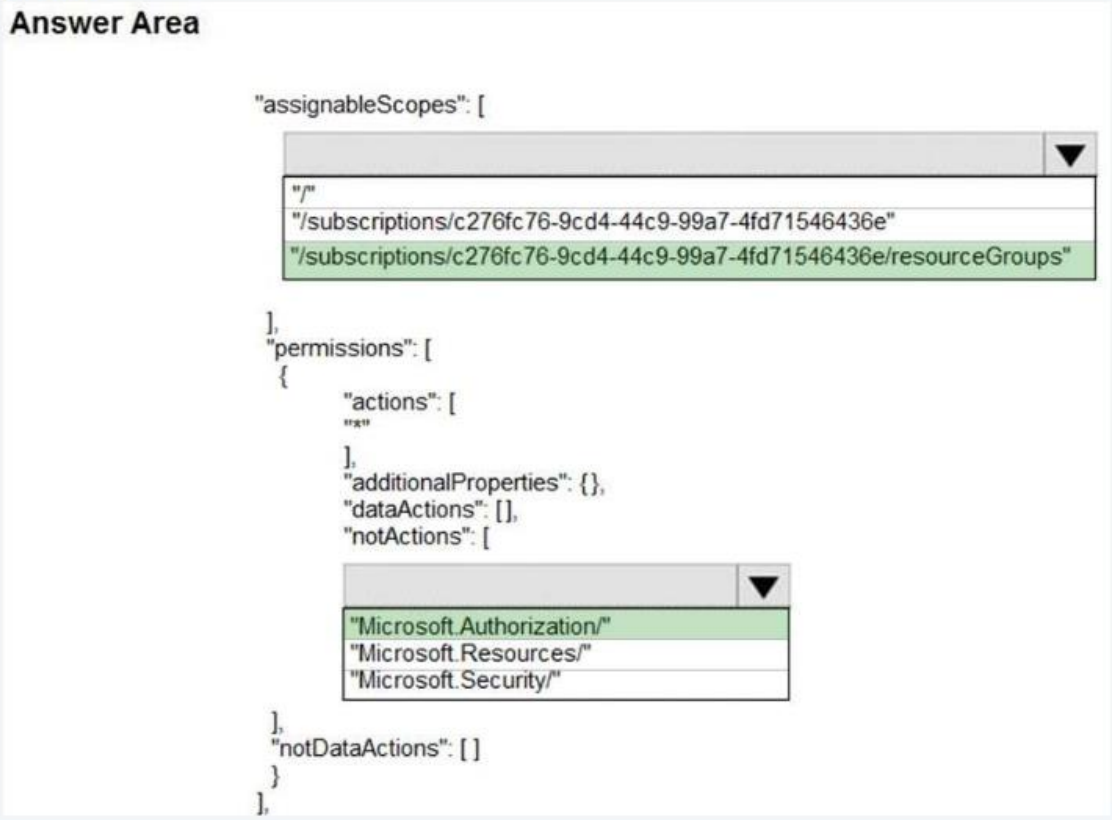
A See Explanation section for answer.

Answer(s): A

Answer(s): A

Explanation:

Answer Area



Reference:

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

https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftresources

QUESTION: 195 **Exam Topic: Manage Azure identities and governance questions**

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(s): D

Reference:
https://docs.microsoft.com/en-us/azure/dns/dns-delegate-domain-azure-dns

QUESTION: 196 **Exam Topic: Manage Azure identities and governance questions**

You have an Azure subscription named Subscription1 that contains an Azure Log Analytics workspace named Workspace1.

You need to view the error event from a table named Event. Which query should you run in Workspace1?

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

B Event | search "error"

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

D Event | where EventType is "error"

Answer(s): B

Reference:
https://docs.microsoft.com/en-us/azure/azure-monitor/log-query/search-queries
https://docs.microsoft.com/en-us/azure/azure-monitor/log-query/get-started-portal
https://docs.microsoft.com/en-us/azure/data-explorer/kusto/query/searchoperator?pivots=azuredataexplorer

QUESTION: 197 **Exam Topic: Manage Azure identities and governance questions**

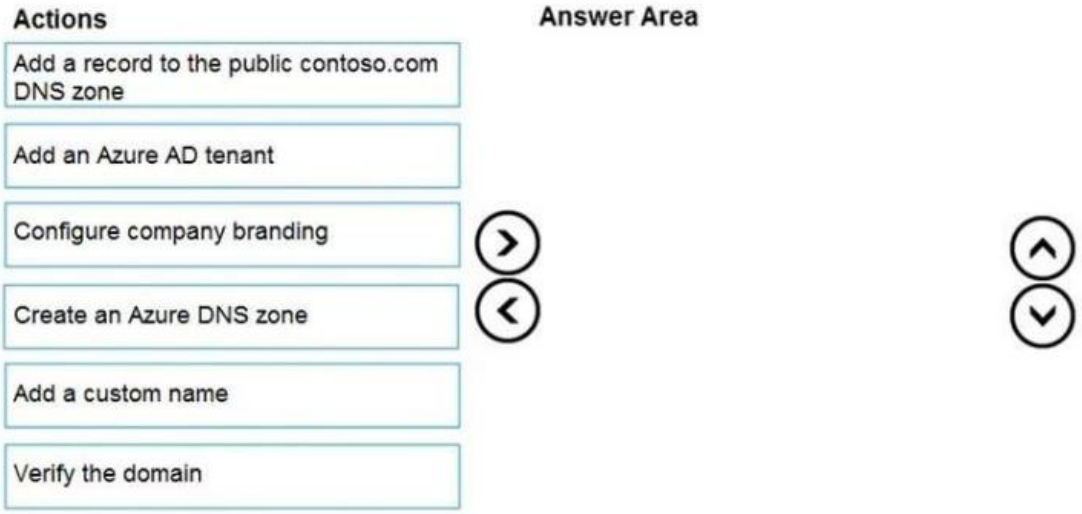
DRAG DROP

You have an Azure Active Directory (Azure AD) tenant that has the contoso.onmicrosoft.com domain name. You have a domain name of contoso.com registered at a third-party registrar.

You need to ensure that you can create Azure AD users that have names containing a suffix of @contoso.com.

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:

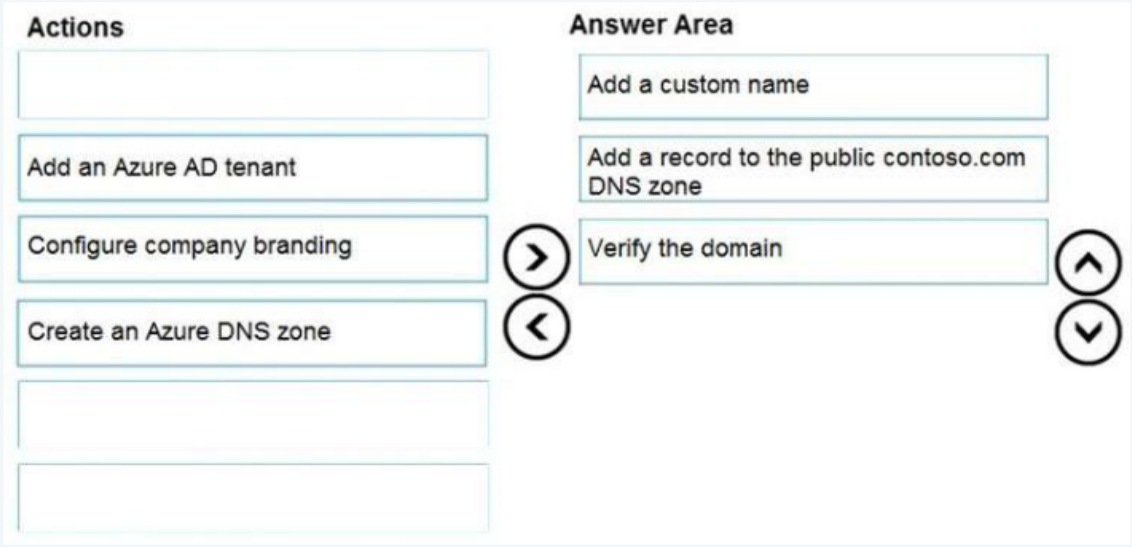


A See Explanation section for answer.

