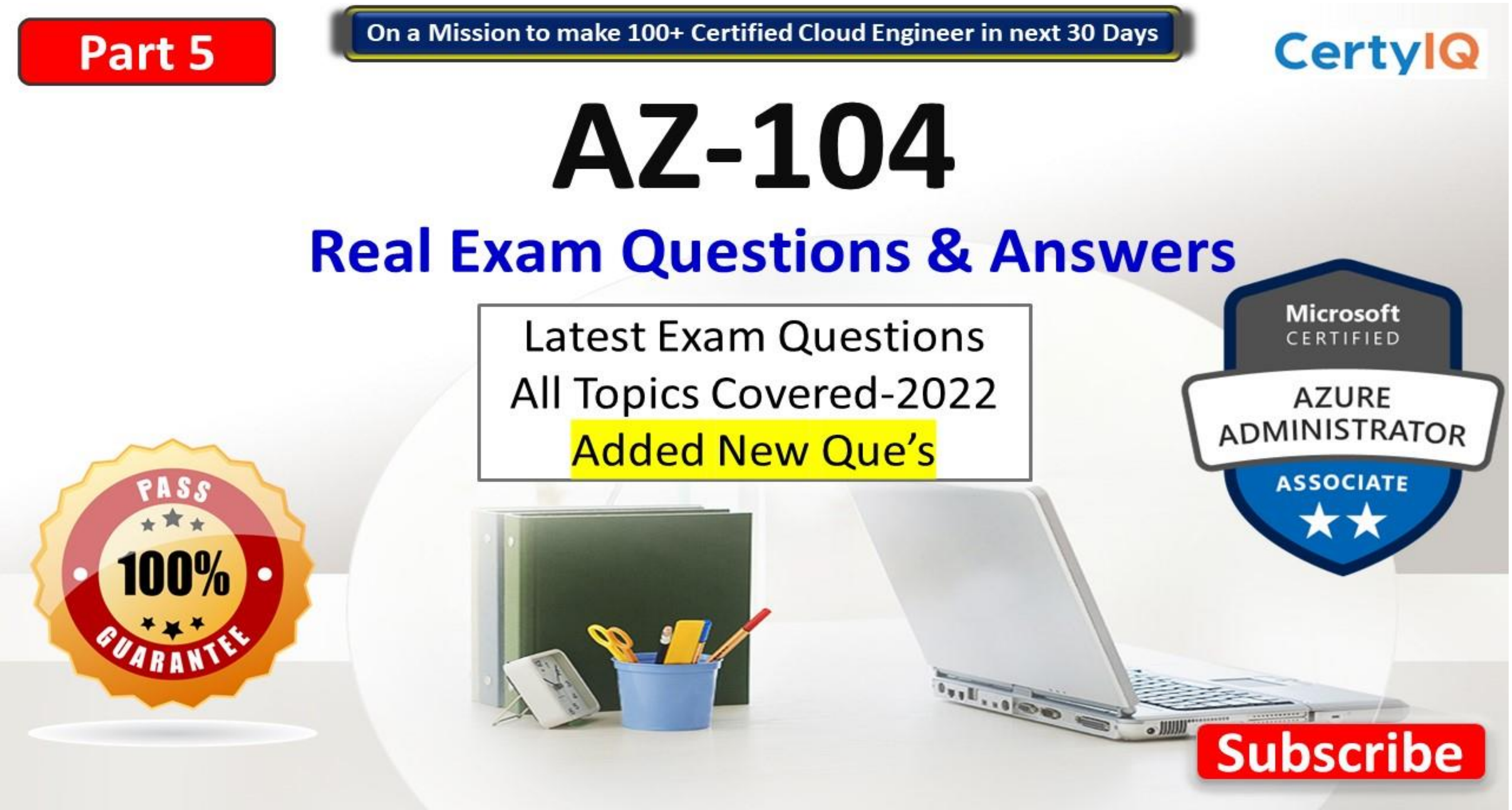


Question 161

CertyIQ

Your Azure subscription has multiple resource groups that host project-level resources. All team members that use the subscription have contributor access at the subscription level and are allowed to manage resources for all projects.

The company1-network-rg resource group contains all the network resources like virtual networks (VNets), network security groups (NSGs), DNS zones, and route tables. As the need arises, network administrators will add new DNS entries and routes, and create additional subnets and NSGs.

You need to ensure that no team members, including the network administrators, delete any resources hosted in the company1-network-rg resource group. You must implement a solution that requires minimal ongoing administrative effort.

What should you do?

Choose the correct answer

A. Apply a CanNotDelete lock to the company1-network-rg resource group.

B. Create a custom role that denies delete for the company1-network-rg resource group. Apply the role to a security group and add all users to that group.

C. Create a custom role that denies delete for VNet, NSG, DNS zones, and route table type resources. Apply the role to a security group and add all users to that group.

D. Apply a ReadOnly lock to the company1-network-rg resource group.

Explanation:

You should apply a CanNotDelete lock on the company1-network-rg resource group. This lock prevents the deletion of resources from the resource group, but it still lets you make changes to the resources within the group. The requirement states that you would want to add additional network resources to the group.

You should not create a custom role preventing the deletion of network resources. A custom role preventing the deletion of network resources would mean that users would not be allowed to delete resources from any resource group. In this case, they should only be prevented from deleting resources in the company1 network-rg resource group.

You should not apply a ReadOnly lock. A ReadOnly lock would prevent the addition of more resources to the resource group. In this case, the requirement is to allow adding more resources to the group.

You should not create a custom role preventing the deletion of resource groups. This would not prevent the deletion of resources in the resource group.

Question 162 CertyIQ

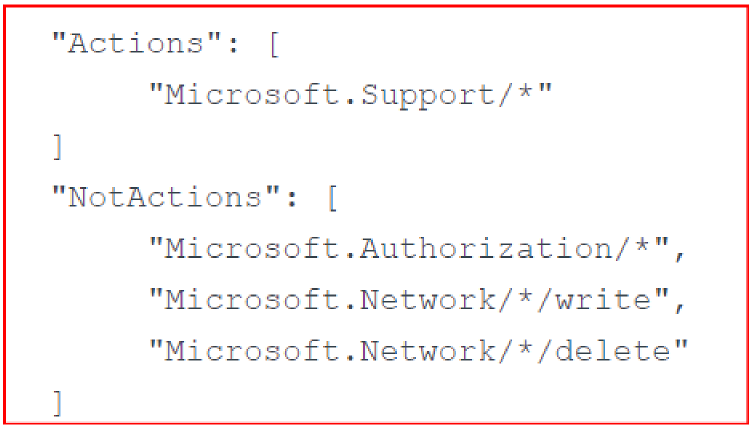
You need to create a custom role that grants the following permissions to the users and groups where the role is applied:

- Read all network resources.
- Do not allow the network resources to be modified.
- Create and manage support requests from Microsoft Support.
- Deny modifications to permissions for other users or groups.

Which Actions and NotActions configuration should you use?

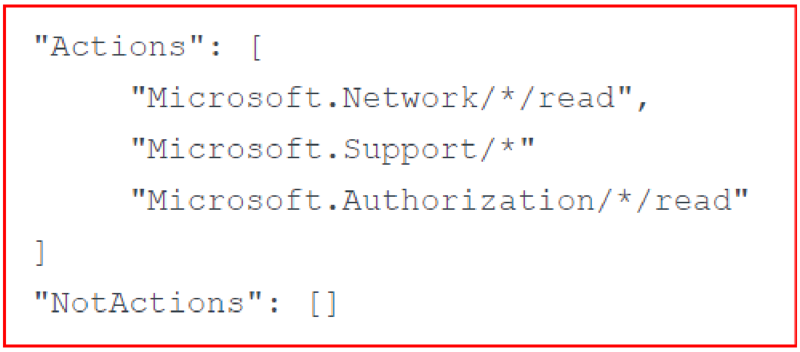
Choose the correct answer

A.



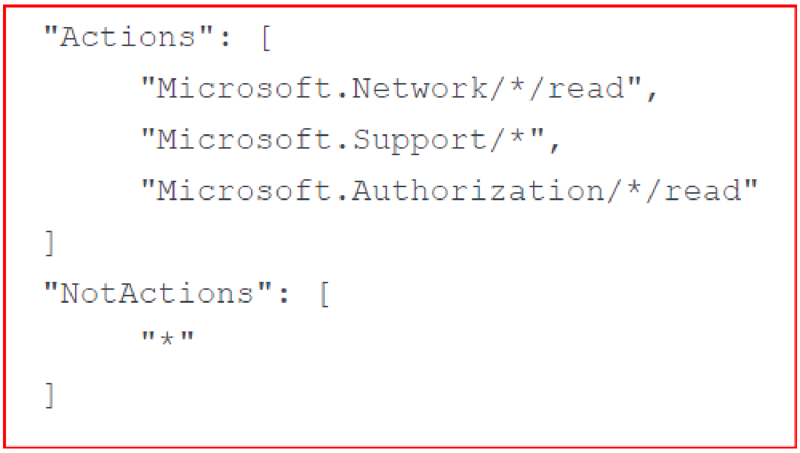
```
"Actions": [
     "Microsoft.Support/*"
]
"NotActions": [
     "Microsoft.Authorization/*",
     "Microsoft.Network/*/write",
     "Microsoft.Network/*/delete"
]
```

B.



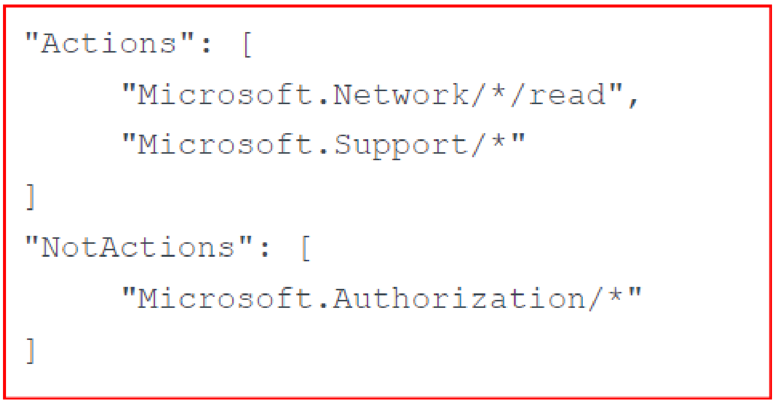
```
"Actions": [
     "Microsoft.Network/*/read",
     "Microsoft.Support/*"
     "Microsoft.Authorization/*/read"
]
"NotActions": []
```

C.



```
"Actions": [
     "Microsoft.Network/*/read",
     "Microsoft.Support/*",
     "Microsoft.Authorization/*/read"
]
"NotActions": [
     "*"
]
```

D.



```
"Actions": [
     "Microsoft.Network/*/read",
     "Microsoft.Support/*"
]
"NotActions": [
     "Microsoft.Authorization/*"
]
```

Explanation:

Correct Answer= B

You should use the following configuration:

"Actions": [

"Microsoft.Network/*/read",

"Microsoft.Support/*"

"Microsoft.Authorization/*/read"

"NotActions": []

In this configuration:

1. "Microsoft.Network/*/read" will allow read on all network resources. Microsoft.Network is the namespace for all network resources such as subnets, network security groups (NSGs), route tables, etc. The "read" action is therefore applied to all resources in the Microsoft.Network namespace.

2. "Microsoft.Support/ will allow all types of support actions. This includes the read/write/manage actions on any support requests.

3. "Microsoft.Authorization/*/read" allows read on roles and permissions assigned to users, however it will not allow them to be modified. The Microsoft.Authorization namespace hosts all the Role Based Access Control actions that a user can perform on resources. Allowing only "read" will prevent them from modifying user permissions.

Question 163 CertyIQ

Your organization owns a subscription with three resource groups named RG1, RG2, and RG3. Your on premises Active Directory has a security group named Sales Department that contains user accounts for all sales employees. You use Azure Active Directory Connect (Azure AD Connect) to synchronize your on premises Active Directory with Azure Active Directory (Azure AD).

You need to implement a solution that follows the least privilege principle and meets the following requirements:

• The Sales team should be able to read resources in RG1 and RG2 only. • The Sales team should be able to create resources in only RG1.

. The Sales team is not allowed to assign permissions to any resources in the subscription.

• The Sales team is not allowed to create additional resource groups.

Which two actions should you perform? Each correct answer presents part of the solution.

Choose the correct answers

A. Assign the built-in Owner role to the Sales Department group for the RG1 resource group.

B. Assign the built-in Contributor role to the Sales Department group for the RG1 resource group.

C. Assign the built-in Reader role to the SalesDepartment group at the subscription level.

D. Assign the built-in Contributor role to the Sales Department group at the subscription level.

E. Assign the built-in Reader role to the Sales Department group for the RG2 resource group.

Explanation:

You should assign the Reader role at the RG2 resource group and the Contributor role at the RG1 resource group level. This will allow the users in the Sales Department group to only manage resources in the RG1 resource group and read resources in RG2.

You should not assign the Contributor permissions at the subscription level. This would let the users in the Sales Department group modify resources anywhere in the subscription and create new resource groups.

You should not assign the Reader role at the subscription level. This would give read-only access to Sales Department group to all resources in the subscriptions, including the resources in RG3.

You should not assign the Owner role for RG1. This would let the Sales Department group users assign other user permissions to that resource group.

Question 164

CertyIQ

You create a Windows Server virtual machine in an Azure resource group named laas-rg. You plan to generalize the operating system and capture an image for use in future deployments.

You need to ensure that other administrators make no changes to the virtual machine configuration until you complete the image capture process. You need to enact your solution as quickly as possible.

What should you do?

Choose the correct answer

A. Set a Read-only lock at the resource group level.

B. Set a Delete lock at the VM level.

C. Edit the role-based access control (RBAC) permissions at the VM level.

D. Edit the role-based access control (RBAC) permissions at the resource group level.

Explanation:

Given that time is of the essence in this scenario, you should set a Read-only lock at the resource group level. Resource locks in Azure allow you to prevent unwanted changes to Azure resources no matter what the user's privilege level is. For example, even subscription owners would not be able to resize a virtual machine (VM) if the resource has a Read-only lock applied to it.

By setting the lock at the VM's parent resource group level, you ensure that other administrators can make no changes to the VM's entire configuration environment, including virtual network interface cards (vNIC), virtual hard disks (VHDs), and so forth.

You should not set a Delete lock at the VM level for two reasons. First, the Delete resource lock prevents only delete operations, so administrators would be able to undertake other management actions on the VM. Second, a resource-level lock does not affect related VM assets contained in the same resource group.

You should not edit the role-based access control (RBAC) permissions at either the resource group or the VM level because the scenario states that you need to enact your solution as quickly as possible.

Question 165

Your Azure subscription has resource groups for production and testing environments.

A user member of the RegularUsers group accidentally deletes the testing resource groups named TST01 RG and TSTO2-RG. TST01-RG had a storage account named STAO1 configured. TSTO2-RG had an App Service named APP01 configured.

You recover the affected resource from the backups. You then decide to implement resource locks so this will not happen again. Your manager would like the following points implemented in order to prevent this type of incident from happening again:

• No resources can be deleted by accident again.

• All resource types should work correctly after implementing the resource locks.

• Any new resource that is added to the subscription should also be protected against accidental deletion.

• The solution should require the least administrative effort.

You need to implement a solution that fulfils all the requirements above.

What should you do?

Choose the correct answer

A. Configure a Delete lock on your subscription.

B. Configure a Read-only lock on TST01-RG and TST02-RG.

C. Configure a Delete lock on TST01-RG and TST02-RG.

D. Configure a Read-only lock on your subscription.

Explanation:

You should configure a Delete lock on your subscription. You can configure locks at the subscription, resource group, and resource levels. The Delete or CanNotDelete lock prevents any resource from being deleted by accident. You still can make modifications to the resources, but you get an error if you try to remove a resource with a Delete lock. When you apply a lock on a container, like a subscription or a resource group, all children inside the container are also affected by the resource lock. This way you ensure that no other resource is deleted by accident without affecting the normal operation of the resources.

You should not configure a Read-only lock on your subscription. A Read-only or ReadOnly lock prevents users from making modifications to the attributes of the resource, although they can still make modifications to the data of the resource itself. Depending on the resource type, applying a Read-only lock may lead to unpredictable behavior. When you configure a Read-only lock in a resource, you are blocking the ability to perform any operation other than read access. There are some resources that perform operations other than reading operations when you try to perform actions that initially could seem to be read-only. For example, if you set a Read-only lock on a storage account, you are preventing users from listing the access keys of the storage account. This is because the service uses a POST request internally to list the keys because these keys are also available for writing operations.

You should not configure a Delete lock on TST01-RG and TST02-RG. This configuration protects both resource groups against accidental deletions, but it does not meet the objective of protecting all resources in the subscription, and it requires more administrative effort. Setting the Delete lock at the subscription level is more efficient and meets all the requirements.

You should not configure a Read-only lock on TST01-RG and TST02-RG. This configuration does not meet the least administrative effort requirement or the requirement that all resource types should work correctly after implementing the lock.

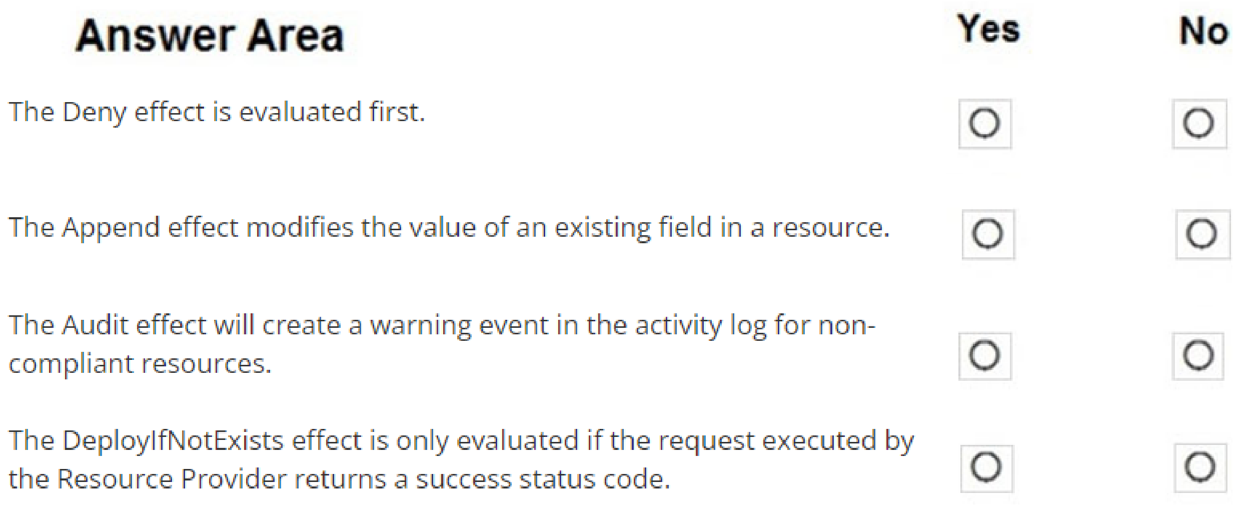
Question 166 CertyIQ

Your company requires all resources deployed in Azure to be assigned to a cost center.

You use a tag named CostCenter to assign each resource to the correct cost center. This tag has a set of valid values assigned.

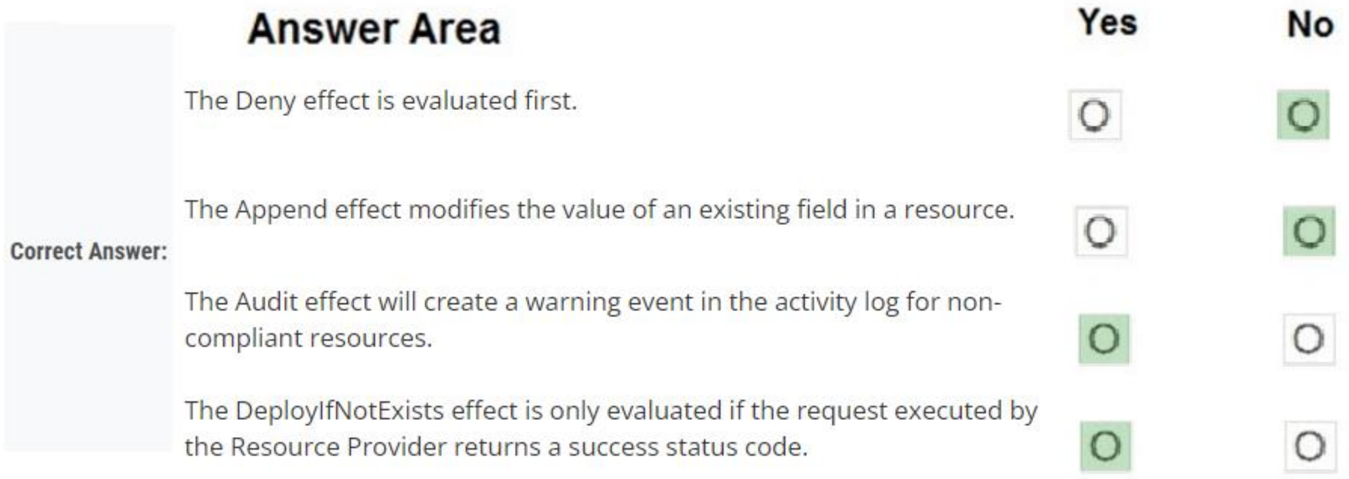
Some of the resources deployed in your subscription already have a value assigned to the CostCenter tag.

You decide to deploy a subscription policy to verify that all resources in the subscription have a valid value assigned.
For each of the following statements, select Yes if the statement is true. Otherwise, select No.



Answer Area	Yes	No
The Deny effect is evaluated first.	○	○
The Append effect modifies the value of an existing field in a resource.	○	○
The Audit effect will create a warning event in the activity log for non-compliant resources.	○	○
The DeployIfNotExists effect is only evaluated if the request executed by the Resource Provider returns a success status code.	○	○

Correct Answer:



Answer Area	Yes	No
The Deny effect is evaluated first.	○	●
The Append effect modifies the value of an existing field in a resource.	○	●
The Audit effect will create a warning event in the activity log for non-compliant resources.	●	○
The DeployIfNotExists effect is only evaluated if the request executed by the Resource Provider returns a success status code.	●	○

Explanation:

The Deny effect is not evaluated first. When a policy is evaluated, the Disabled effect is always evaluated first to decide whether the rule should be evaluated afterwards. The correct order of evaluation of the policy effects is: Disabled, Append, Deny and Audit

The Append effect does not modify the value of an existing field in a resource. The Append effect adds additional fields during the creation or update of a resource. If the field already exists in the resource and the values in the resource and the policy are different, then the policy acts as a deny and rejects the request

The Audit effect will create a warning event in the activity log for non-compliant resources. The audit effect is evaluated last, before the Resource Provider handles a create or update request. You typically use the audit effect when you want to track non-compliant resources

The DeployIfNotExists effect is only evaluated if the request executed by the Resource Provider returns a success status code. Once the effect has been evaluated, it is triggered if the resource does not exist or if the resource defined by ExistenceCondition is evaluated as false

Question 167

CertyIQ

You use taxonomic tags to logically organize resources and to make billing reporting easier

You use Azure PowerShell to append an additional tag on a storage account named corpstorage99. The code is as follows

```
St Get-AzResource -ResourceName "corpstorage99" -ResourceGroupName "prod-rg" Set-AzResource -Tag @(Dept="IT") -ResourceId $r.ResourceId -Force
```

The code returns unexpected results.

You need to append the additional tag as quickly as possible.

What should you do?

Choose the correct answer

A. Edit the script to call the Add() method after getting the resource to append the new tag.

B. Assign the Enforce tag and its value Azure Policy to the resource group.

C. Refactor the code by using the Azure Command-Line Interface (CLI).

D. Deploy the tag by using an Azure Resource Manager template.

Explanation:

You should edit the script to call the Add() method after getting the resource to append the new tag as shown in the second line of this refactored Azure PowerShell code:

```
$r = Get-AzResource -ResourceName "corpstorage99" -ResourceGroupName "prod-rg" $r.Tags.Add("Dept", "IT")
```

Set-AzResource -Tag $r.Tags -ResourceId Sr.ResourceId -Force

Unless you call the Add() method, the Set-AzResource cmdlet will overwrite any existing taxonomic tags on the resource. The Add() method preserves existing tags and includes one or more tags to the resource tag list

You should not deploy the tag by using an Azure Resource Manager template. Doing so is unnecessary in this case because the Azure PowerShell is mostly complete as-is. Furthermore, you must find the solution as quickly as possible

You should not assign the Enforce tag and its value Azure Policy to the resource group. Azure Policy is a governance feature that helps businesses enforce compliance in resource creation. In this case, the solution involves too much administrative overhead to be a viable option. Moreover, the scenario makes no mention of the need for governance policy in specific terms.

You should not refactor the code by using the Azure Command-Line Interface (CLI). Either Azure PowerShell or Azure CLI can be used to institute this solution. It makes no sense to change the development language, since you have already completed most of the code in PowerShell.

Question 168 CertyIQ

Your company has an Azure Subscription with several resources deployed. The subscription is managed by a Cloud Service Provider.

The accounting department is currently granted the billing reader role, so they are able to see cost-related Information. They need to get a better understanding of the costs so they can assign them to the correct cost center

You need to provide cost center information. Your solution should minimize administrative effort

What two actions should you perform? Each correct answer presents part of the solution.

Choose the correct answers

A. Create a tag named CostCenter and assign it to each resource group.

B. Instruct the accounting department to use the Azure Account Center.

C. Create a tag named CostCenter and assign it to each resource.

D. Instruct the accounting department to use the Cost Analysis blade in the subscription panel.

Explanation:

You should create a tag named CostCenter and assign it to each resource group. Creating a tag and assigning it to each resource group allows you to easily identify the cost center associated with each resource group. When you associate a tag with a resource or resource group, you need to provide a value to that tag. You can instruct the accounting department to use the Azure Cost Management tool to review the costs associated with each cost center by filtering by the newly created tag.

You should also create a tag named CostCenter and assign it to each resource. If you apply a tag to a resource group, that tag is not inherited by the resources in the resource group. You need to manually configure the tag for each resource that you want to include in the cost center. You can automate this action by using a PowerShell or Azure CLI script.

You should not instruct the accounting department to use either the Cost Analysis blade in the subscription panel or the Azure Account Center. Because your subscription is managed by a Cloud Service Provider, you can get that information from your provider. You can also get this information by using the Azure Cost Management tool.

Question 169 CertyIQ

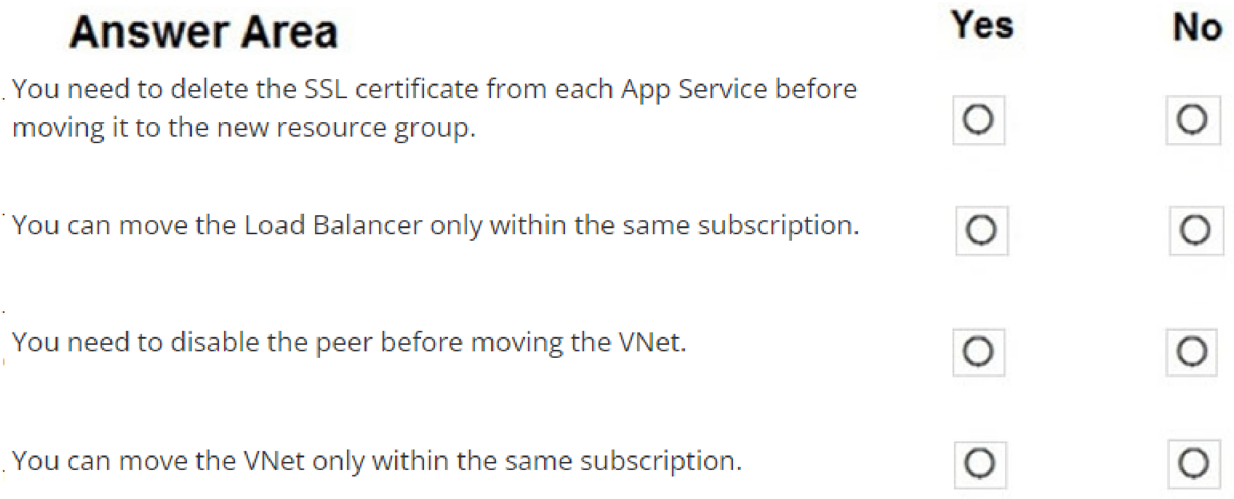
You deploy an application in a resource group named App-RG01 in your Azure subscription.

App-RG01 contains the following components:

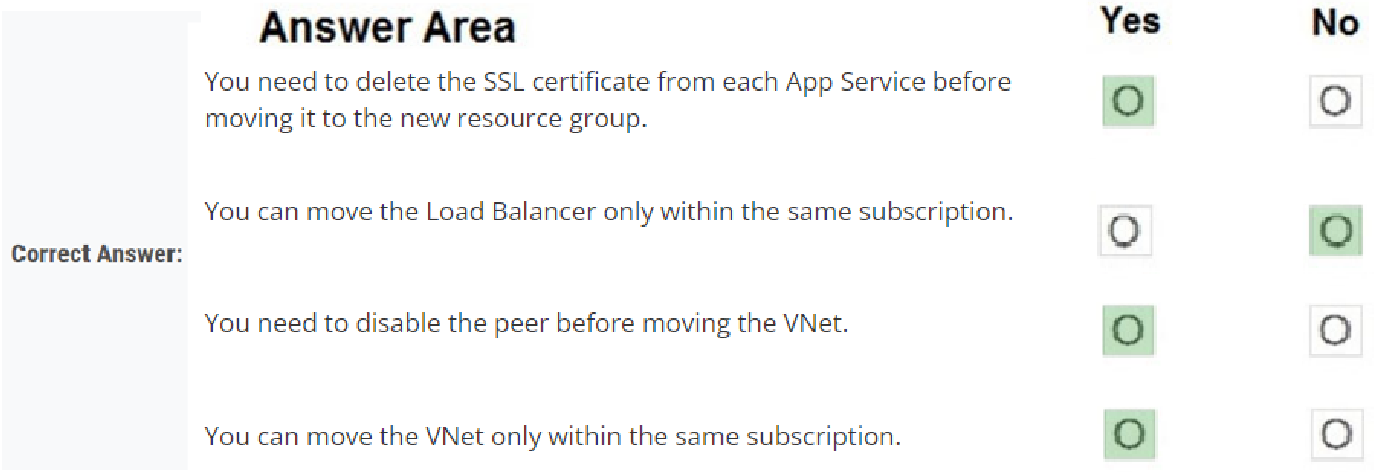
- Two App Services, each with an Secure Sockets Layer (SSL) certificate
- A peered virtual network (VNet)
- Redis cache deployed in the VNet
- A standard Load Balancer

You need to move all resources in App-RG01 to a new resource group named App-RG02.