Answer(s): A

Answer(s): A

Explanation:



1. Add the custom domain name to your directory
2. Add a DNS entry for the domain name at the domain name registrar
3. Verify the custom domain name in Azure AD

Reference:
https://docs.microsoft.com/en-us/azure/dns/dns-web-sites-custom-domain

QUESTION: 198 **Exam Topic: Manage Azure identities and governance questions**

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 an 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(s): A

Explanation:
You need to create a name server (NS) record for the zone.

Reference:
https://docs.microsoft.com/en-us/azure/dns/delegate-subdomain

QUESTION: 199 **Exam Topic: Manage Azure identities and governance questions**

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(s): C

Explanation:
When you delete a resource group, all of its resources are also deleted. Deleting a resource group deletes all of its template deployments and currently stored operations.

Reference:
https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/delete-resource-group?tabs=azure-powershell

QUESTION: 200 **Exam Topic: Manage Azure identities and governance questions**

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(s): A

Explanation:
Managed identities for Azure resources provides Azure services with an automatically managed identity in Azure Active Directory. You can use this identity to authenticate to any service that supports Azure AD authentication, without having credentials in your code.

You can enable and disable the system-assigned managed identity for VM using the Azure portal.

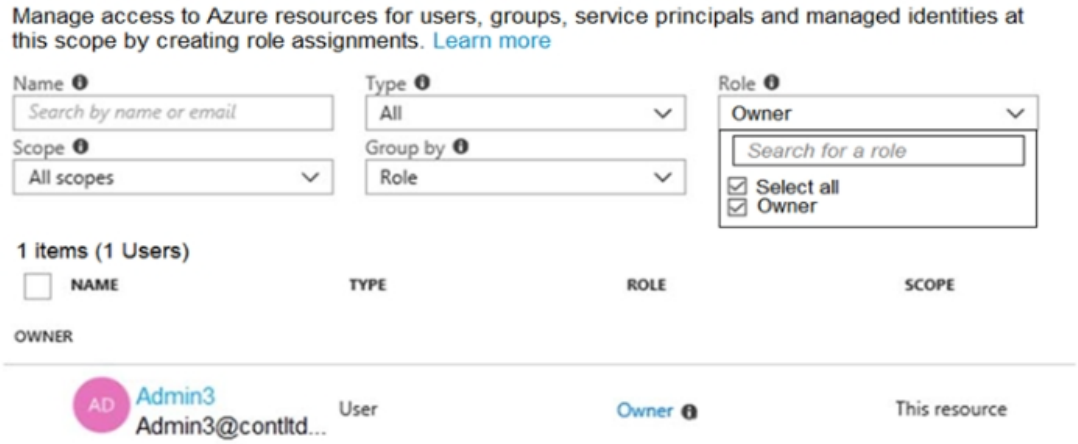
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/qs-configure-portal-windows-vm

QUESTION: 201 **Exam Topic: Manage Azure identities and governance questions**

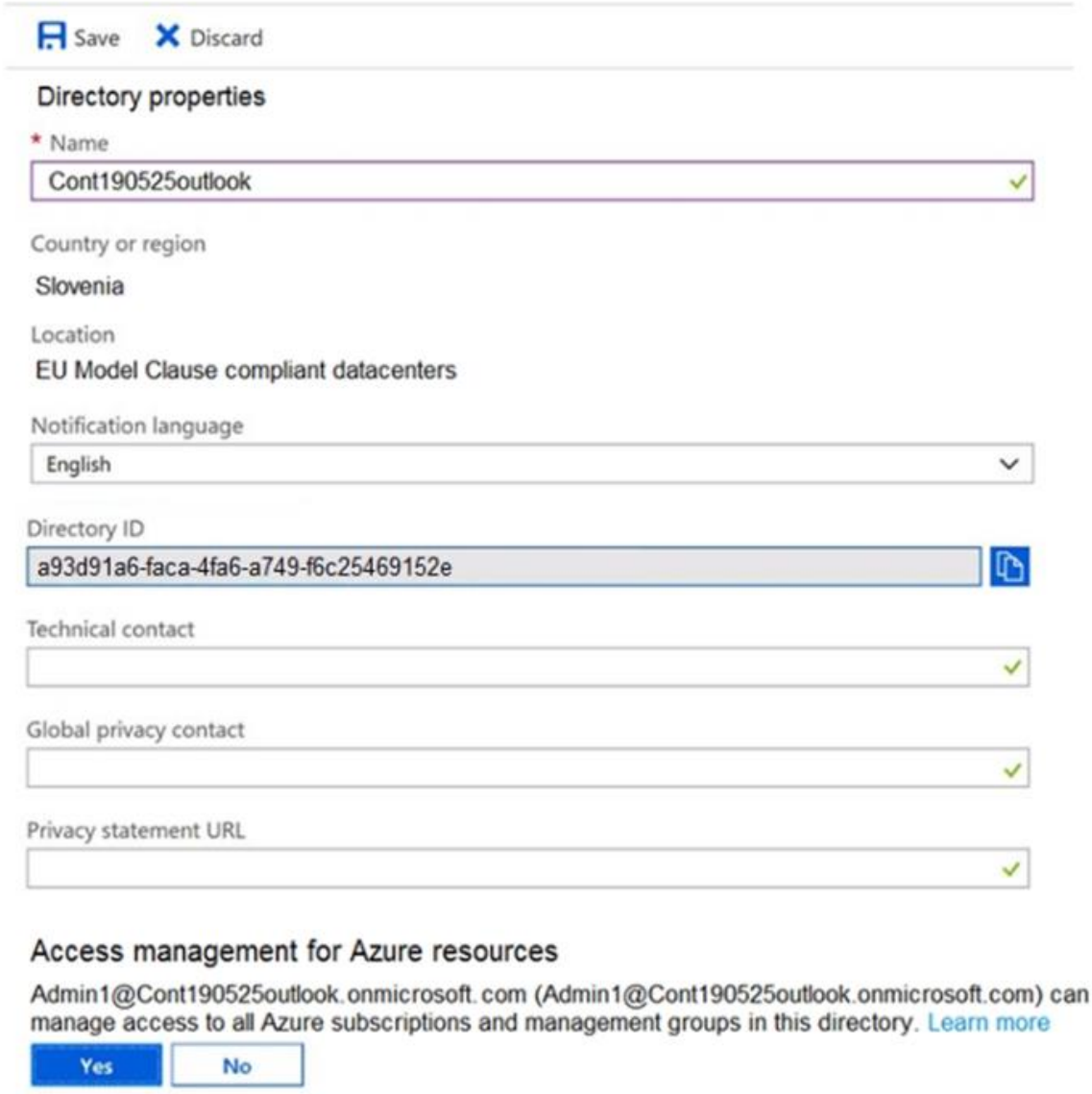
HOTSPOT

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.)


Save
Discard
Directory properties
* Name
Cont190525outlook
Country or region
Slovenia
Location
EU Model Clause compliant datacenters
Notification language
English
Directory ID
a93d91a6-faca-4fa6-a749-f6c25469152e
Technical contact
Global privacy contact
Privacy statement URL
Access management for Azure resources
Admin1@Cont190525outlook.onmicrosoft.com (Admin1@Cont190525outlook.onmicrosoft.com) can manage access to all Azure subscriptions and management groups in this directory. Learn more
Yes
No

For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.
Hot Area:

Answer Area

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

A See Explanation section for answer.

Answer(s): A

Answer(s): A

Explanation:

Answer Area

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

Box 1: No
Only Admin3, the owner, can assign ownership. Box 2: Yes
Box 3: No

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

QUESTION: 202 **Exam Topic: Manage Azure identities and governance questions**

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

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

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

A Owner

B Virtual Machine Contributor

C Contributor

D Virtual Machine Administrator Login

Answer(s): B

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

Incorrect Answers:
A: Owner: Grants full access to manage all resources, including the ability to assign roles in Azure RBAC. C: Contributor: Grants full access to manage all resources, but does not allow you to assign roles in Azure RBAC.
D: Virtual Machine Administrator Login: View Virtual Machines in the portal and login as administrator.

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

QUESTION: 203 **Exam Topic: Manage Azure identities and governance questions**

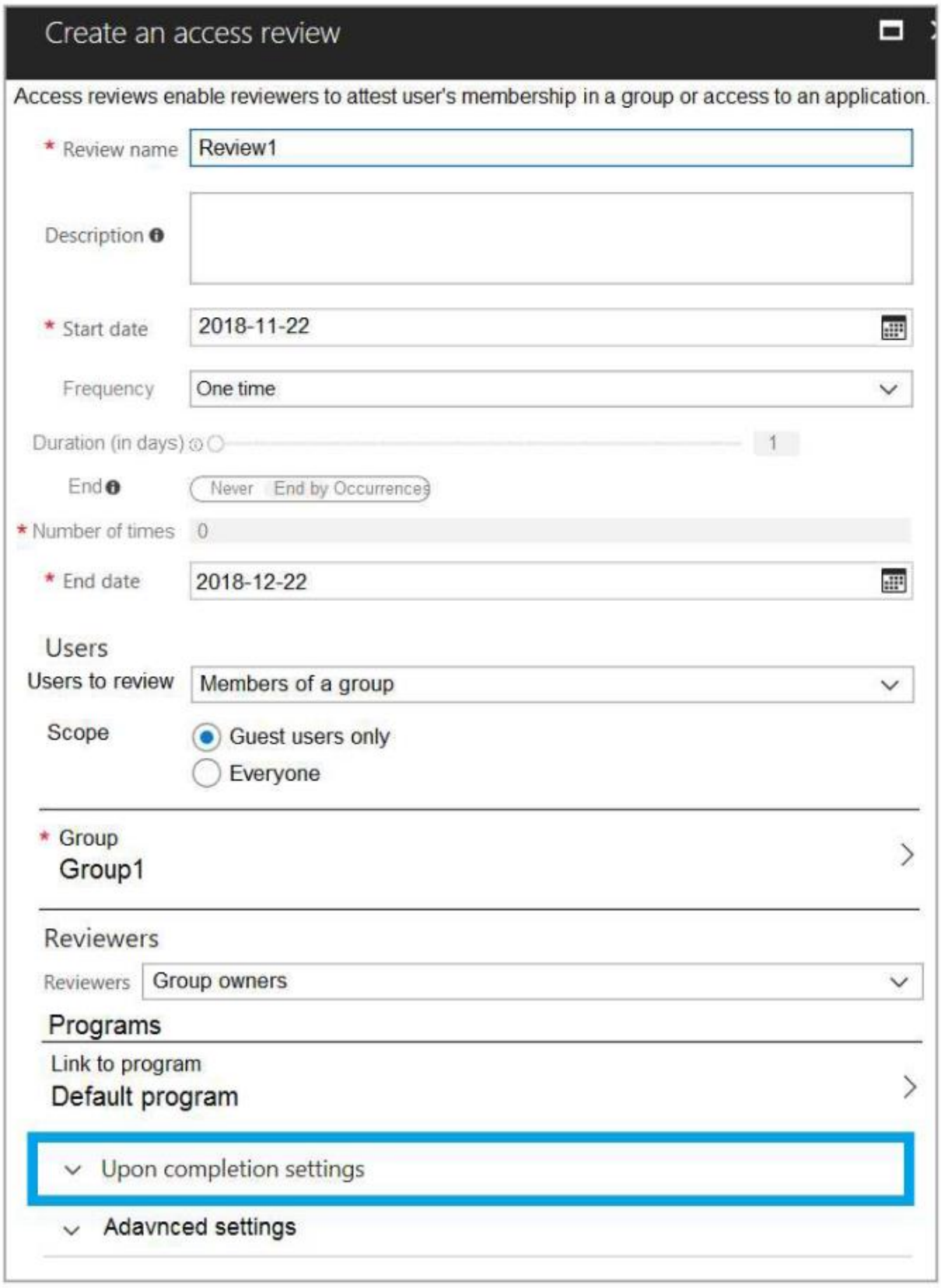
HOTSPOT

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

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

User3 is the owner of Group1. Group2 is a member of Group1.

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


Create an access review
Access reviews enable reviewers to attest user's membership in a group or access to an application.
* Review name
Review1
Description
* Start date
2018-11-22
Frequency
One time
Duration (in days)
1
End
Never
End by Occurrences
* Number of times
0
* End date
2018-12-22
Users
Users to review
Members of a group
Scope
Guest users only
Everyone
* Group
Group1
Reviewers
Reviewers
Group owners
Programs
Link to program
Default program
Upon completion settings
Adavnced settings

For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.
Hot Area:

Answer Area

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

A See Explanation section for answer.

Answer(s): A

Explanation:

Answer Area

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

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

QUESTION: 204 **Exam Topic: Manage Azure identities and governance questions**

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

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

Solution: You assign the Reader role at the subscription level to Admin1.
Does this meet the goal?

A Yes

B No

Answer(s): A

Explanation:
Your account must meet one of the following to enable traffic analytics:
Your account must have any one of the following Azure roles at the subscription scope: owner, contributor, reader, or network contributor.

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

QUESTION: 205 **Exam Topic: Manage Azure identities and governance questions**

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

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

Solution: You assign the Network Contributor role at the subscription level to Admin1.
Does this meet the goal?

A Yes

B No

Answer(s): A

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

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

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

QUESTION: 206 **Exam Topic: Manage Azure identities and governance questions**

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

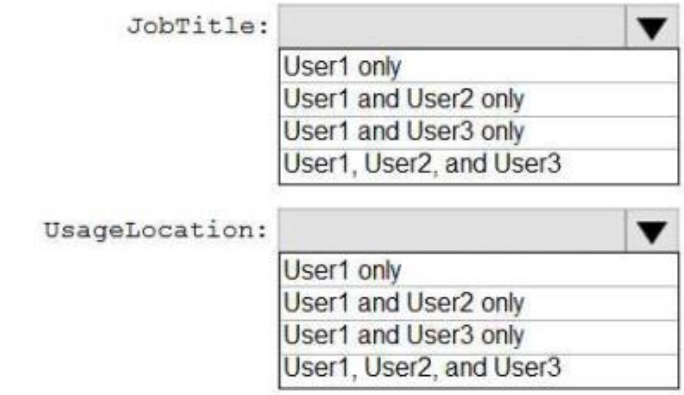
Name	Type	Source
User1	Member	Azure AD
User2	Member	Windows Server Active Directory
User3	Guest	Microsoft account

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

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

NOTE: Each correct selection is worth one point.
Hot Area:

Answer Area

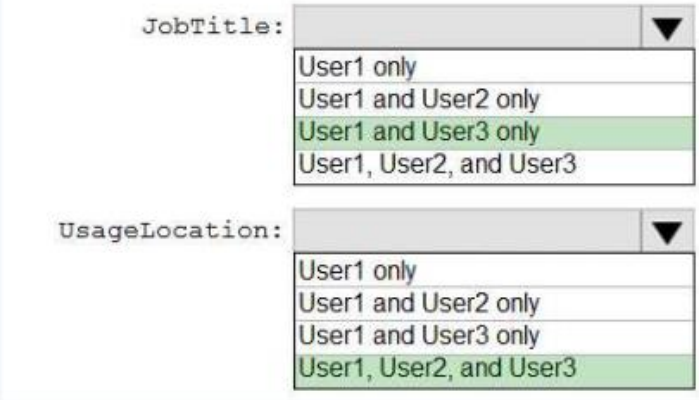


A See Explanation section for answer.