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



Answer Area	Yes	No
You need to delete the SSL certificate from each App Service before moving it to the new resource group.	○	○
You can move the Load Balancer only within the same subscription.	○	○
You need to disable the peer before moving the VNet.	○	○
You can move the VNet only within the same subscription.	○	○



Correct Answer:

Answer Area	Yes	No
You need to delete the SSL certificate from each App Service before moving it to the new resource group.	[✓ ○]	○
You can move the Load Balancer only within the same subscription.	○	[✓ ○]
You need to disable the peer before moving the VNet.	[✓ ○]	○
You can move the VNet only within the same subscription.	[✓ ○]	○

Explanation:

You need to delete the Secure Sockets Layer (SSL) certificate from each App Service before moving it to the new resource group. You cannot move an App Service with an SSL certificate configured. You need to delete the certificate first, move the App Service, and then upload the certificate again.

You cannot move the Load Balancer within the same subscription. A Standard Load Balancer cannot be moved either within the same subscription or between subscriptions.

You need to disable the peer before moving the VNet. When you want to move a VNet with a peer configured, you need to disable it before moving the VNet. When you move a VNet, you need to move all of its dependent resources.

You can only move the VNet within the same subscription. When you want to move a VNet, you also need to move all of its dependent resources. In this case, you also need to move the Redis cache, which can be moved only within the same subscription. Because you want to move the resources from App-RG01 to App RG02, which is in the same subscription, you can move the VNet with no problem.

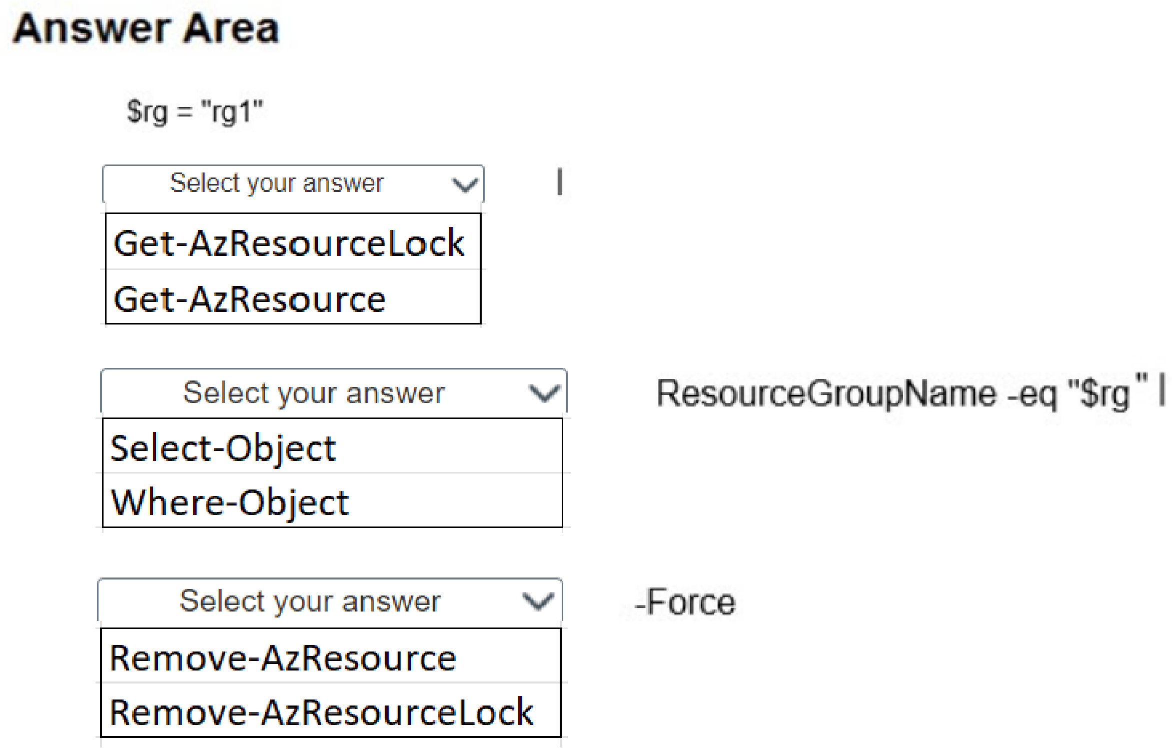
Question 170 CertyIQ

You have an Azure resource group named RG1. RG1 contains 12 virtual machines (VMs) that run Windows Server or Linux.

You need to use Azure Cloud Shell to lift any resource locks that were applied to.the VMs.

How should you complete the Azure PowerShell command? To answer, select the appropriate options from the drop-down menus.

Choose the correct options



Answer Area

$rg = "rg1"

Select your answer

Get-AzResourceLock

Get-AzResource

|

Select your answer

Select-Object

Where-Object

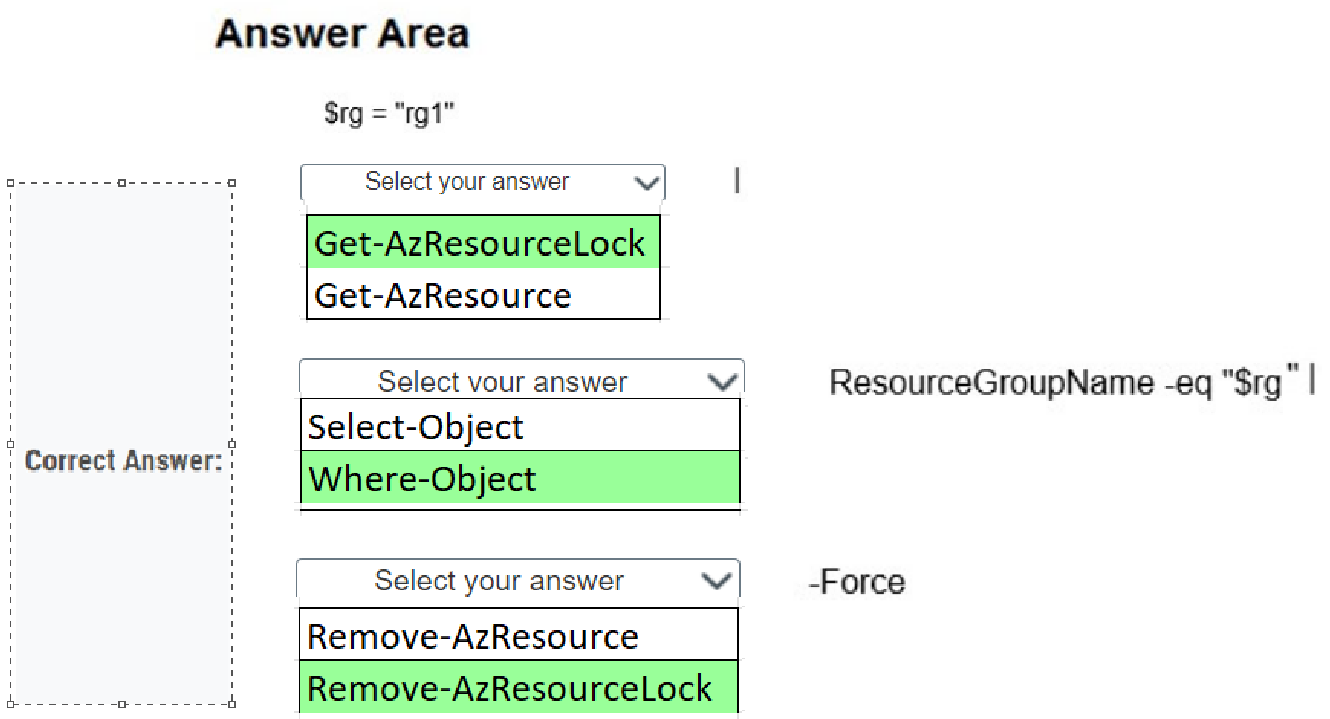
ResourceGroupName -eq "$rg" |

Select your answer

Remove-AzResource

Remove-AzResourceLock

-Force



Answer Area

$rg = "rg1"

Correct Answer:

Select your answer

[✓ Get-AzResourceLock]

Get-AzResource

|

Select vour answer

Select-Object

[✓ Where-Object]

ResourceGroupName -eq "$rg" |

Select your answer

Remove-AzResource

[✓ Remove-AzResourceLock]

-Force

Explanation:

You should use the following command:

Srg = "rg1"

Get-AzResourceLock |

Where-Object ResourceGroupName eq "$rg" |

Remove-AzResourceLock -Force

To programmatically lift resource locks in Azure, start with the Get-AzResourceLock command to retrieve all resource locks in your current subscription context. You can add a where-Object filter expression to retrieve only locks from a particular resource group.

Next, you can take advantage of the PowerShell pipeline by piping your results to the Remove AzResourceLock cmdlet to actually remove the locks. The Force switch parameter forces the command to run without asking for user confirmation.

You should not use the Get-AzResource or Remove-AzResource cmdlets because doing so requires far more PowerShell code than is shown in the scenario, and you only need to retrieve the locked resources from a specific resource group.

You should not use the Select-Object cmdlet because it filters at the property level, and not the row level, and would therefore not restrict output to locked resources within a single resource group.

Question 171

CertyIQ

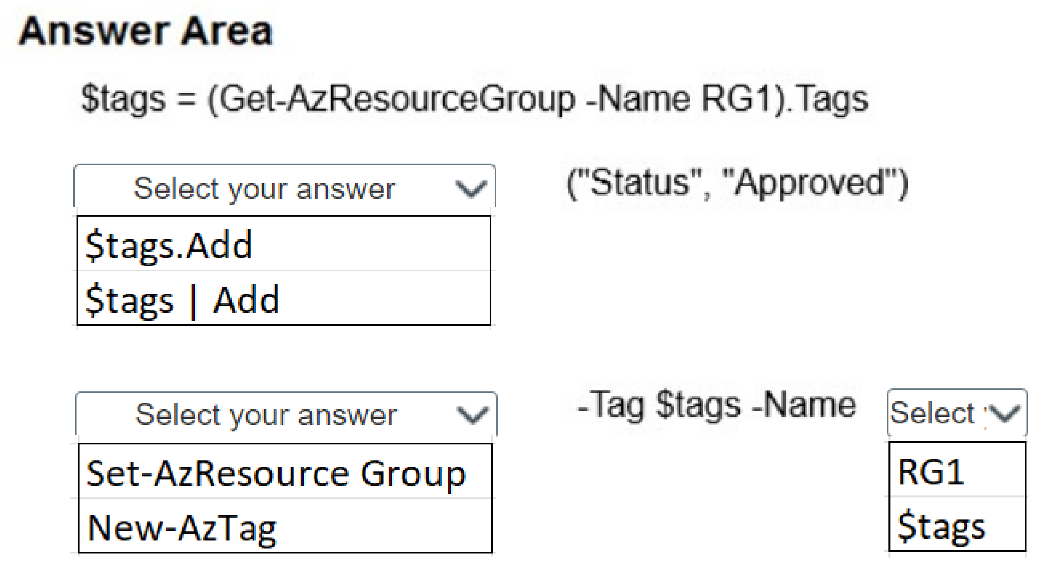
You build a new Marketing solution in an Azure resource group called RG1. RG1 has an existing tag with the name Department and its value is Marketing.

You plan to use Azure Cloud Shell to add another tag to RG1 with the name Status and the value of

Approved. You need to ensure that RG1's existing tag is preserved.

How should you complete the Azure PowerShell command? To answer, select the appropriate options from the drop-down menus.

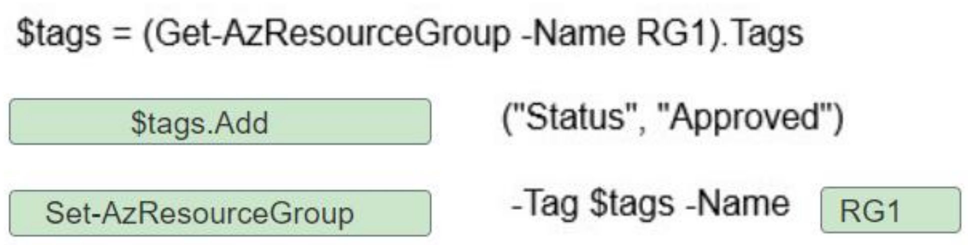
Choose the correct options



Answer Area

```
$tags = (Get-AzResourceGroup -Name RG1).Tags
```

Correct Answer: -



```
$tags = (Get-AzResourceGroup -Name RG1).Tags
$tags.Add ("Status", "Approved")
Set-AzResourceGroup -Tag $tags -Name RG1
```

Explanation:

You should use the following command:

Stags (Get-AzResourceGroup Name RG1). Tags $tags.Add("Status", "Approved") Set-AzResourceGroup -Tag Stags -Name RG1

You should access the Add() method of your Stags object to add a new tag to the target resource group. You should not use the pipe () character because in PowerShell you use the dot (.) and not the pipe to

access object members such as properties, methods, or events.

You should use the Set-AzResourceGroup cmdlet to modify a resource group.

You should not use the New-Az Tag cmdlet because it only creates a new tag. The New-Az Tag cmdlet does not assign the tag to the relevant Azure resources.

You should specify RG1 for the -Name property of the Set-AzResourceGroup cmdlet because this parameter requires a string value that matches the name of the target resource group.

You should not use the Stags variable because this is an object that stores the resource group's current tag

list.

Question 172 CertyIQ

You are the lead architect for your company's Microsoft Azure infrastructure.

To maintain corporate compliance certifications, you need to ensure that any virtual machines are created only in approved Azure regions.

What should you do?

Choose the correct answer

A. Enforce conditional access policy in Azure Active Directory (Azure AD).

B. Define and deploy a custom Azure Policy template.

C. Create an Azure management group.

D. Define and deploy an Azure Automation Desired State Configuration (DSC).

Explanation:

You should define and deploy a custom Azure Policy by using JSON and Azure PowerShell. Azure Resource Manager includes a number of predefined policy templates that cover various governance use cases. However, you can also build a custom template and upload it to Azure to make it available in your subscriptions.

You should not define and deploy an Azure Automation Desired State Configuration (DSC). Azure Automation DSC prevents configuration drift on newly deployed or existing Azure or on-premises nodes. This scenario requires that you enforce compliance on virtual machine (VM) locations at deployment time.

You should not deploy a management group. A management group is a scope level above an Azure subscription and it allows you to assign Azure Policy that affects multiple subscriptions simultaneously. In this case, you need to define a policy first, and then you can optionally scope the new custom policy to a management group.