Answer(s): A

Explanation:

Answer Area



Box 1: User1 and User3 only

You must use Windows Server Active Directory to update the identity, contact info, or job info for users whose source of authority is Windows Server Active Directory.
Box 2: User1, User2, and User3

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

QUESTION: 207 **Exam Topic: Manage Azure identities and governance questions**

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

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

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

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

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

NOTE: Each correct selection is worth one point.
Hot Area:

Answer Area

User1:

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

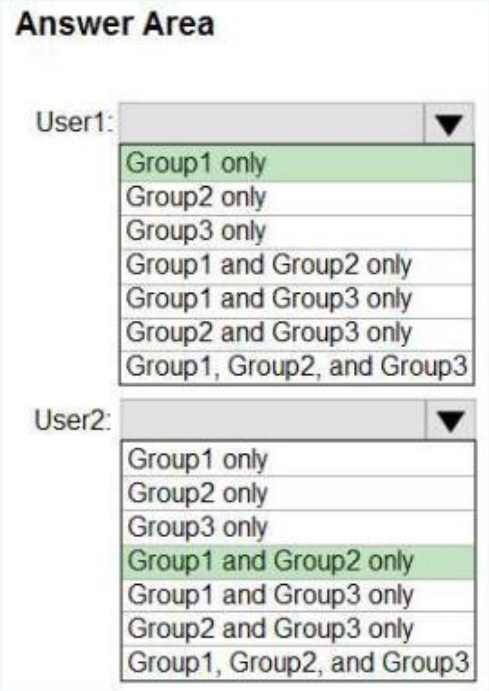
User2:

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

A See Explanation section for answer.

Answer(s): A

Explanation:



Box 1: Group 1 only First rule applies

Box 2: Group1 and Group2 only Both membership rules apply.

Reference:

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

QUESTION: 208 **Exam Topic: Manage Azure identities and governance questions**

You have an Azure subscription that contains 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(s): B

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

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

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

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

QUESTION: 209 **Exam Topic: Manage Azure identities and governance questions**

You have an Azure Active Directory (Azure AD) tenant named contoso.onmicrosoft.com. The User administrator role is assigned to a user named Admin1.
An external partner has a Microsoft account that uses the user1@outlook.com sign in.

Admin1 attempts to invite the external partner to sign in to the Azure AD tenant and receives the following error message: "Unable to invite user user1@outlook.com – Generic authorization exception."

You need to ensure that Admin1 can invite the external partner to sign in to the Azure AD tenant.
What should you do?

A From the Users blade, modify the External collaboration settings.

B From the Custom domain names blade, add a custom domain.

C From the Organizational relationships blade, add an identity provider.

D From the Roles and administrators blade, assign the Security administrator role to Admin1.

Answer(s): A

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

QUESTION: 210 **Exam Topic: Manage Azure identities and governance questions**

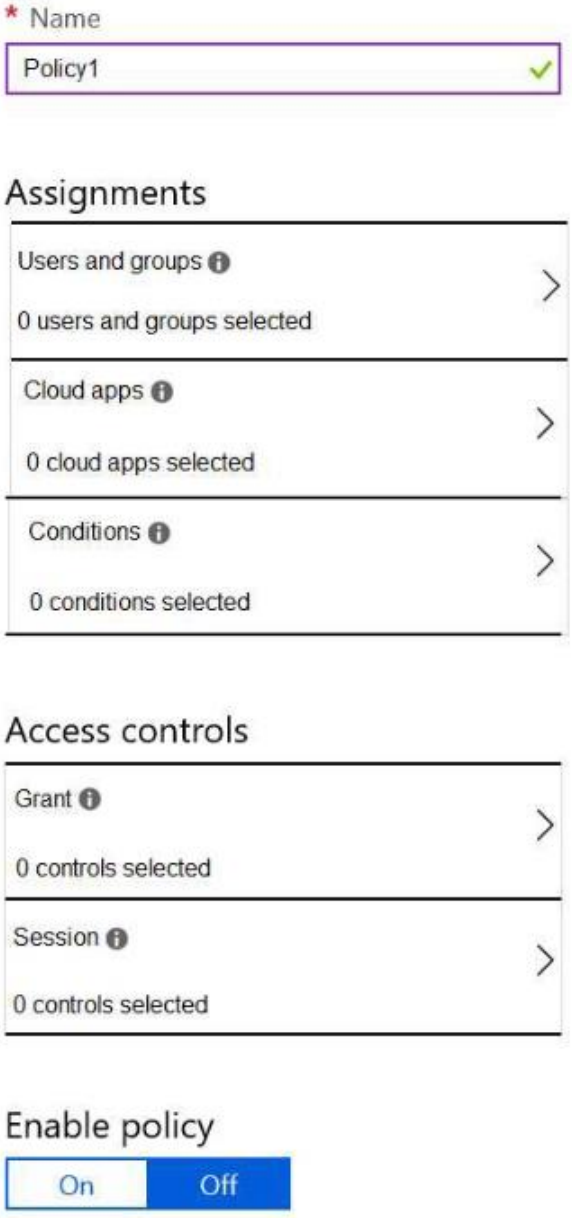
HOTSPOT
You have an Azure Active Directory (Azure AD) tenant.

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

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

NOTE: Each correct selection is worth one point.
Hot Area:

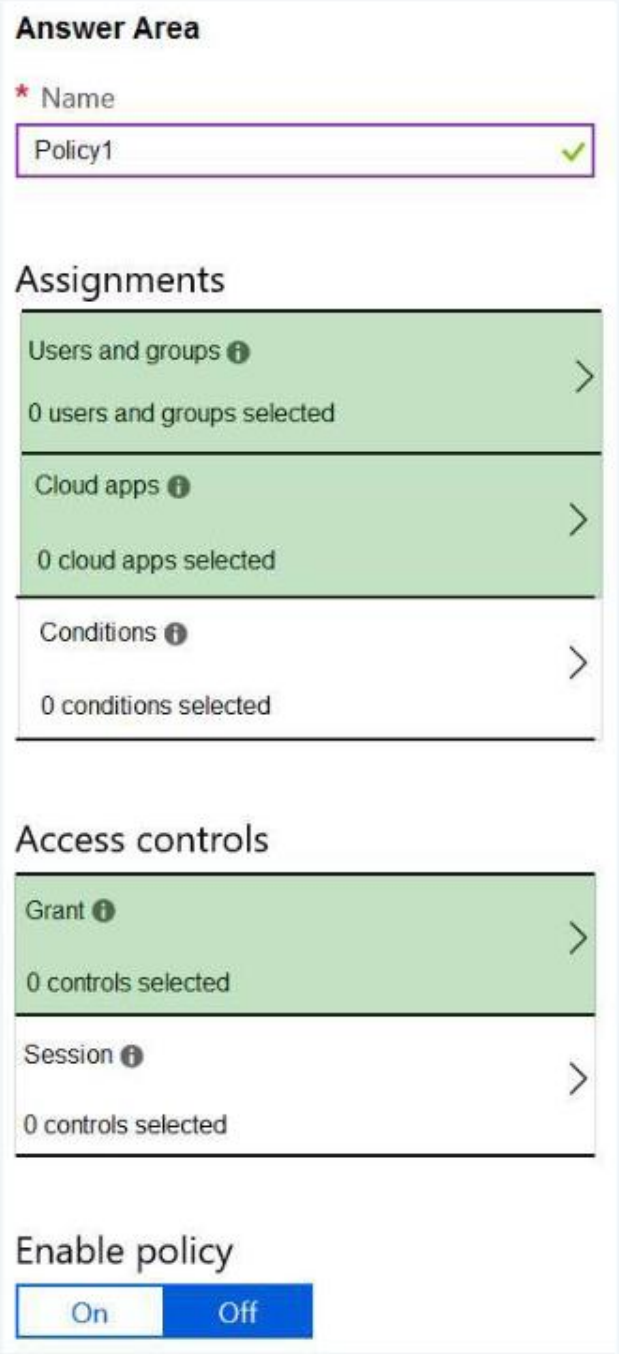
Answer Area



A See Explanation section for answer.

Answer(s): A

Explanation:



Reference:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/app-based-mfa

QUESTION: 211 **Exam Topic: Manage Azure identities and governance questions**

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(s): B

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

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

QUESTION: 212 **Exam Topic: Manage Azure identities and governance questions**

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(s): A,E

Answer(s): A,E

Explanation:
Network traffic from the VPN gateway is routed to the cloud application through an internal load balancer. The load balancer is located in the front-end subnet of the application.

Reference:
https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/hybrid-networking/vpn
https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-overview
https://docs.microsoft.com/en-us/azure/application-gateway/overview

QUESTION: 213 **Exam Topic: Manage Azure identities and governance questions**

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

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

Solution: You assign the Owner role at the subscription level to Admin1.
Does this meet the goal?

A Yes

B No

Answer(s): A

Explanation:
Your account must meet one of the following to enable traffic analytics:
Your account must have any one of the following Azure roles at the subscription scope: owner, contributor, reader, or network contributor.

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

QUESTION: 214 **Exam Topic: Manage Azure identities and governance questions**

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.

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.	○	○

A See Explanation section for answer.

Answer(s): A

Explanation:

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.	○	○

Reference:
https://docs.microsoft.com/en-us/azure/storage/files/storage-files-identity-ad-ds-assign-permissions?tabs=azure-portal

QUESTION: 215 **Exam Topic: Manage Azure identities and governance questions**

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

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

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

Which two groups should you create? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

A an Office 365 group that uses the Assigned membership type

B a Security group that uses the Assigned membership type

C an Office 365 group that uses the Dynamic User membership type

D a Security group that uses the Dynamic User membership type

E a Security group that uses the Dynamic Device membership type

Answer(s): A,C

Answer(s): A,C

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

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

When a group expires, all of its associated services (the mailbox, Planner, SharePoint site, etc.) are also deleted.
You can set up a rule for dynamic membership on security groups or Office 365 groups.
Incorrect Answers:
B, D, E: You can set expiration policy only for Office 365 groups in Azure Active Directory (Azure AD).

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

QUESTION: 216 **Exam Topic: Manage Azure identities and governance questions**

HOTSPOT
You have an Azure subscription named Subscription1 that contains a resource group named RG1. In RG1, you create an internal load balancer named LB1 and a public load balancer named LB2.
You need to ensure that an administrator named Admin1 can manage LB1 and LB2. The solution must follow the principle of least privilege.

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

NOTE: Each correct selection is worth one point.
Hot Area:

Answer Area

To add a backend pool to LB1:

- Contributor on LB1
- Network Contributor on LB1
- Network Contributor on RG1
- Owner on LB1

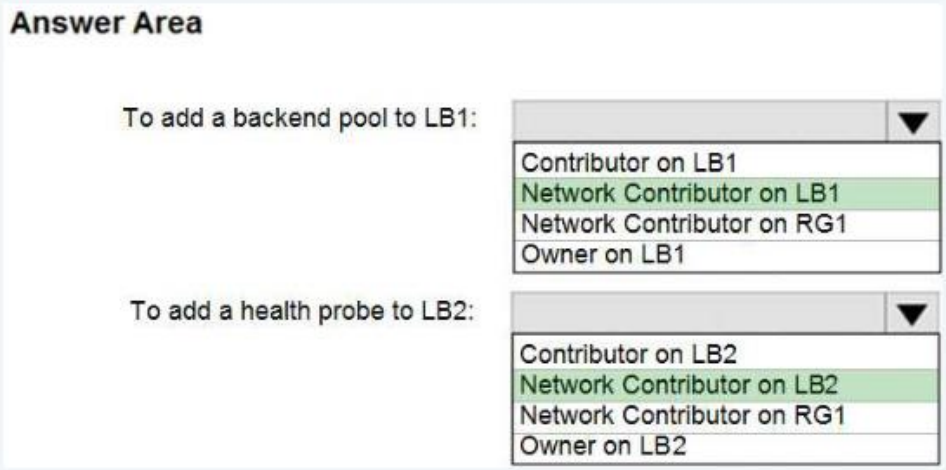
To add a health probe to LB2:

- Contributor on LB2
- Network Contributor on LB2
- Network Contributor on RG1
- Owner on LB2

A See Explanation section for answer.

Answer(s): A

Explanation:



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

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

QUESTION: 238 **Exam Topic: Manage Azure identities and governance questions**

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

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

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

User1 creates a new Azure Active Directory tenant named external.contoso.onmicrosoft.com. You need to create new user accounts in external.contoso.onmicrosoft.com.
Solution: You instruct User3 to create the user accounts.

Does that meet the goal?

A Yes

B No

Answer(s): B

Explanation:
Only a global administrator can add users to this tenant.

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

QUESTION: 239 **Exam Topic: Manage Azure identities and governance questions**

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

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

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

User1 creates a new Azure Active Directory tenant named external.contoso.onmicrosoft.com. You need to create new user accounts in external.contoso.onmicrosoft.com.
Solution: You instruct User4 to create the user accounts.
Does that meet the goal?

A Yes

B No

Answer(s): B

Explanation:
Only a global administrator can add users to this tenant.

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

QUESTION: 240 **Exam Topic: Manage Azure identities and governance questions**

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

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

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

User1 creates a new Azure Active Directory tenant named external.contoso.onmicrosoft.com.
You need to create new user accounts in external.contoso.onmicrosoft.com.
Solution: You instruct User2 to create the user accounts.
Does that meet the goal?

A Yes

B No

Answer(s): A

Explanation:
Only a global administrator can add users to this tenant.

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

QUESTION: 246 **Exam Topic: Manage Azure identities and governance questions**

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

An administrator reports that she is unable to grant access to AKS1 to the users in contoso.com.
You need to ensure that access to AKS1 can be granted to the contoso.com users.
What should you do first?

A. From contoso.com, modify the Organization relationships settings.

B. From contoso.com, create an OAuth 2.0 authorization endpoint.

C. Recreate AKS1.

D. From AKS1, create a namespace.

Answer(s): B

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

QUESTION: 257 **Exam Topic: Manage Azure identities and governance questions**

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.