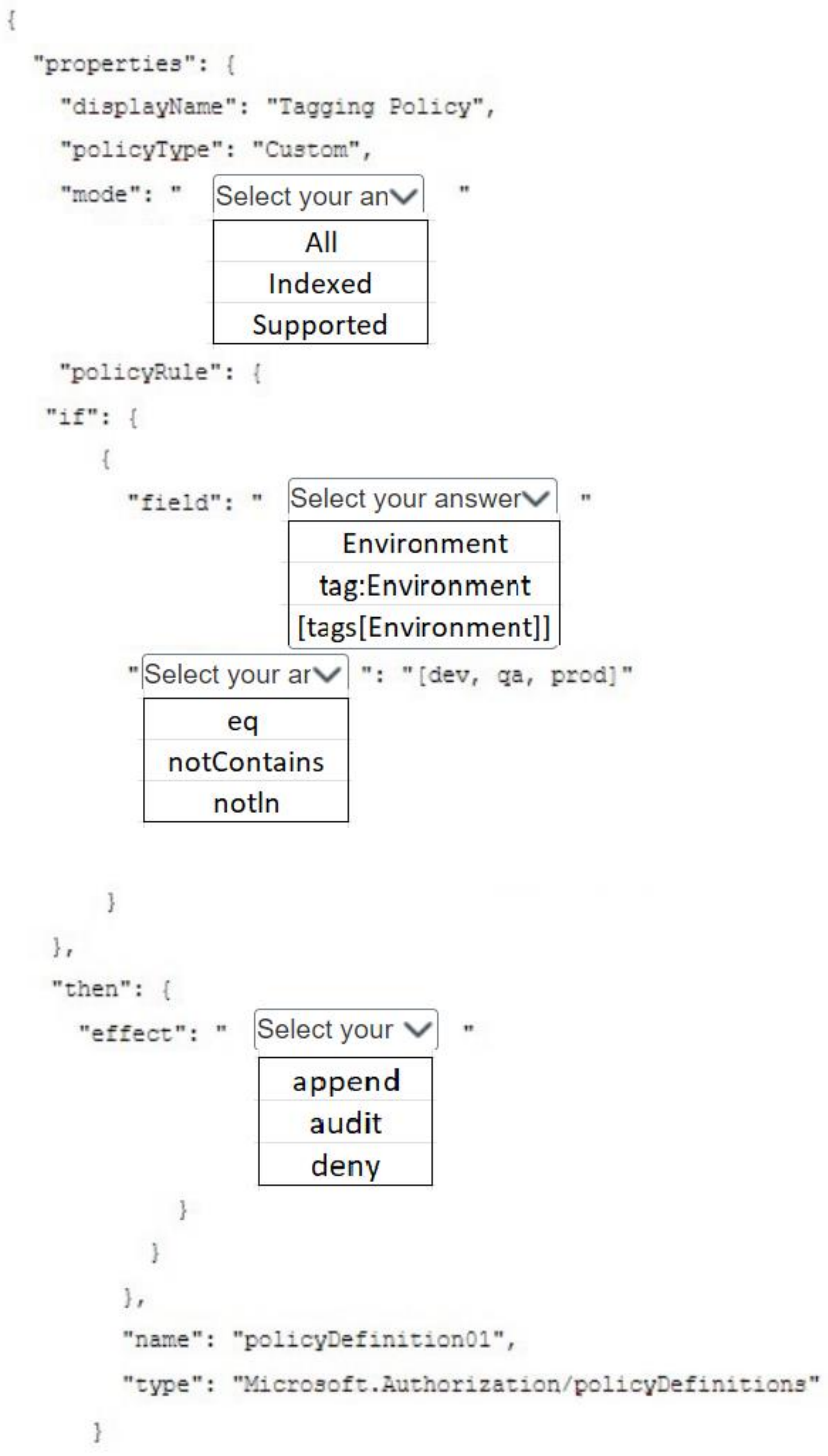
You should not enforce conditional access policy in Azure Active Directory (Azure AD). This feature affects user accounts, not VMS deployed in Azure. Conditional access allows you to specify requirements for your users to access Azure AD-protected apps. For instance, you might require that users can only authenticate to an app if they are connecting from a corporate IP address.

Question 173 CertyIQ

You are developing a policy that will deny the creation of any resource that does not have an environment tag with a value of either dev, qa, or prod.

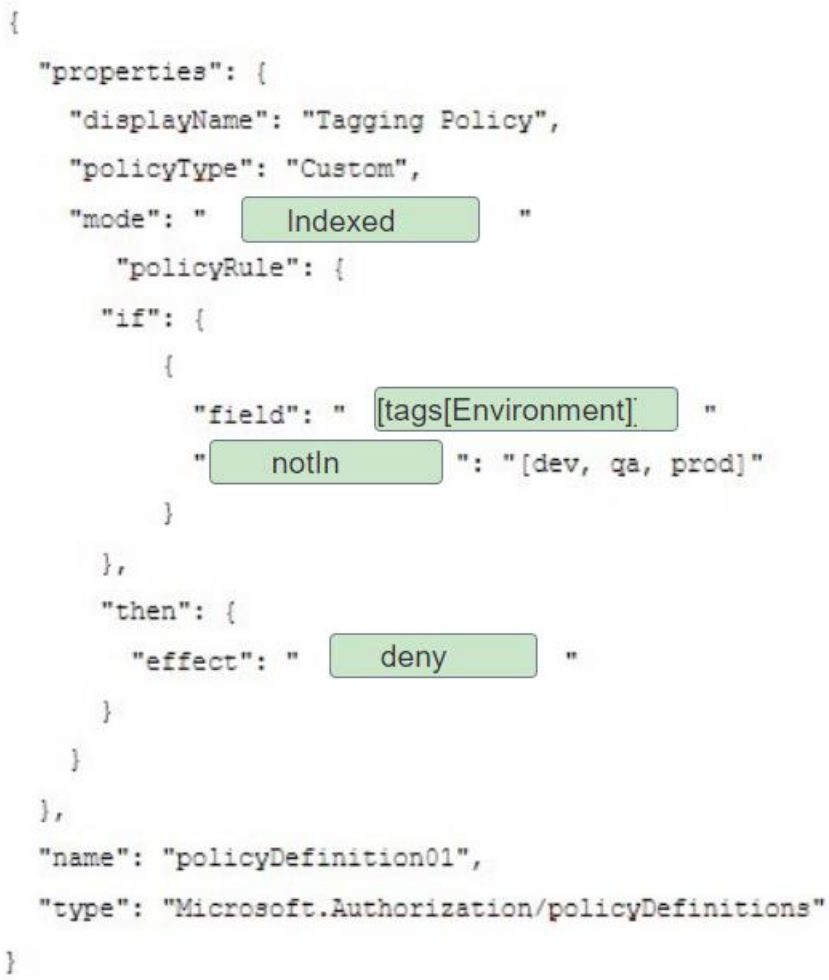
You need to ensure that only resources that support tagging are checked by the policy.

How should you configure the policy? To answer, complete the JSON template by selecting the correct options from the drop-down menus.



```
{
  "properties": {
    "displayName": "Tagging Policy",
    "policyType": "Custom",
    "mode": " Select your an▽   "
              All
              Indexed
              Supported
   "policyRule": {
  "if": {
      {
        "field": " Select your answer▽  "
                    Environment
                    tag:Environment
                    [tags[Environment]]
        "Select your ar▽ ": "[dev, qa, prod]"
           eq
           notContains
           notIn


      }
  },
  "then": {
    "effect": " Select your ▽  "
                 append
                 audit
                 deny
          }
        }
      },
      "name": "policyDefinition01",
      "type": "Microsoft.Authorization/policyDefinitions"
    }
```

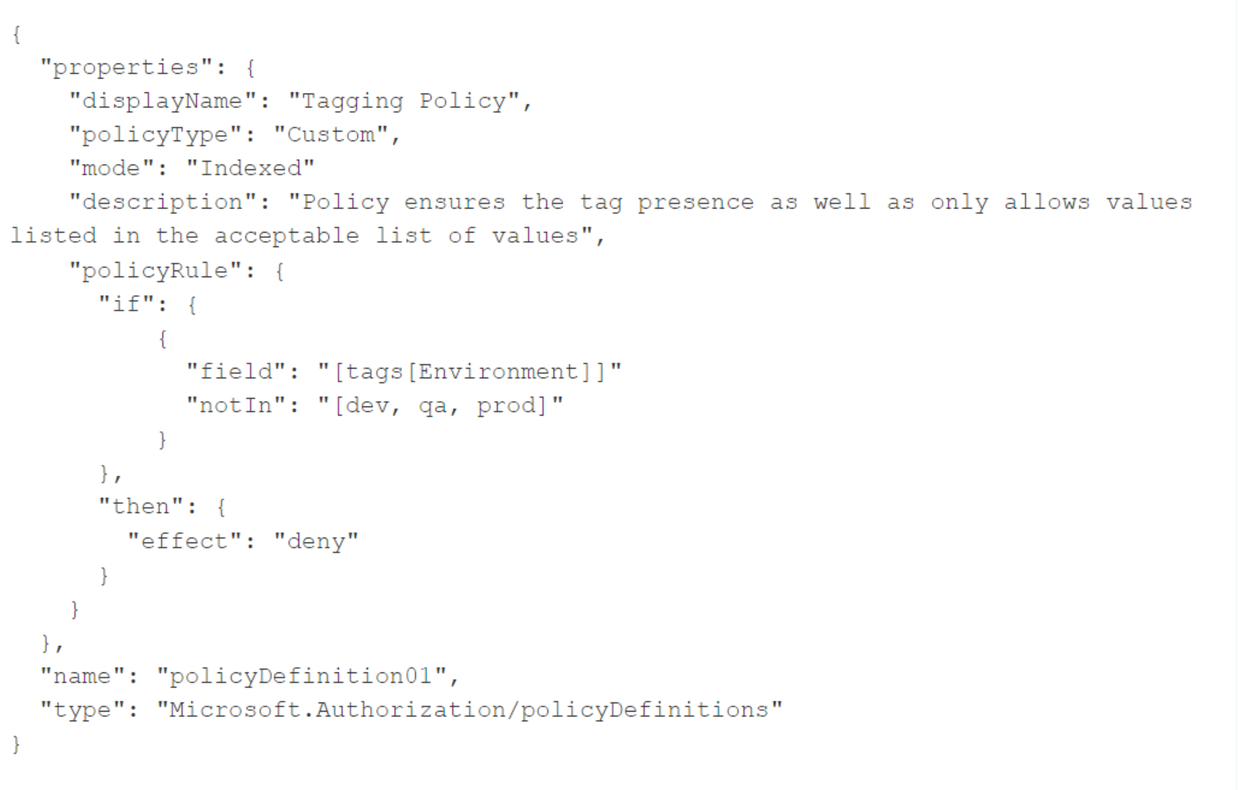
Correct Answer: -



```
{
  "properties": {
    "displayName": "Tagging Policy",
    "policyType": "Custom",
    "mode": " Indexed "
      "policyRule": {
    "if": {
        {
          "field": " [tags[Environment]] "
          " notIn ": "[dev, qa, prod]"
        }
    },
    "then": {
      "effect": " deny "
    }
  }
 },
 "name": "policyDefinition01",
 "type": "Microsoft.Authorization/policyDefinitions"
}
```

Explanation:

You should configure the policy as follows:



```
{
  "properties": {
    "displayName": "Tagging Policy",
    "policyType": "Custom",
    "mode": "Indexed"
    "description": "Policy ensures the tag presence as well as only allows values
listed in the acceptable list of values",
    "policyRule": {
      "if": {
          {
            "field": "[tags[Environment]]"
            "notIn": "[dev, qa, prod]"
          }
      },
      "then": {
        "effect": "deny"
      }
    }
  },
  "name": "policyDefinition01",
  "type": "Microsoft.Authorization/policyDefinitions"
}
```

You should use Indexed for the mode property. Indexed policies check whether a resource supports a feature before it checks for it. Selecting All would try to apply the policy to all resources even if the resource does not support tagging. Supported is not a valid option for the mode property.

You should use [tags[Environment]] as the field value. You should not select Environment because there is no field for Azure resources named Environment. You should not select tag: Environment because tags are an array.

You should use notin for the check condition. If the tag value for Environment is not in dev, qa, and prod, you want to deny the creation of the resource. You should not select eq or notContains. Neither can be applied to check for an array value. They will check for string values.

You should use deny for the effect property. The "then" block specifies the effect to apply if the policy rule block evaluates to false. In this case, you want to deny creation. You should not use audit because that would allow creation and genenerate a compliance log entry. You should not use append because it would add an empty Environment tag to the resource and not set a value equal to either dev, qa, or prod.

Question 174

CertyIQ

Your company creates multiple management groups under your Root Management Group. You are re organizing the management groups and want to move all resources for the Sales and Marketing management groups under the Marketing management group. Once finished, you plan to delete the Sales management group.

You need to move the subscription named SalesSub to the Marketing management group.

Which PowerShell cmdlet should you use?

Choose the correct answer

A. New-AzManagement Group Deployment

B. Update-AzManagement Group

C. New-AzManagementGroupSubscription

D. Remove-AzManagement GroupSubscription

E. Remove-AzManagementGroup

Explanation:

You should use the New-AzManagementGroup Subscription cmdlet. You can use this cmdlet to add an existing subscription to an existing management group, which is what is required by this scenario. This command creates a link between the subscription and the specified management group.

You should not use Remove-AzManagementGroup Subscription. This is used to sever the link between a subscription and a management group. This does not delete the subscription or the management group.

You should not use Update-AzManagementGroup. This is used to update supported parameters, such as the management group display name or change the management group parent.

You should not use New-AzManagementGroupDeployment. This is used to add a deployment to a management group. You must specify the management group, location, and a template when using the cmdlet to tell the resource manager where to store deployment data.

You should not use Remove-AzManagementGroup. This cmdlet is used to delete a management group.

Question 175

CertyIQ

A company has an Azure Active Directory (Azure AD) tenant. A recent governance audit of the Azure AD tenant has found that all users currently have the ability to create management groups within the tenant. You need to enable hierarchy protection so that only admins with the relevant permissions can create management groups.

You must create a JSON script to set the permissions.

Which operation do you need to set in your JSON file to grant the relevant permission level to ensure that standard users are no longer allowed to create management groups?

Choose the correct answer

A. Microsoft.Management/managementGroups/read

B. Microsoft Management/managementGroups/delete

C. Microsoft.Management/managementgroup/subscriptions/write

D. Microsoft.Management/managementGroups/write

Explanation:

You need to set the Microsoft.Management/managementGroups/write operation in the JSON file. If this level of permission is enabled on the root management group, it will ensure that only users who have this level of permission will be able to create management groups. Standard users will no longer be able to create management groups.

You should not set the Microsoft.Management/managementGroups/delete operation in the JSON file. This would enable users at this level of permission to delete management groups. Standard users will no longer be able to delete management groups, but they will still be able to create them.

You should not set the Microsoft.Management/managementGroups/read operation in the JSON file. If this level of permission is enabled on the root management group, it will ensure that only users at this permission level will be able to read management groups. Standard users will no longer be able to read management groups, but they will still be able to create them.

You should not set the Microsoft.Management/managementgroup/subscriptions/write operation in the JSON file. This operation sets write access on the subscription level, rather than just for the management group. Therefore standard users will still be able to create management groups at the top level, but not at the subscription level.