Answer Area

Add a subnet to VNet1:

- User1 only
- User3 only
- User1 and User3 only
- User2 and User3 only
- User1, User2, and User3

Assign a user the Reader role to VNet1:

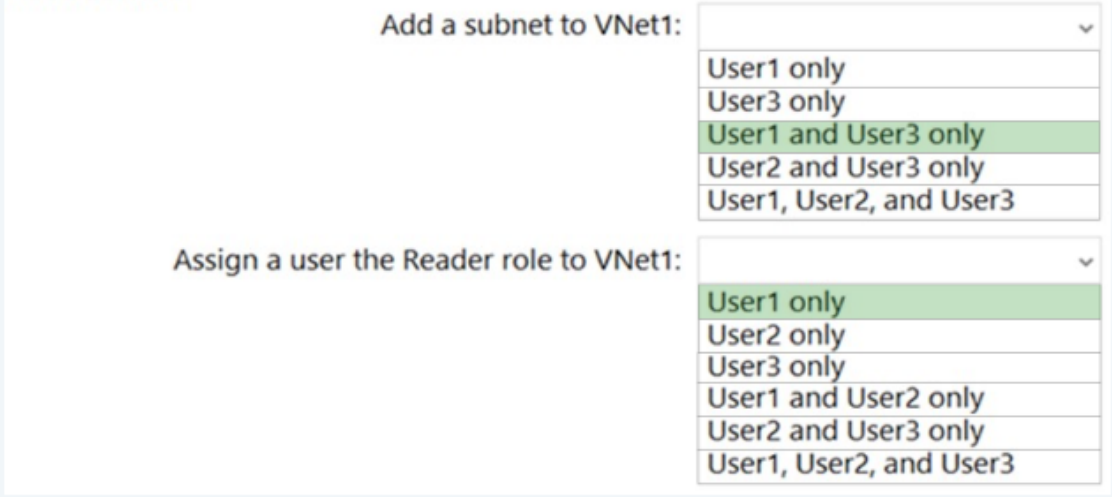
- User1 only
- User2 only
- User3 only
- User1 and User2 only
- User2 and User3 only
- User1, User2, and User3

A See Explanation section for answer.

Answer(s): A

Explanation:

Answer Area



Box 1: User1 and User3 only.

User1: The Owner Role lets you manage everything, including access to resources.

User3: The Network Contributor role lets you manage networks, including creating subnets.

Box 2: User1 only.

The Security Admin role: In Security Center only: Can view security policies, view security states, edit security policies, view alerts and recommendations, dismiss alerts and recommendations.

Reference:

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

https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftnetwork

QUESTION: 258 **Exam Topic: Manage Azure identities and governance questions**

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 area.
NOTE: Each correct selection is worth one point.
Hot Area:

Answer Area

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

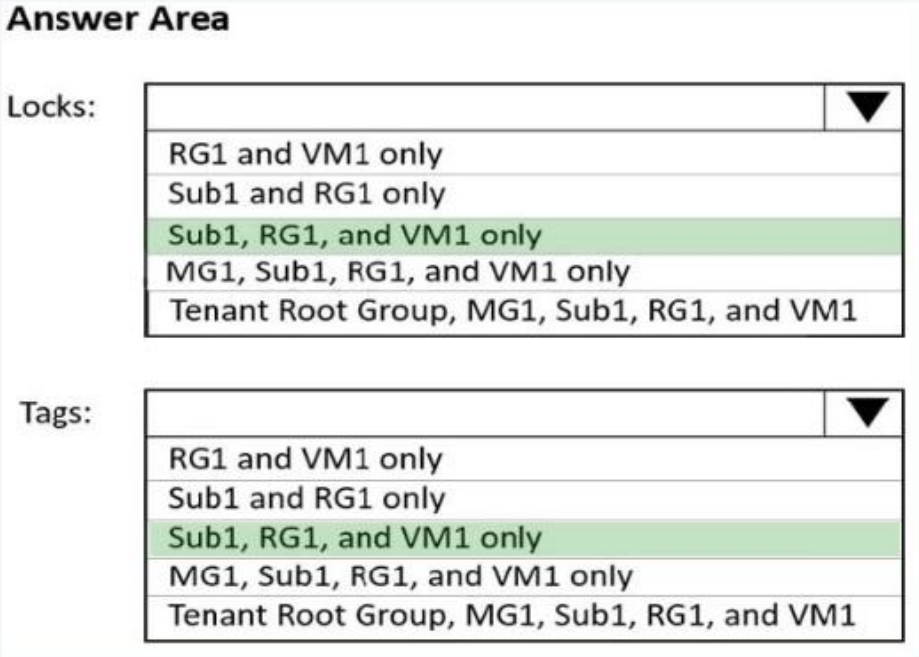
Tags:

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

A See Explanation section for answer.

Answer(s): A

Explanation:



Box 1: Sub1, RG1, and VM1 only

You can lock a subscription, resource group, or resource to prevent other users in your organization from accidentally deleting or modifying critical resources.

Box 2: Sub1, RG1, and VM1 only

You apply tags to your Azure resources, resource groups, and subscriptions.

Reference:

https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/lock-resources?tabs=json

https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/tag-resources?tabs=json

QUESTION: 259 **Exam Topic: Manage Azure identities and governance questions**

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(s): B

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/users-bulk-delete

QUESTION: 315 **Exam Topic: Manage Azure identities and governance questions**

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

☐Reader Security Admin
☐Security Reader

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

A Remove User1 from the Security Reader role for Subscription1. Assign User1 the Contributor role for RG1.

B Assign User1 the Owner role for VNet1.

C Assign User1 the Contributor role for VNet1.

D Assign User1 the Network Contributor role for VNet1.

Answer(s): B

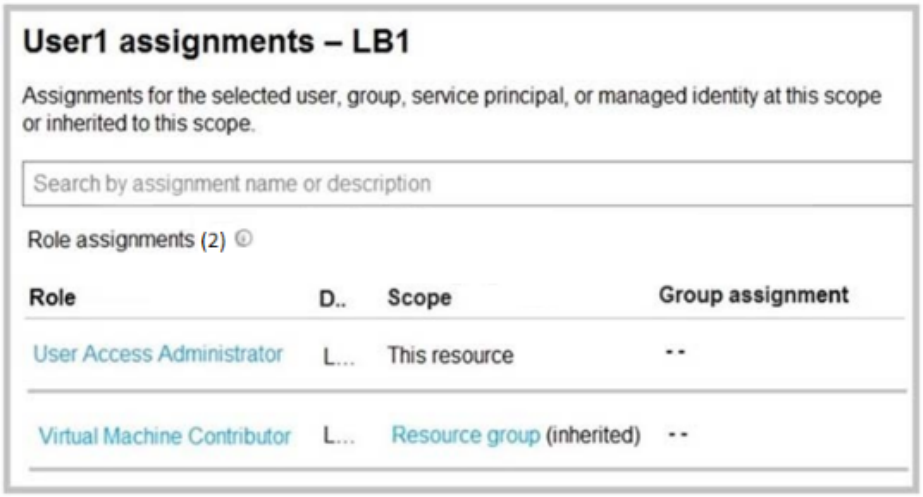
Reference:
https://docs.microsoft.com/en-us/azure/role-based-access-control/rbac-and-directory-admin-roles
https://docs.microsoft.com/en-us/azure/role-based-access-control/overview

QUESTION: 316 **Exam Topic: Manage Azure identities and governance questions**

HOTSPOT

You have an Azure Load Balancer named LB1.

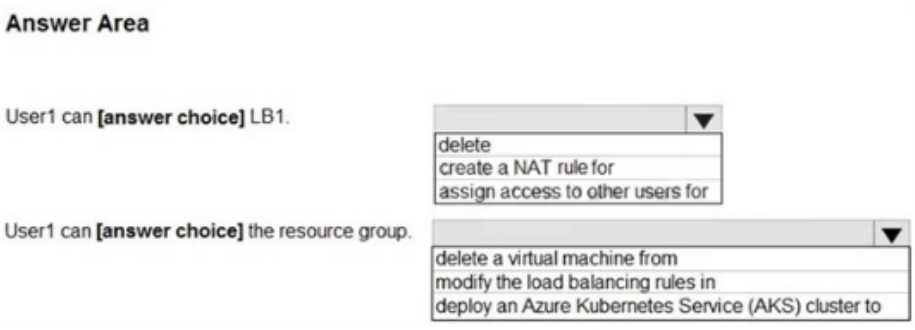
You assign a user named User1 the roles shown in the following exhibit.



Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Hot Area:



A See Explanation section for answer.

Answer(s): A

Explanation:

Reference:

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

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

QUESTION: 317 **Exam Topic: Manage Azure identities and governance questions**

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have an Azure Directory (Azure AD) tenant named Adatum and an Azure Subscription named Subscription1. Adatum contains a group named Developers. Subscription1 contains a resource group named Dev.
You need to provide the Developers group with the ability to create Azure logic apps in the Dev resource group.

Solution: On Dev, you assign the Logic App Contributor role to the Developers group. Does this meet the goal?

A Yes

B No

Answer(s): A

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

QUESTION: 318 **Exam Topic: Manage Azure identities and governance questions**

You have three offices and an Azure subscription that contains an Azure Active Directory (Azure AD) tenant. You need to grant user management permissions to a local administrator in each office. What should you use?

A Azure AD roles

B administrative units

C access packages in Azure AD entitlement management

D Azure roles

Answer(s): B

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/roles/administrative-units

QUESTION: 319 **Exam Topic: Manage Azure identities and governance questions**

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You need to ensure that an Azure Active Directory (Azure AD) user named Admin1 is assigned the required role to enable Traffic Analytics for an Azure subscription.
Solution: You assign the Traffic Manager Contributor role at the subscription level to Admin1. Does this meet the goal?

(A) Yes

(B) No

Answer(s): B

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

QUESTION: 320 **Exam Topic: Manage Azure identities and governance questions**

HOTSPOT
You have an Azure subscription named Sub1 that contains the Azure resources shown in the following table.

Name	Type
RG1	Resource group
storage1	Storage account
VNET1	Virtual network

You assign an Azure policy that has the following settings:
Scope: Sub1
Exclusions: Sub1/RG1/VNET1
Policy definition: Append a tag and its value to resources
Policy enforcement: Enabled
Tag name: Tag4
Tag value: value4

You assign tags to the resources as shown in the following table.

Resource	Tag
Sub1	Tag1:subscription
RG1	Tag2:IT
storage1	Tag3:value1
VNET1	Tag3:value2

For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.
Hot Area:

Answer Area

Statements	Yes	No
RG1 has the `Tag2:IT` tag assigned only	◯	◯
Storage1 has the `Tag1:subscription`, `Tag2:IT`, `Tag3:value1`, and `Tag4:value4` tags assigned.	◯	◯
VNET1 has the `Tag2:IT` and `Tag3:value2` tags assigned only	◯	◯

A See Explanation section for answer.

Answer(s): A

Explanation:

Answer Area

Statements	Yes	No
RG1 has the `Tag2:IT` tag assigned only	◯	◯
Storage1 has the `Tag1:subscription`, `Tag2:IT`, `Tag3:value1`, and `Tag4:value4` tags assigned.	◯	◯
VNET1 has the `Tag2:IT` and `Tag3:value2` tags assigned only	◯	◯

Box 1: No

The Azure Policy will add Tag4 to RG1. Box 2: No

Tags applied to the resource group or subscription aren't inherited by the resources although you can enable inheritance with Azure Policy. Storage1 has Tag3: Value1 and the Azure Policy will add Tag4.

Box 3: No

Tags applied to the resource group or subscription aren't inherited by the resources so VNET1 does not have Tag2.

VNET1 has Tag3:value2. VNET1 is excluded from the Azure Policy so Tag4 will not be added to VNET1.

QUESTION: 313 **Exam Topic: Manage Azure identities and governance**

You need to meet the user requirement for Admin1. What should you do?

A. From the Azure Active Directory blade, modify the Groups

B. From the Azure Active Directory blade, modify the Properties

C. From the Subscriptions blade, select the subscription, and then modify the Access control (IAM) settings

D. From the Subscriptions blade, select the subscription, and then modify the Properties

Answer(s): D

Explanation:
Scenario:
- Designate a new user named Admin1 as the service admin for the Azure subscription.
- Admin1 must receive email alerts regarding service outages.

Follow these steps to change the Service Administrator in the Azure portal.
1. Make sure your scenario is supported by checking the limitations for changing the Service Administrator.
2. Sign in to the Azure portal as the Account Administrator.
3. Open Cost Management + Billing and select a subscription.
4. In the left navigation, click Properties.
5. Click Service Admin.

Reference:
https://docs.microsoft.com/en-us/azure/role-based-access-control/classic-administrators

Testlet 3

Case study
This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study
To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview

General Overview
Contoso, Ltd. is a consulting company that has a main office in Montreal and branch offices in Seattle and New York.

Environment

Existing Environment

Contoso has an Azure subscription named Sub1 that is linked to an Azure Active Directory (Azure AD) tenant.

The network contains an on-premises Active Directory domain that syncs to the Azure AD tenant.

The Azure AD tenant contains the users shown in the following table.

Name	Type	Role
User1	Member	**None**
User2	Guest	**None**
User3	Member	**None**
User4	Member	**None**

Sub1 contains two resource groups named RG1 and RG2 and the virtual networks shown in the following table.

Name	Subnet	Peered with
VNET1	Subnet1, Subnet2	VNET2
VNET2	Subnet1	VNET1, VNET3
VNET3	Subnet1	VNET2
VNET4	Subnet1	**None**

User1 manages the resources in RG1. User4 manages the resources in RG2.

Sub1 contains virtual machines that run Windows Server 2019 as shown in the following table

Name	IP address	Location	Connected to
VM1	10.0.1.4	West US	VNET1/Subnet1
VM2	10.0.2.4	West US	VNET1/Subnet2
VM3	172.16.1.4	Central US	VNET2/Subnet1
VM4	192.168.1.4	West US	VNET3/Subnet1
VM5	10.0.22.4	East US	VNET4/Subnet1

No network security groups (NSGs) are associated to the network interfaces or the subnets.

Sub1 contains the storage accounts shown in the following table.

Name	Kind	Location	File share	Identity-based access for file share
storage1	Storage (general purpose v1)	West US	sharea	Azure Active Directory Domain Services (Azure AD DS)
storage2	StorageV2 (general purpose v2)	East US	shareb, sharec	Disabled
storage3	BlobStorage	East US 2	**Not applicable**	**Not applicable**
storage4	FileStorage	Central US	shared	Azure Active Directory Domain Services (Azure AD DS)

Requirements

Planned Changes

Contoso plans to implement the following changes:

☐Create a blob container named container1 and a file share named share1 that will use the Cool storage tier.

☐Create a storage account named storage5 and configure storage replication for the Blob service.

☐Create an NSG named NSG1 that will have the custom inbound security rules shown in the following table.

Priority	Port	Protocol	Source	Destination	Action
500	3389	TCP	10.0.2.0/24	Any	Deny
1000	Any	ICMP	Any	VirtualNetwork	Allow

☐Associate NSG1 to the network interface of VM1.

☐Create an NSG named NSG2 that will have the custom outbound security rules shown in the following table.

Priority	Port	Protocol	Source	Destination	Action
200	3389	TCP	10.0.0.0/16	VirtualNetwork	Deny
400	Any	ICMP	10.0.2.0/24	10.0.1.0/24	Allow

☐Associate NSG2 to VNET1/Subnet2.

Technical Requirements

Contoso must meet the following technical requirements:

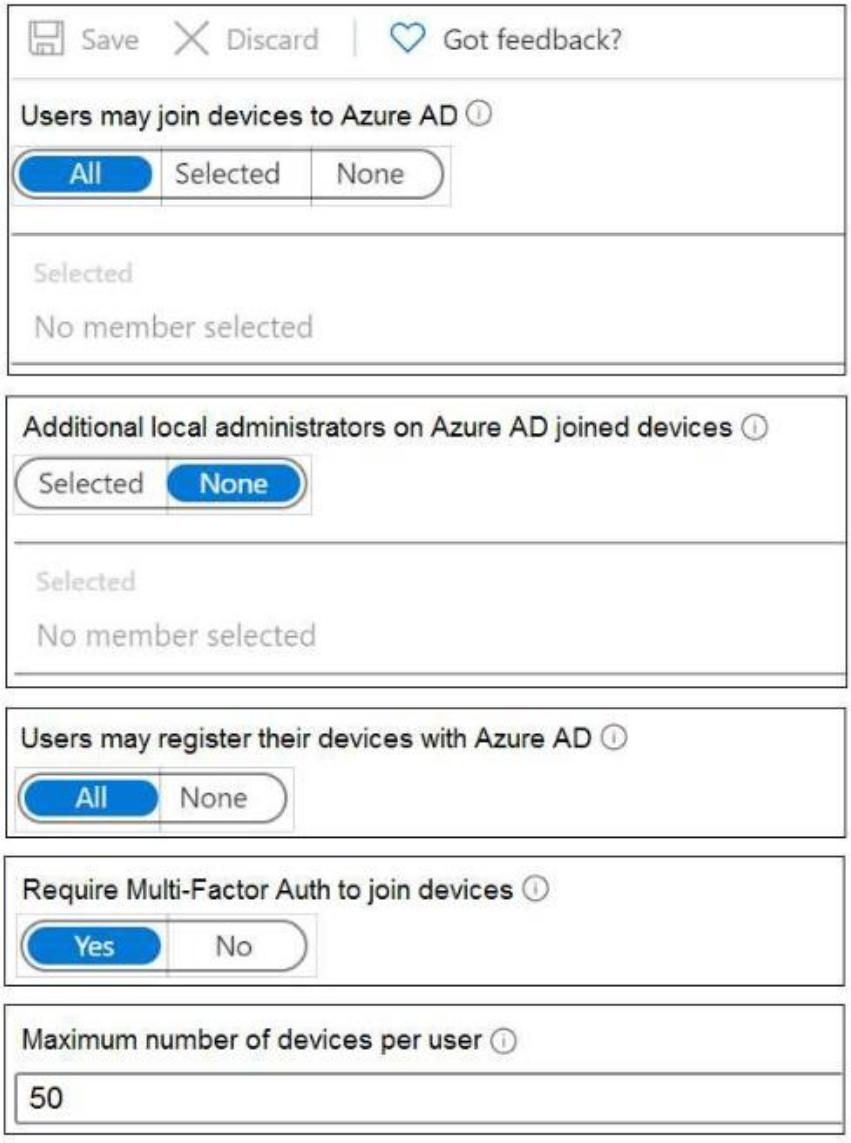
- Create container1 and share1.
- Use the principle of least privilege.
- Create an Azure AD security group named Group4.
- Back up the Azure file shares and virtual machines by using Azure Backup.
- Trigger an alert if VM1 or VM2 has less than 20 GB of free space on volume C.
- Enable User1 to create Azure policy definitions and User2 to assign Azure policies to RG1.
- Create an internal Basic Azure Load Balancer named LB1 and connect the load balancer to VNET1/Subnet1
- Enable flow logging for IP traffic from VM5 and retain the flow logs for a period of eight months.
- Whenever possible, grant Group4 Azure role-based access control (Azure RBAC) read-only permissions to the Azure file shares.

QUESTION: 314 **Exam Topic: Manage Azure identities and governance**

HOTSPOT
You need to configure the Device settings to meet the technical requirements and the user requirements. Which two settings should you modify? To answer, select the appropriate settings in the answer area.

Hot Area:

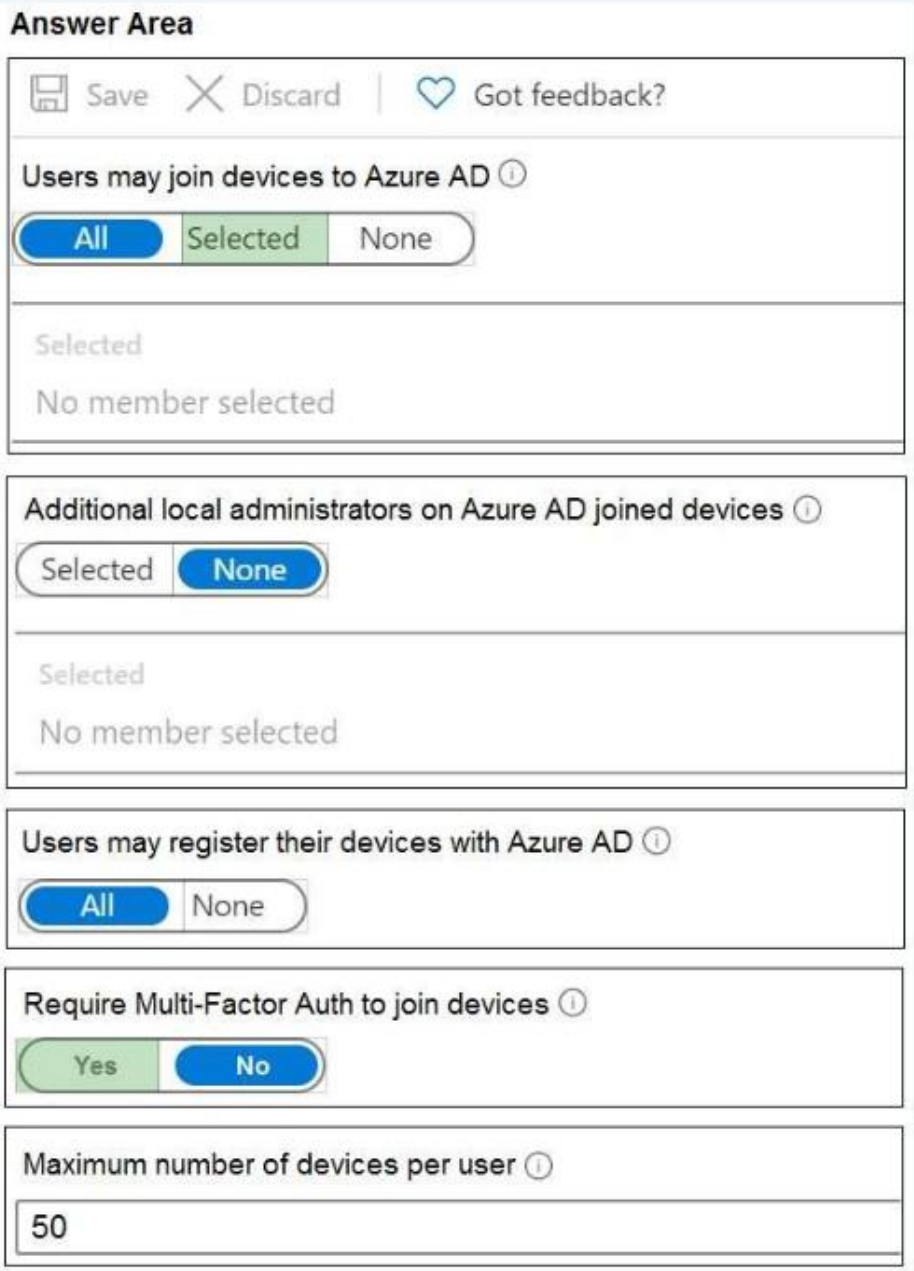
Answer Area



A See Explanation section for answer.

Answer(s): A

Explanation:



Box 1: Selected
Only selected users should be able to join devices

Box 2: Yes
Ensure that when users join devices to Azure Active Directory (Azure AD), the users use a mobile phone to verify their identity.