Question 176

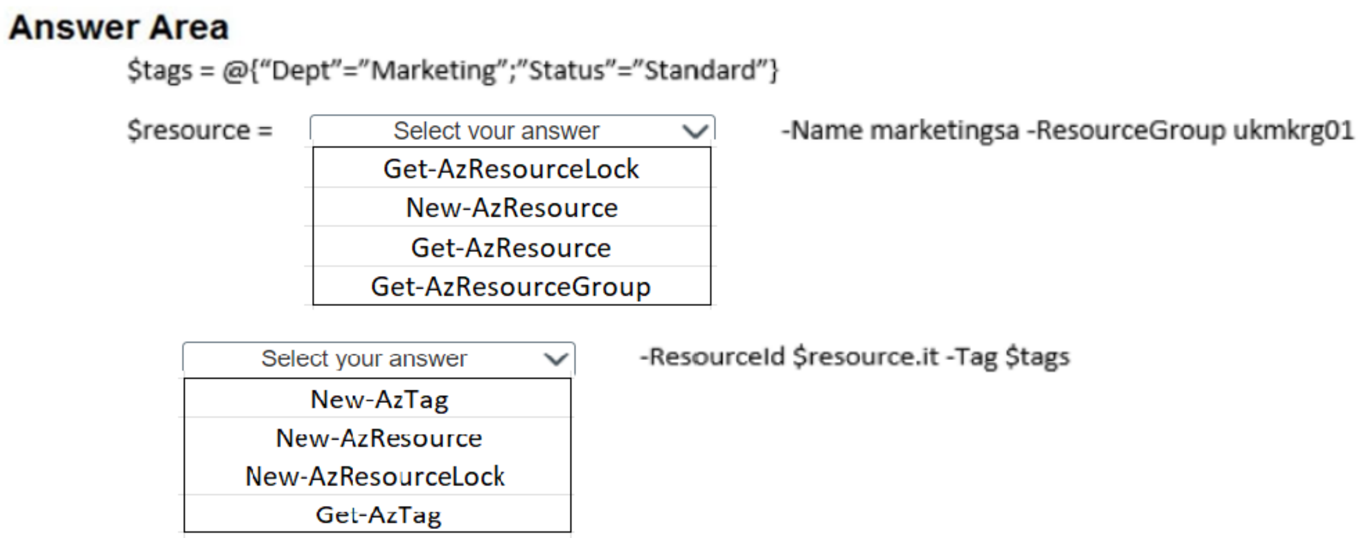
A company hosts resources in Azure and Microsoft 365. A storage account was recently created for the Marketing department, but it was not picked up in the monthly usage report. Further investigation shows that no resource tags were configured during the creation of the storage account.

You need to add a resource tag to the storage account so it will show up in the monthly reports under the Marketing department with a status of Standard.

You want to configure the resource tag via PowerShell.

Which cmdlets should you use? To answer, complete the commands by selecting the correct options from the drop-down menus.

Choose the correct options



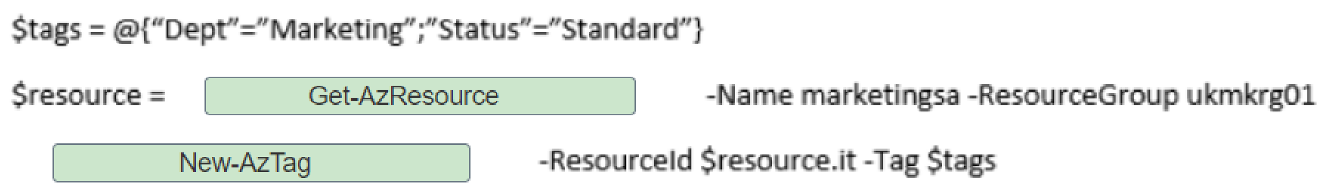
Answer Area

$tags = @{“Dept”=”Marketing”;”Status”=”Standard”}

$resource = [Select vour answer] -Name marketingsa -ResourceGroup ukmkrg01

[Select your answer] -ResourceId $resource.it -Tag $tags

Correct Answer: -



$tags = @{“Dept”=”Marketing”;”Status”=”Standard”}

$resource = Get-AzResource -Name marketingsa -ResourceGroup ukmkrg01

New-AzTag -ResourceId $resource.it -Tag $tags

Explanation:

You should complete the code as follows:

$tags = @("Dept"="Marketing"; "Status"-"Standard"}

$resource = Get-AzResource -Name marketingsa -ResourceGroup ukmkrg01 New-AzTag ResourceId $resource.id -Tag $tags

You should use the Get-AzResource cmdlet to first call the storage account that you want to add the new tag to. For this cmdlet, you need to know both the storage account name and the resource group name that it resides in.

You should use the New-AzTag cmdlet to create the new resource tag. This will create the new tag against the storage account you called in the previous line, which in this case is the marketingsa storage account in the ukmkrg01 resource group.

You should not use the Get-AzResourceLock cmdlet. This would attempt to call any existing resource locks or a specific resource lock if you enter the relevant name and resource group details. In this scenario you do not want to make any changes to resource locks.

You should not use the New-AzResource cmdlet. This cmdlet is utilized to create a new Azure resource. However, at the start of our PowerShell script you do not need to create a new resource, you only need to call on the storage account. This means you would need to use a 'Get' cmdlet, not a 'New' cmdlet.

You should not use the Get-AzResourceGroup cmdlet. Although the 'Get' cmdlet is the correct syntax, you do not want to call upon a resource group, upon a specific resource.

You should not use the New-AzResource cmdlet. Although the 'New' cmdlet is the correct syntax at this stage of the PowerShell script as you need to create a new tag, this specific cmdlet will create a new Azure resource, not a tag.

You should not use the New-AzResourceLock cmdlet. Although the 'New' cmdlet is the correct syntax at this stage of the PowerShell script as you need to create a new tag, this specific cmdlet will create a new Azure resource lock, not a tag.

You should not use the Get-AzTag cmdlet. At this stage of the PowerShell script you do not need to call on any resources as this will have been done on the previous line. You need to create the resource tag and therefore need to use the 'New' syntax rather than the 'Get' syntax.

Question 177

CertyIQ

Your company hosts its Infrastructure as a Service (IaaS) infrastructure in Azure. You have taken over the management of the Azure IaaS infrastructure from the previous IT technician, who was responsible for creating and managing all resources within the tenant. The owner of the development subscription within the tenant wants to block anyone from deleting the devtestrg resource group, without having to add any type of resource lock at the subscription level.

You need to recommend a solution to facilitate this requirement. You want to use minimal amount of administrative effort.

What solution should you recommend?

Choose the correct answer

A. Add a delete lock on each individual resource in the resource group.

B. Add a read-only lock on a single resource in the resource group.

C. Add a delete lock on a single resource in the resource group.

D. Add a read-only lock on the resource group.

Explanation:

You should add a delete lock on a single resource in the resource group. Adding a delete lock to a single resource within the resource group will cause an error to be shown if a user tries to delete the resource group. Therefore a lock has not been added at the resource group level or the subscription level, but users are still blocked from deleting the resource group.

You should not add a delete lock on each individual resource in the resource group. Although this would block anyone from deleting the resource group, it involves much more administrative effort to add a lock to each resource individually. You only need to add a delete lock on a single resource in the resource group to stop the group from being deleted.

You should not add a read-only lock on the resource group. A read-only lock will not prevent the resource group from being deleted, it will only prevent the resource group from being edited.

You should not add a read-only lock on a single resource in the resource group. Although you should recommend adding a resource lock to a single resource, it needs to be a delete lock, not a read-only lock.

Question 178

CertyIQ

A company has an existing on-premises environment and a newly created Azure subscription. You need to start testing cloud features and services with a view to eventually migrating the company environment to the Cloud. You have been given Global Administrator rights and the Resource Policy Contributor role on the subscription, and you need to test Azure Policy first.

You have downloaded version 2.38 of the Azure Command-Line-Interface (CLI) to configure new policies, but you find that the Azure Policies you are creating are not working with your subscription.

You need to find the cause of this problem.

What is causing the Azure Policy to not function with your subscription when using the Azure CLI?

Choose the correct answer: -

A. You do not have the relevant access to the subscription.

B. You have not registered Azure Policy Insights resource provider.

C. You do not have the relevant role assignment to manage Azure Policy.

D. Your version of the Azure CLI needs updating.

Explanation:

You have not registered Azure Policy Insights resource provider. You need to register the Azure Policy Insights resource provider using the Azure Command-Line-Interface (CLI). This ensures that the subscription you are logged into works with the Azure Policies you create. The specific operation that is missing is Microsoft.PolicyInsights, which is included with the Contributor and Owner roles. However, it is not included in the Resource Policy Contributor role that you have been assigned, and therefore, you would need to register it.

You do not need to change the permissions to the subscription. You have been assigned the Resource Policy Contributor role at the subscription level, which has the relevant access required to configure Azure Policy. This role allows users to create and configure policies, create support tickets, and read resources.

You do not need to upgrade the version of the Azure CLI. You have version 2.38, which is currently the most up-to-date version of the Azure CLI. You need version 2.0.7.6 or later to utilize the Azure CLI to configure Azure Policy.

You do not need a different role assignment within Azure. As the scenario states, you have been given Global Admin rights to the Azure portal. The Global Admin role has full control over all services and features in the Azure stack. Therefore, it has sufficient access to create and manage Azure Policy.

Question 179

CertyIQ

You manage a number of Azure subscriptions for a global organization and have ownership of all the subscriptions. You have been asked to use Powershell to migrate the resources on an existing subscription called sub010 to a new subscription called sub020. After the migration, you find that all the Azure role assignments for individual resources have been orphaned on the virtual machines (VMs) but are still in place for the Resource Groups.

You need to find what has caused the missing role assignments to ensure that it is mitigated in future migrations:

What should you identify as the cause?

Choose the correct answer

A. The migration was between subscriptions.

B. The user account moving the resources to sub020 did not have the relevant permissions.

C. There was a network outage during the migration.

D. The Azure portal was not used for the migration.

Explanation:

The migration was between subscriptions, and therefore, any roles assigned directly to the resources were not moved. All role assignments that are directly assigned to a resource or a child resource are not fully migrated, but instead orphaned in the destination subscription. Once the move has been completed, all Azure role assignments need to be re-created and the orphaned role assignments will be removed automatically.

It is not necessary to have used the Azure Portal for the migration. In this scenario, you were using PowerShell to complete the migration of resources from sub010 to sub020, but it is irrelevant if the task is done via PowerShell or via the Azure portal, the outcome would still be orphaned role assignments directly assigned to resources.

The user account moving the resources to sub020 did have the relevant permissions. The scenario states that you are the owner of all the subscriptions and you therefore have the highest level of permissions.

There was not a network outage during the migration. Any type of network outage would cause the entire migration to potentially stop, rather than just affecting the Azure role assignment.

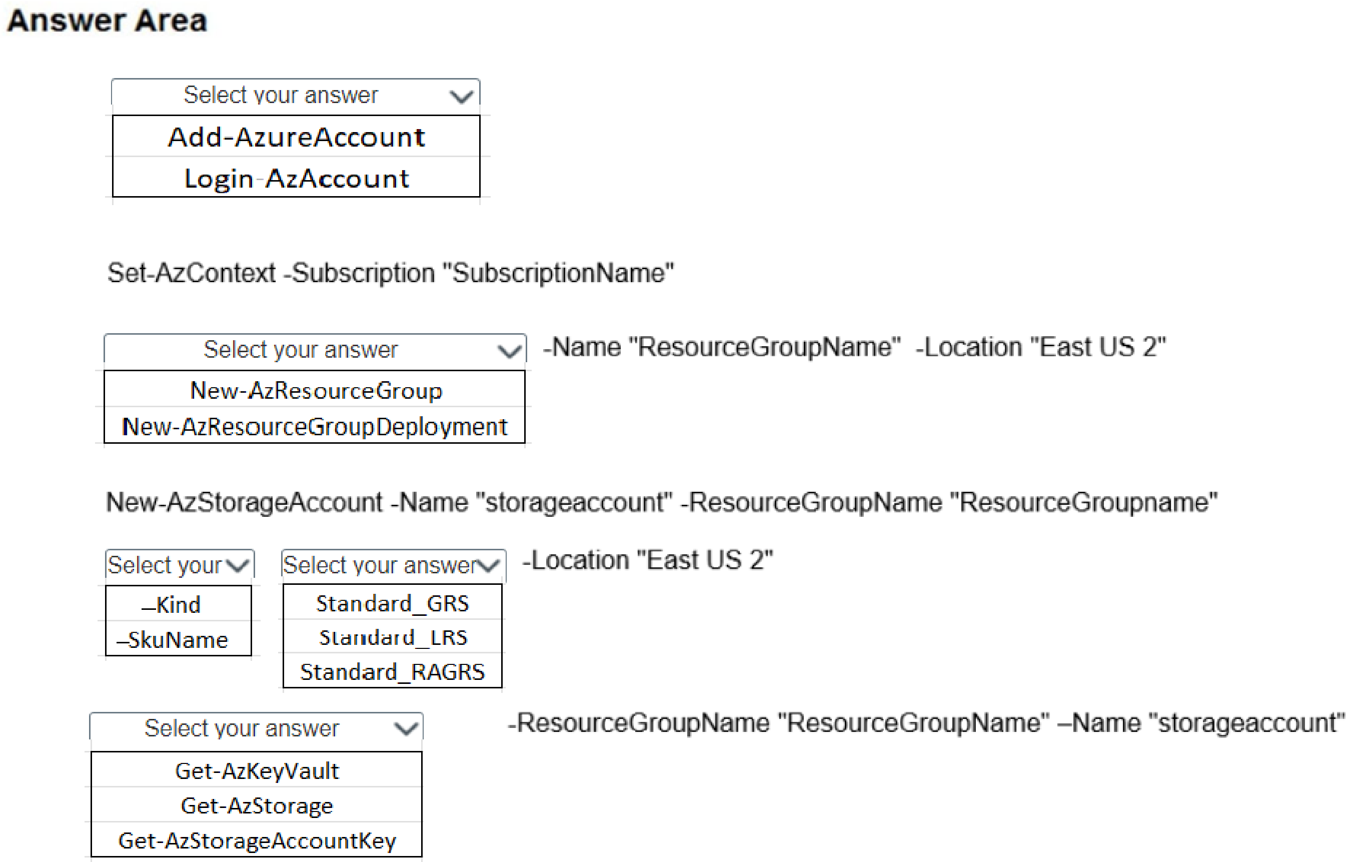
Question 180

The core application development team in your company needs read/write access to an Azure-based storage account as a repository for a new, company-wide application.

You need to create a geo-redundant storage account within an Azure resource group and provide the access control keys to the application development team.

How should you complete the PowerShell script? To answer, select the appropriate options from the drop down menus.

Choose the correct options



Answer Area

Select your answer
- Add-AzureAccount
- Login-AzAccount

Set-AzContext -Subscription "SubscriptionName"

Select your answer -Name "ResourceGroupName" -Location "East US 2"
- New-AzResourceGroup
- New-AzResourceGroupDeployment

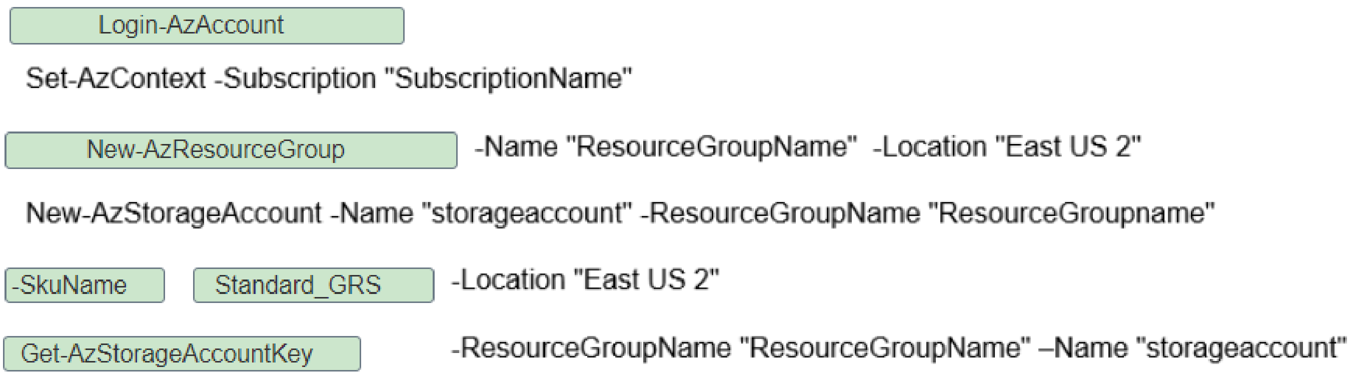
New-AzStorageAccount -Name "storageaccount" -ResourceGroupName "ResourceGroupname"

Select your Select your answer -Location "East US 2"
- –Kind
- –SkuName

- Standard_GRS
- Standard_LRS
- Standard_RAGRS

Select your answer -ResourceGroupName "ResourceGroupName" –Name "storageaccount"
- Get-AzKeyVault
- Get-AzStorage
- Get-AzStorageAccountKey

Correct Answer: -



```
Login-AzAccount
Set-AzContext -Subscription "SubscriptionName"
New-AzResourceGroup -Name "ResourceGroupName" -Location "East US 2"
New-AzStorageAccount -Name "storageaccount" -ResourceGroupName "ResourceGroupname"
-SkuName Standard_GRS -Location "East US 2"
Get-AzStorageAccountKey -ResourceGroupName "ResourceGroupName" –Name "storageaccount"
```

Explanation:

You should first execute the Login-AzAccount cmdlet. This is because the rest of the script is clearly dependent on Azure resource manager cmdlets, and Add-AzureAccount will only support the older Azure service management capability.

You should use the New-AzResourceGroup cmdlet and not New-AzResourceGroup Deployment. New AzResourceGroup creates a new resource group in Azure, whereas New-AzResourceGroup Deployment will deploy a set of resources from an Azure Resource Manager (ARM) template to a resource group in Azure.

Next, you need to provide the parameter to indicate the type of storage requested. You need to provide read/write geo-redundant storage, and this can only be identified as the SkuName of the storage type. The use of -kind indicates the newer V2 storage types, but that parameter does not allow the entry of the storage access type or replication strategy.

Next, you need to provide the SkuName of the storage type. You should use Standard GRS. GRS represents Geo-redundant Storage and is read/write in nature. Standard LRS is Local Replicated Storage only, and Standard RAGRS is Geo-redundant but in Read Access mode only, so neither of these meets the requirements.

Then you need to request the Access Keys for the newly created storage account. You should use Get AzStorageAccountKey because this requests the key for the storage account. Get-AzStorageAccount will get context for the Storage Account itself, but not the access keys. The access keys could be derived from the Storage Context, but not without additional script content. You should not use Get-AzKeyVault because this cmdlet gets the context of an Azure key vault, which is used for multiple reasons but predominantly for providing secure storage of secrets and credentials.

Question 181 CertyIQ

Your Azure subscription has the following resources:

- three App Services
- one backup vault
- one Azure event hub
- a virtual network (VNet) named VNET01
- a VPN Gateway

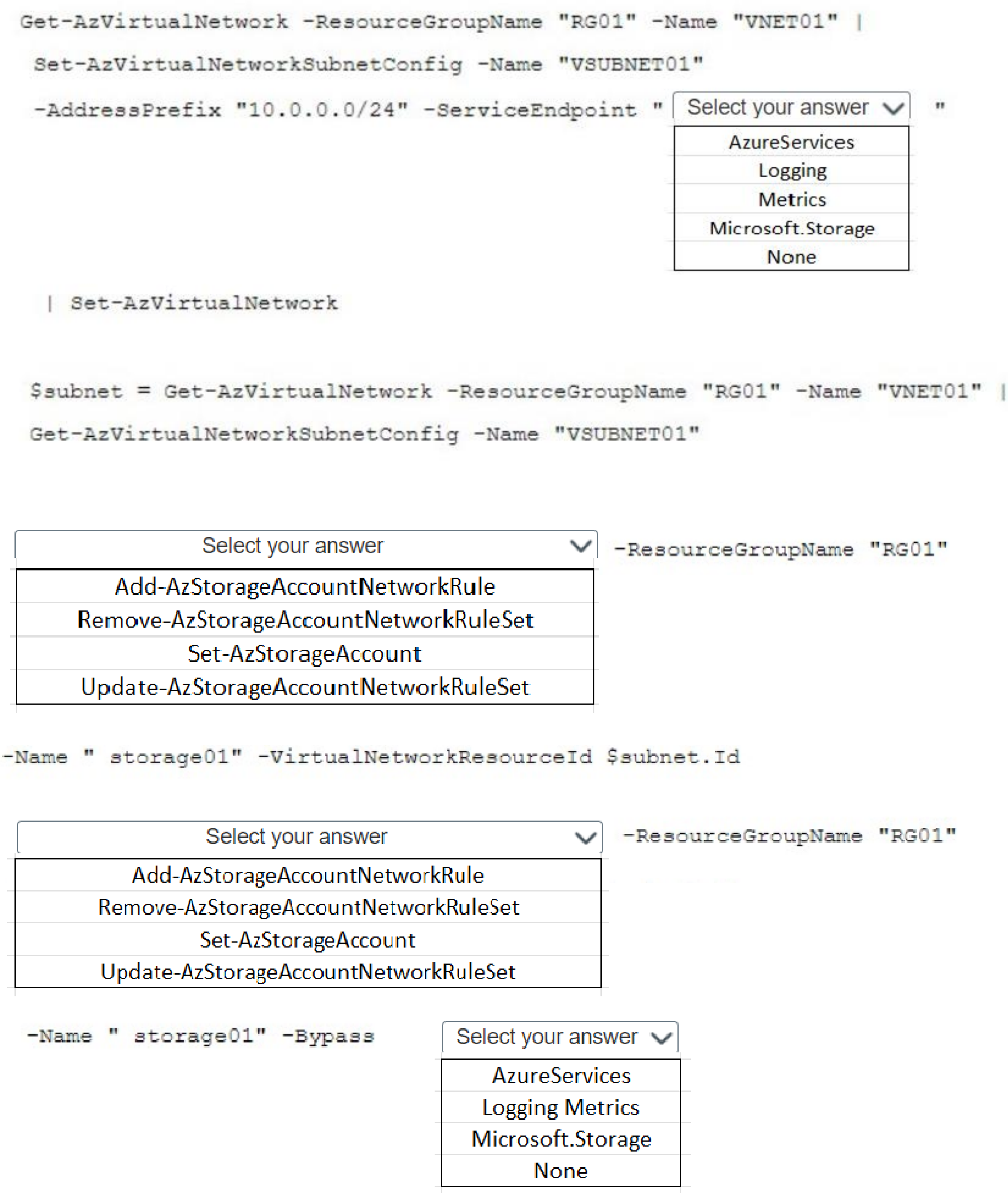
You deploy a new storage account named storage1 in a resource group named RG01.

You need to ensure that the App Services, the backup vault, and the event hub can access the new storage account. Access should be enabled from within Azure only, and not via public internet.

You decide to use PowerShell to set up the new storage account.

How should you complete the command string? To answer, select the appropriate options from the drop down menus.

Choose the correct options



```
Get-AzVirtualNetwork -ResourceGroupName "RG01" -Name "VNET01" |
 Set-AzVirtualNetworkSubnetConfig -Name "VSUBNET01"
 -AddressPrefix "10.0.0.0/24" -ServiceEndpoint " Select your answer "
```

Select your answer
AzureServices
Logging
Metrics
Microsoft.Storage
None

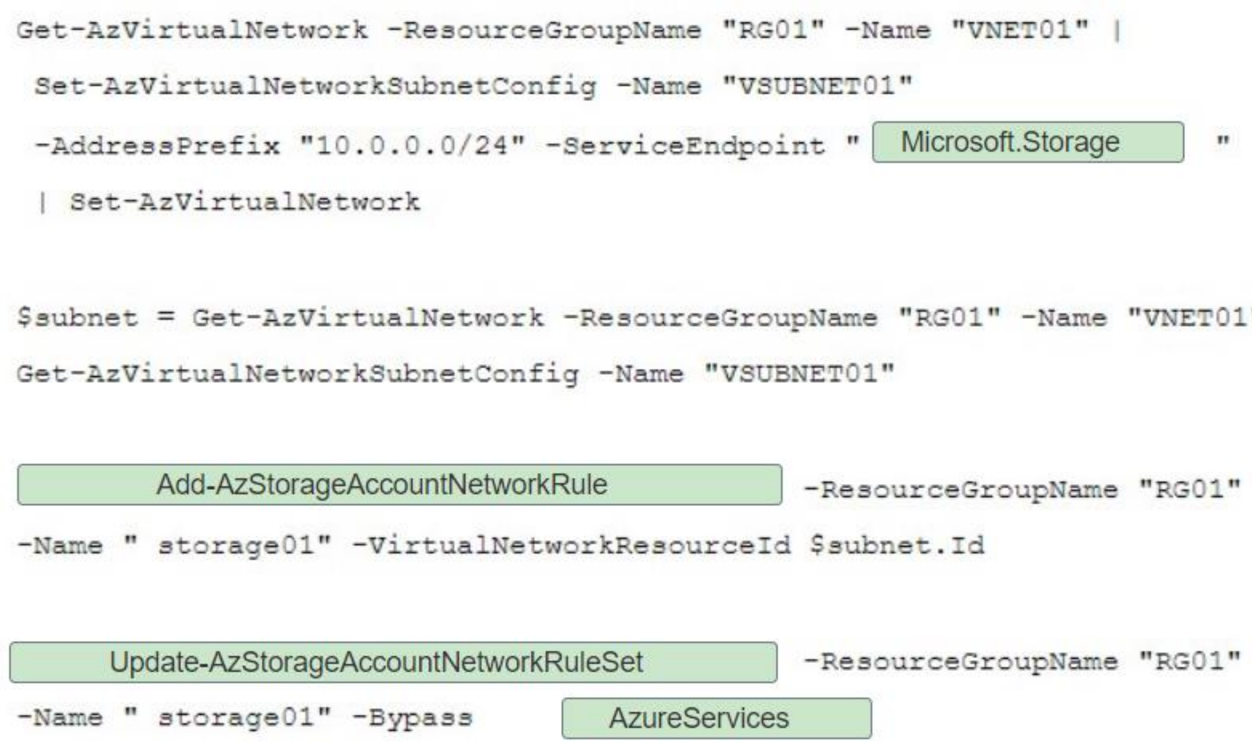
```
  | Set-AzVirtualNetwork


 $subnet = Get-AzVirtualNetwork -ResourceGroupName "RG01" -Name "VNET01" |
 Get-AzVirtualNetworkSubnetConfig -Name "VSUBNET01"
```

Select your answer
Add-AzStorageAccountNetworkRule
Remove-AzStorageAccountNetworkRuleSet
Set-AzStorageAccount
Update-AzStorageAccountNetworkRuleSet

```
-ResourceGroupName "RG01"

-Name " storage01" -VirtualNetworkResourceId $subnet.Id
```

Select your answer
Add-AzStorageAccountNetworkRule
Remove-AzStorageAccountNetworkRuleSet
Set-AzStorageAccount
Update-AzStorageAccountNetworkRuleSet

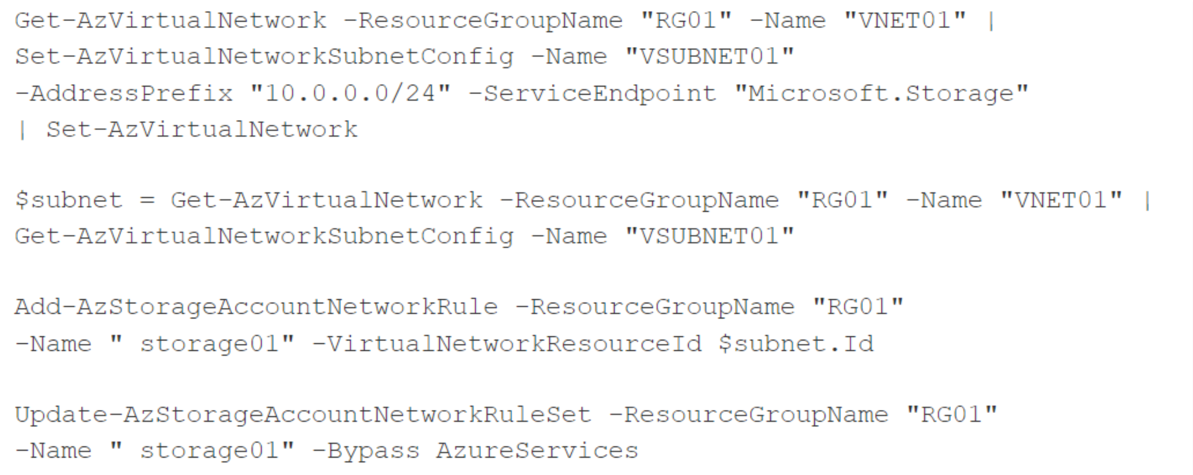
```
-ResourceGroupName "RG01"

 -Name " storage01" -Bypass
```



```
Get-AzVirtualNetwork -ResourceGroupName "RG01" -Name "VNET01" |
 Set-AzVirtualNetworkSubnetConfig -Name "VSUBNET01"
 -AddressPrefix "10.0.0.0/24" -ServiceEndpoint " Microsoft.Storage "
 | Set-AzVirtualNetwork

$subnet = Get-AzVirtualNetwork -ResourceGroupName "RG01" -Name "VNET01" |
Get-AzVirtualNetworkSubnetConfig -Name "VSUBNET01"

Add-AzStorageAccountNetworkRule -ResourceGroupName "RG01"
-Name " storage01" -VirtualNetworkResourceId $subnet.Id

Update-AzStorageAccountNetworkRuleSet -ResourceGroupName "RG01"
-Name " storage01" -Bypass AzureServices
```

Explanation:

You should run the following script to ensure that the backup vault and the event hub services have access to the storage account:



```
Get-AzVirtualNetwork -ResourceGroupName "RG01" -Name "VNET01" |
Set-AzVirtualNetworkSubnetConfig -Name "VSUBNET01"
-AddressPrefix "10.0.0.0/24" -ServiceEndpoint "Microsoft.Storage"
| Set-AzVirtualNetwork

$subnet = Get-AzVirtualNetwork -ResourceGroupName "RG01" -Name "VNET01" |
Get-AzVirtualNetworkSubnetConfig -Name "VSUBNET01"

Add-AzStorageAccountNetworkRule -ResourceGroupName "RG01"
-Name " storage01" -VirtualNetworkResourceId $subnet.Id

Update-AzStorageAccountNetworkRuleSet -ResourceGroupName "RG01"
-Name " storage01" -Bypass AzureServices
```

You should use Microsoft.Storage as the service endpoint. Using the Set-AzVirtual NetworkSubnetConfig cmdlet enables the service endpoint on the subnet VSUBNET01 for a storage account. This will allow connections to the virtual subnet from the storage account. This cmdlet makes modifications only to the memory representation of the virtual network. You need to run Set-AzVirtualNetwork to make the changes persistent.

You should use the Add-AzStorageAccountNetworkRule cmdlet to add a firewall exception on the NetworkRule property in the storage account. This will allow communication from the virtual subnet to the storage account.

You should use the Update-AzStorageAccountNetwork RuleSet cmdlet. This cmdlet also updates the Network Rule property. It allows you to modify the Network Rule property to allow other Azure services, like Backup or Event Hub, to have access to the storage account.

You should use AzureServices for the -Bypass parameter. This way, you instruct the Update AzStorageAccountNetworkRuleSet cmdlet to allow connections from other Azure services. Allowed values are AzureServices, Metrics, Logging, and None.

You should not use the Set-AzStorageAccount cmdlet. can use this cmdlet to modify a storage account, but not the NetworkRule property of the storage account. You typically use this cmdlet when you want to set a tag to a storage account, update a customer domain, or update the type of the account.

You should not use the Remove-AzStorageAccountNetwork RuleSet cmdlet. You use this cmdlet to remove a Network Rule property from the storage account. In this scenario, you need to add and modify a new network rule, not remove it.

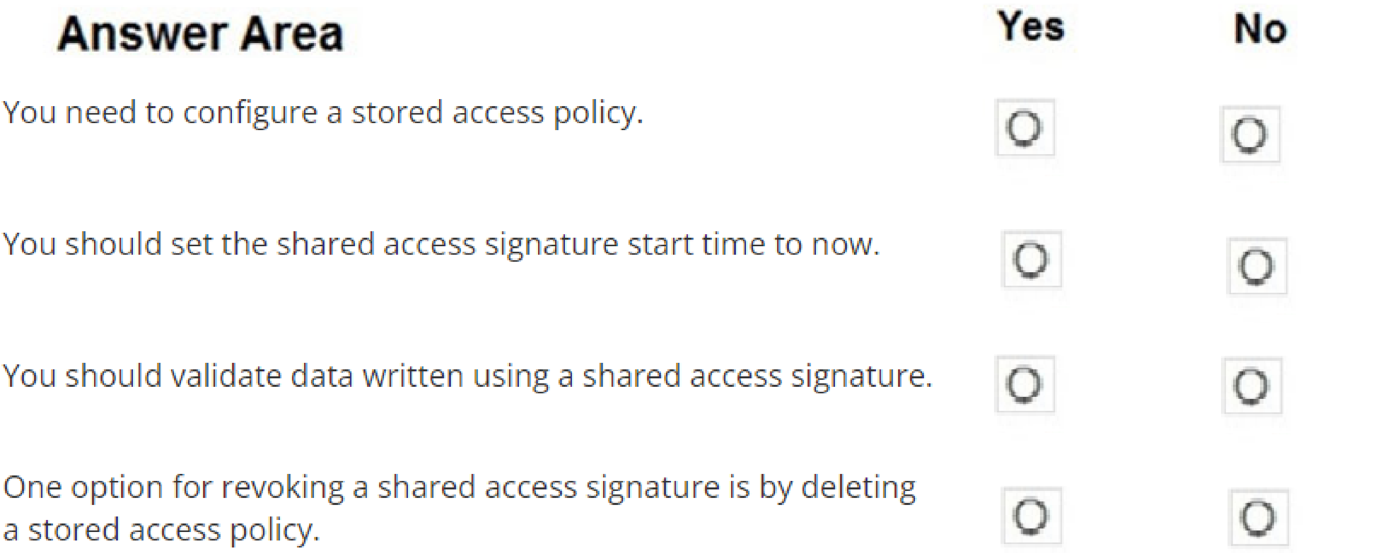
You should not use the Logging. None, or Metrics values. These are valid for the -Bypass parameter for Update-AzStorageAccountNetwork RuleSet. You use the None value when you want to remove the access to all Azure services, including monitoring and logging services. You use the Metrics or Logging values when you want to allow access to monitoring or logging Azure Services respectively.

Question 182

CertyIQ

Your company is developing a .NET application that stores part of the information in an Azure Storage account. The application will be installed on end users' computers.

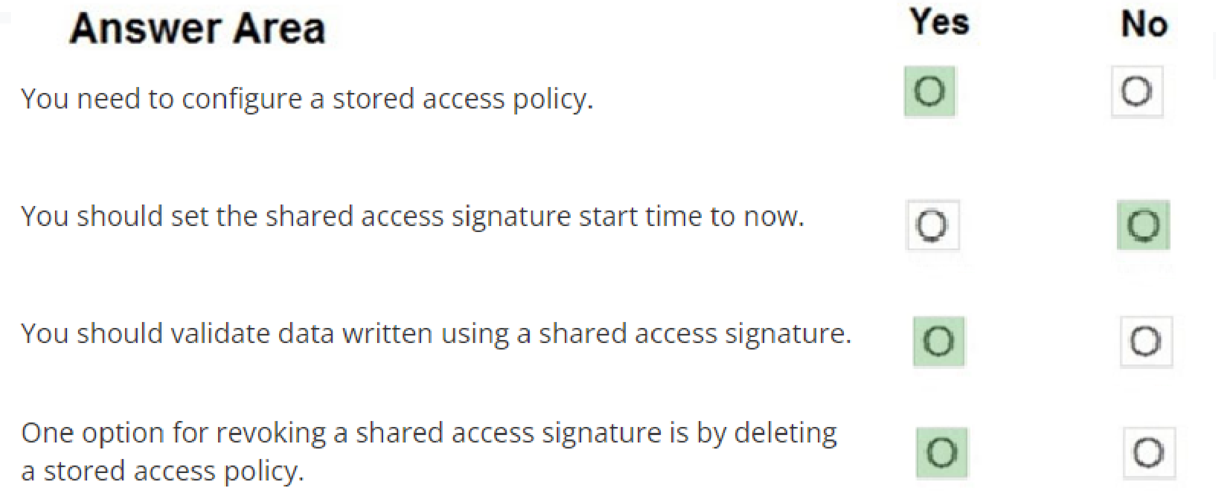
You need to ensure that the information stored in the storage account is accessed in a secure way, so you ask the developers to use a shared access signature when accessing said information. You need to make the required configurations on the storage account to follow security best practices and enable access to the account with immediate effect.
For each of the following statements, select Yes if the statement is true. Otherwise, select No.



Answer Area

	Yes	No
You need to configure a stored access policy.	○	○
You should set the shared access signature start time to now.	○	○
You should validate data written using a shared access signature.	○	○
One option for revoking a shared access signature is by deleting a stored access policy.	○	○

Correct Answer:



Answer Area

	Yes	No
You need to configure a stored access policy.	[✓ ○]	○
You should set the shared access signature start time to now.	○	[✓ ○]
You should validate data written using a shared access signature.	[✓ ○]	○
One option for revoking a shared access signature is by deleting a stored access policy.	[✓ ○]	○

Explanation:

You need to configure a stored access policy. When you use a shared access signature, you have two different options. You can either use an ad-hoc shared access signature or configure a stored access policy. By using an ad-hoc shared access signature, you specify the start time, expiration time, and permissions in the Uniform Resource Identifier (URI). If someone copies this URI, they will have the same level of access as the corresponding user. This means that this type of shared access signature can be used by anyone in the world. By configuring a stored access policy, you define the start time, expiration time, and permissions in the policy and then associate a shared access signature with that policy. You can associate more than one shared access signature with the same policy.

You should not set the shared access signature start time to now. When you set the start time of a shared access signature to now, there can be slight differences in the clocks of the servers that host the storage account. These differences could lead to an access problem for a few minutes after the configuration. If you need your shared access signature to be available as soon as possible, you should set the start time to 15 minutes before the current time, or you can just not set the start time. Not setting the start time parameter means that the shared access signature will be active immediately.

You should validate data written using a shared access signature. When the user uses a shared access signature, the information they write to the storage account can cause problems, such as communication Issues or corruption. Because of this, it is a best practice to validate the data written to the storage account after it is written and before the information is used by any other service or application.

You can revoke a shared access signature by deleting a stored access policy. If you associate a shared access signature with a stored access policy, the start time, expiration time, and permissions are inherited from the policy. If you remove the policy, you are invalidating the shared access signature, thus making it unusable. Keep in mind that if you remove a stored access policy with an associated shared access signature and then create another stored access policy with the exact same name as the original policy, the associated shared access signature will be enabled again.

Question 183 CertyIQ

You are asked to configure an Azure storage account to be accessible from only one specific Virtual Network in an Azure Virtual Network (VNet). It must not be accessible from any other network or region in use across your company's Azure subscription.

You need to implement this requirement.

What should you do?

Choose the correct answer

A. Add a network security group.

B. Activate the Secure transfer required option.

C. Create a VNet service endpoint.

D. Deploy Azure Traffic Manager.

Explanation:

You should implement a VNet service endpoint. Service endpoints are used to limit network access to a specific set of resources. To meet the requirement, you can implement a storage endpoint on an Azure Resource Manager deployed storage account to restrict access to a specific VNet and exclude access from all other resources, including the internet and on-premises connected resources.

You should not add a network security group. This is used to limit access to the resources within a VNet by implementing rules such as IP filters and role-based access control (RBAC). It cannot restrict access to a storage account by itself.

You should not deploy Azure Traffic Manager. This is used to control the flow of network traffic into and out of Azure networks. It cannot restrict access to a storage account by itself.

You should not activate the Secure transfer required option. This feature forces all the traffic into and out of the storage account to be secured over HTTPS instead of allowing fallback to HTTP.

Question 184 CertyIQ

You manage several Windows Server virtual machines (VMs) located in a virtual network (VNet) named prod-vnet. These VMs are used internally by development staff and are not accessible from the internet.

You need to provide your development staff with secure access to object and table data to support their Azure-based applications. The storage account data must reside in Azure and must not be exposed to the internet.

What two actions should you perform? Each correct answer presents part of the solution.

Choose the correct answers

A. Configure a service endpoint.

B. Configure an Azure content delivery network (CDN) profile.

C. Deploy a general-purpose storage account.

D. Deploy a blob storage account.

E. Deploy an Azure File Sync group.

F. Configure a Point-to-Site (P2S) virtual private network (VPN).

Explanation:

You should deploy a general-purpose storage account, and then configure a service endpoint. A general purpose storage account consists of four services, two of which are called for in this scenario:

- Binary large object (blob) object storage
- Table (key-value pair) storage
- Queue (messaging) storage
- File (Server Message Block (SMB) file share) storage

Service endpoints allow you to bind certain Azure services, including storage accounts and Azure SQL Databases, to a VNet in order to restrict their access. In this scenario, you would create a service endpoint on prod-vnet to allow the Microsoft.Storage resource provider access. You would then complete the configuration by associating the storage account with the target VNet.

You should not deploy a blob storage account because a blob storage account has only one service (object storage) and the scenario requires both object and table storage to support your developers. The blob storage account includes access tiers that save costs on cool and cold (archival) storage for block blobs such as documents or media files.

You should not deploy an Azure File Sync group. Azure File Sync is a mechanism offering tiered and synchronized storage for on-premises Server Message Block (SMB) file shares. This feature meets none of the scenario's requirements.

You should not configure an Azure content delivery network (CDN) profile. CDN profiles are used in conjunction with Azure App Service web applications to deliver static website assets to worldwide customers with low latency.

You should not configure a Point-to-Site virtual protected network (P2S VPN) A P25 VPN is appropriate when you need to give individual users a secure connection to an Azure VNet. In this scenario, you are concerned with providing secure access from the VNet to a storage account.

Question 185 CertyIQ

You create a binary large object (blob) storage account named reportstorage99 that contains archival reports from past corporate board meetings.

A board member requests access to a specific report. The member does not have an Azure Active Directory (Azure AD) user account. Moreover, he has access only to a web browser on his Google Chromebook device

You need to provide the board member with least-privilege access to the requested report while maintaining security compliance and minimizing administrative overhead.

What should you do?

Choose the correct answer

A. Generate a shared access signature token for the report and share the Uniform Resource Locator (URL) with the board member.

B. Copy the report to an Azure File Service share and provide the board member with a PowerShell connection script.

C. Create an Azure AD account for the board member and grant him role-based access control (RBAC) access to the storage account.

D. Deploy a point-to-site virtual private network (VPN) connection on the board member's Chromebook and grant the board member role-based access control (RBAC) access to the report

Explanation:

You should generate an shared access signature token for the report and share the Uniform Resource Locator (URL) with the board member, shared access signature enables you to define time limited read-only or read write access to Azure storage account resources. It is important that you set the time restriction properly because the shared access signature includes no authentication. Any person with access to the URL can access the target resource(s) within the token's lifetime. In this case, you both minimize administrative effort as well as maintain security compliance because the shared access signature token points only to a single file, not the entire blob container that hosts the requested report.

You should not create an Azure AD account for the board member and grant him RBAC access to the storage account. First, it requires significant management overhead to create and manage Azure AD accounts, even for external (guest) users. Second, shared access signature and not RBAC is the way Azure provides screened access to individual storage account resources. You can use RBAC roles only at the storage account scope.

You should not copy the report to an Azure File Service share and provide the board member with a PowerShell connection script. Here you create security and governance problems by creating multiple copies of the source report, as well as producing unnecessary administrative complexity.

You should not deploy a point-to-site (P2S) VPN connection on the board member's Chromebook and grant the board member RBAC access to the report. The scenario stipulates that the board member is limited to using a web browser on his Chromebook. Furthermore, the Azure P2S VPN client is supported only on Windows, macOS, and endorsed Linux distributions. Chrome OS is not supported.

Question 186

CertyIQ

The development team asks you to provision an Azure storage account for their use.

To maintain compliance with IT security policy, you need to ensure that the new Azure storage account meets the following requirements:

- Access keys should be kept in a secure way and be programmatically accessible.
- Access keys must facilitate automatic rotation.
- The company must manage the access keys.

What should you do?

Choose the correct answer

A. Enable Storage Service Encryption (SSE) on the storage account.

B. Require secure transfer for the storage account.

C. Create a service endpoint between the storage account and a virtual network (VNet).

D. Configure the storage account to store its keys in Azure Key Vault.

Explanation:

You should configure the storage account to store its keys in Azure Key Vault. Azure Key Vault provides a secure mechanism to store secrets, such as storage account keys, user credentials, and digital certificates. in the Microsoft

Azure cloud. You can access the underlying Representational State Transfer (REST) application programming interface (API) to rotate or retrieve the secrets in your source code.

You should not enable SSE on the storage account for two reasons: first, SSE is enabled automatically on all Azure storage accounts and encrypts all storage account data at rest; and second, SSE in its native form uses Microsoft-managed access keys, which violates the scenario constraint for customer-managed keys.

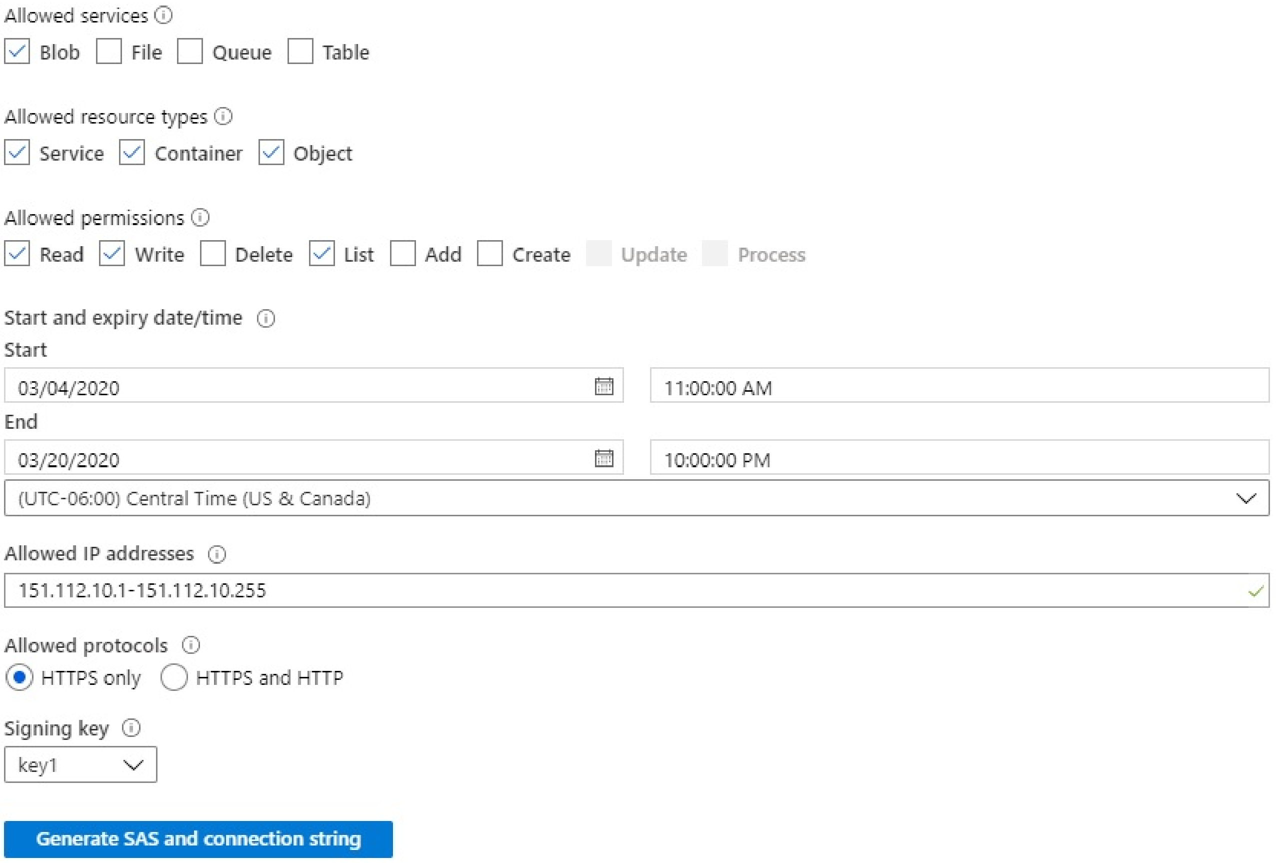
You should not require secure transfer for the storage account. Secure transfer forces all REST API calls to use HTTPS instead of HTTP. This feature has nothing to do with either access keys or their management and rotation.

You should not create a service endpoint between the storage account and a VNet. A service endpoint allows you to limit traffic to a storage account from resources residing on an Azure VNet.

Question 187 CertyIQ

You have a storage account named salesstorage in a subscription named Sales Subscription. You create a container in a blob storage named salescontainer.

You create the shared access signature (SAS) shown in the below exhibit:



Allowed services

☑ Blob □ File □ Queue □ Table

Allowed resource types

☑ Service ☑ Container ☑ Object

Allowed permissions

☑ Read ☑ Write □ Delete ☑ List □ Add □ Create □ Update □ Process

Start and expiry date/time

Start

03/04/2020 11:00:00 AM

End

03/20/2020 10:00:00 PM

(UTC-06:00) Central Time (US & Canada)

Allowed IP addresses

151.112.10.1-151.112.10.255

Allowed protocols

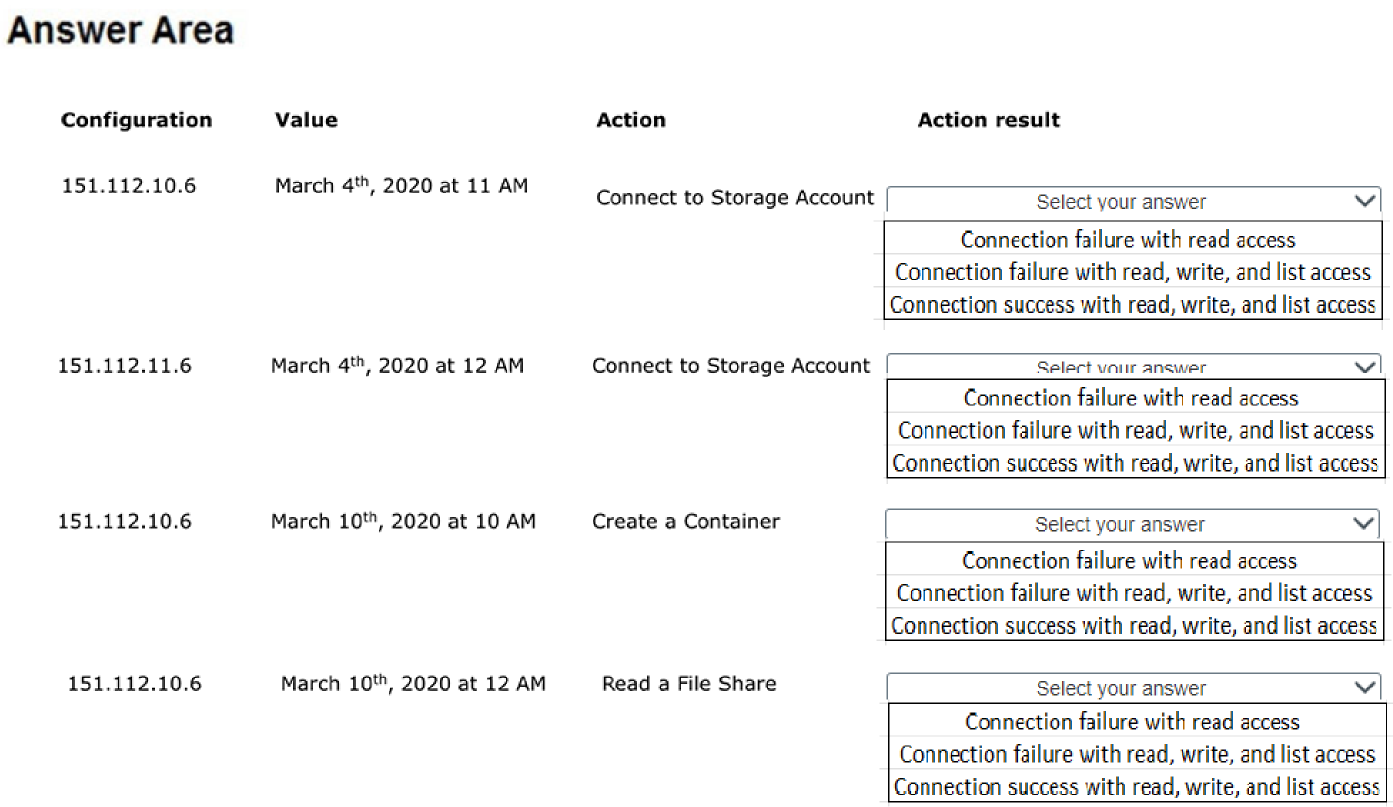
● HTTPS only ○ HTTPS and HTTP

Signing key

key1

You try to carry out actions from several computers at different times using the SAS key1 configurations shown in the exhibit.

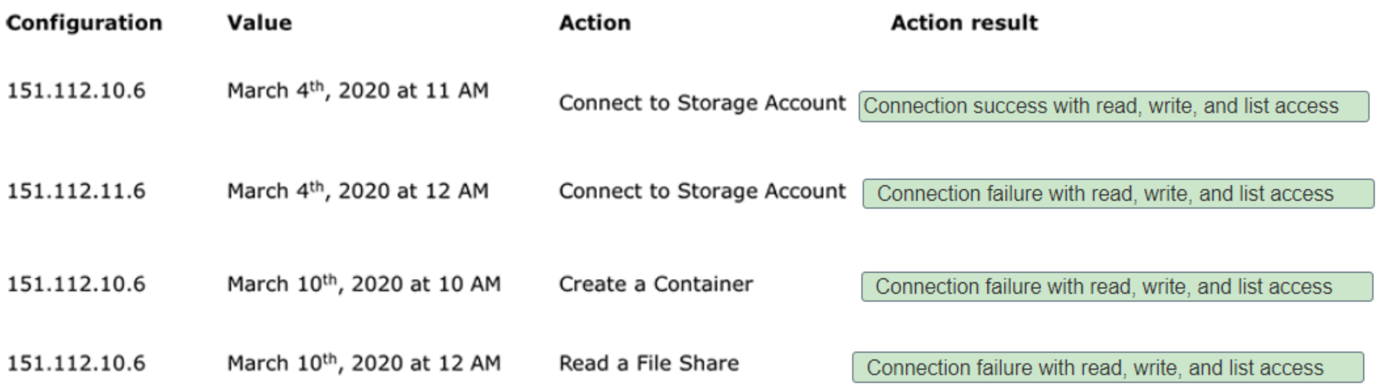
What level of access would be available in each scenario? To answer, select the appropriate options from the drop-down menus.



Answer Area

Configuration	Value	Action	Action result
151.112.10.6	March 4th, 2020 at 11 AM	Connect to Storage Account	Select your answer Connection failure with read access Connection failure with read, write, and list access Connection success with read, write, and list access
151.112.11.6	March 4th, 2020 at 12 AM	Connect to Storage Account	Select your answer Connection failure with read access Connection failure with read, write, and list access Connection success with read, write, and list access
151.112.10.6	March 10th, 2020 at 10 AM	Create a Container	Select your answer Connection failure with read access Connection failure with read, write, and list access Connection success with read, write, and list access
151.112.10.6	March 10th, 2020 at 12 AM	Read a File Share	Select your answer Connection failure with read access Connection failure with read, write, and list access Connection success with read, write, and list access

Correct Answer: -



Configuration	Value	Action	Action result
151.112.10.6	March 4th, 2020 at 11 AM	Connect to Storage Account	Connection success with read, write, and list access
151.112.11.6	March 4th, 2020 at 12 AM	Connect to Storage Account	Connection failure with read, write, and list access
151.112.10.6	March 10th, 2020 at 10 AM	Create a Container	Connection failure with read, write, and list access
151.112.10.6	March 10th, 2020 at 12 AM	Read a File Share	Connection failure with read, write, and list access

Explanation:

In the first scenario, you would have connection success with read, write, and list access, because the IP address and the dates meet the criteria when the shared access signature (SAS) key1 is active.

In the second scenario, you would have connection failure with read, write, and list access, because the IP address does not fall in the allowed IP address range.

In the third scenario, you would have connection failure with read, write, and list access, because the permissions provided for the SAS key1 do not grant permissions to create a new container.

In the fourth scenario, you would have connection failure with read, write, and list access, because the permissions granted are only for containers and not file shares.

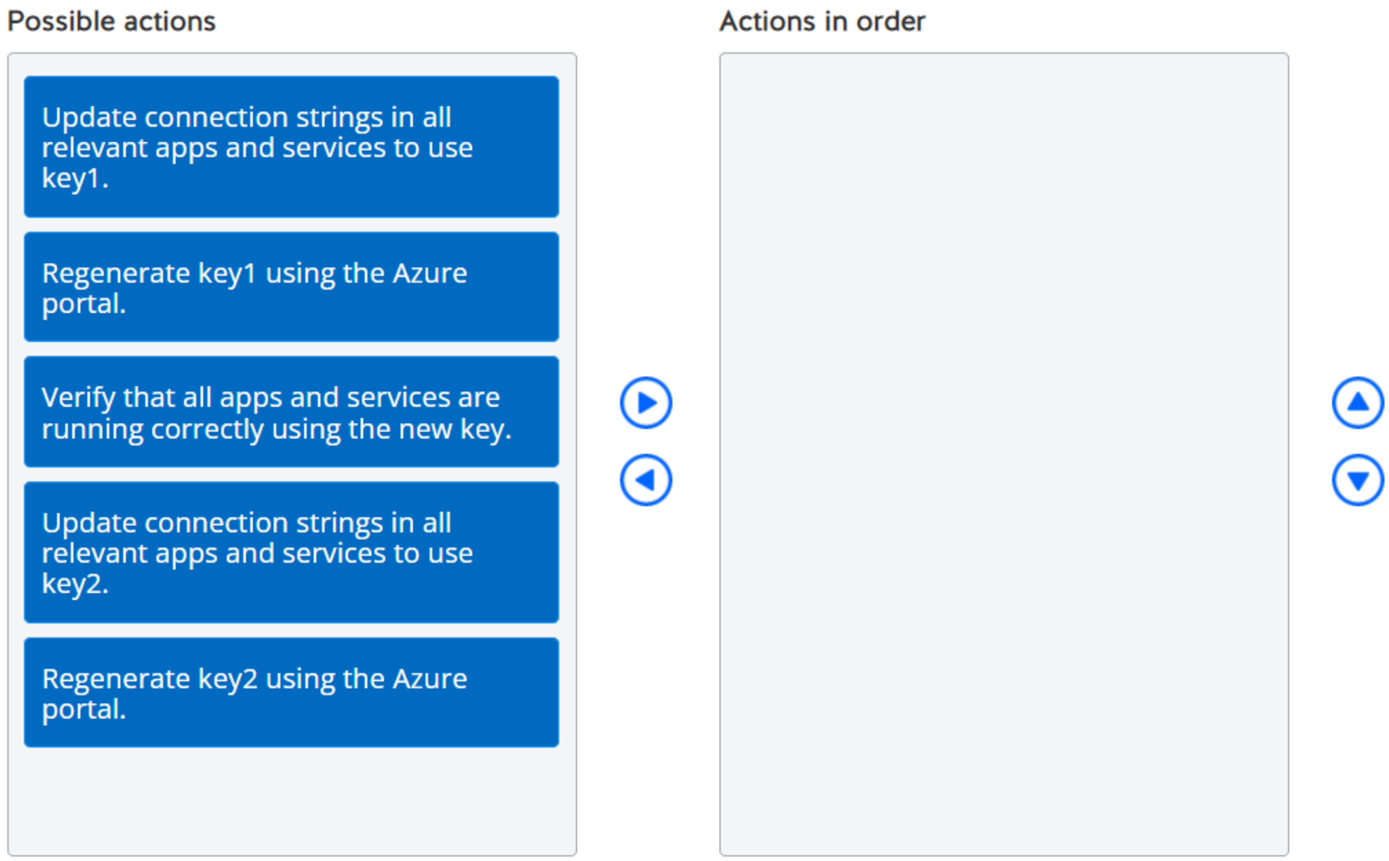
Question 188

You have two storage account keys: key1 and key2. Your apps and services use key!, and you maintain key2 as a backup key.

You are concerned that both keys may have been compromised. You want to use the Azure portal to regenerate them without interrupting access to the storage account.

Which four actions should you perform in sequence? To answer, move the appropriate actions from the list of possible actions to the answer area and arrange them in the correct order.

Create a list in the correct order

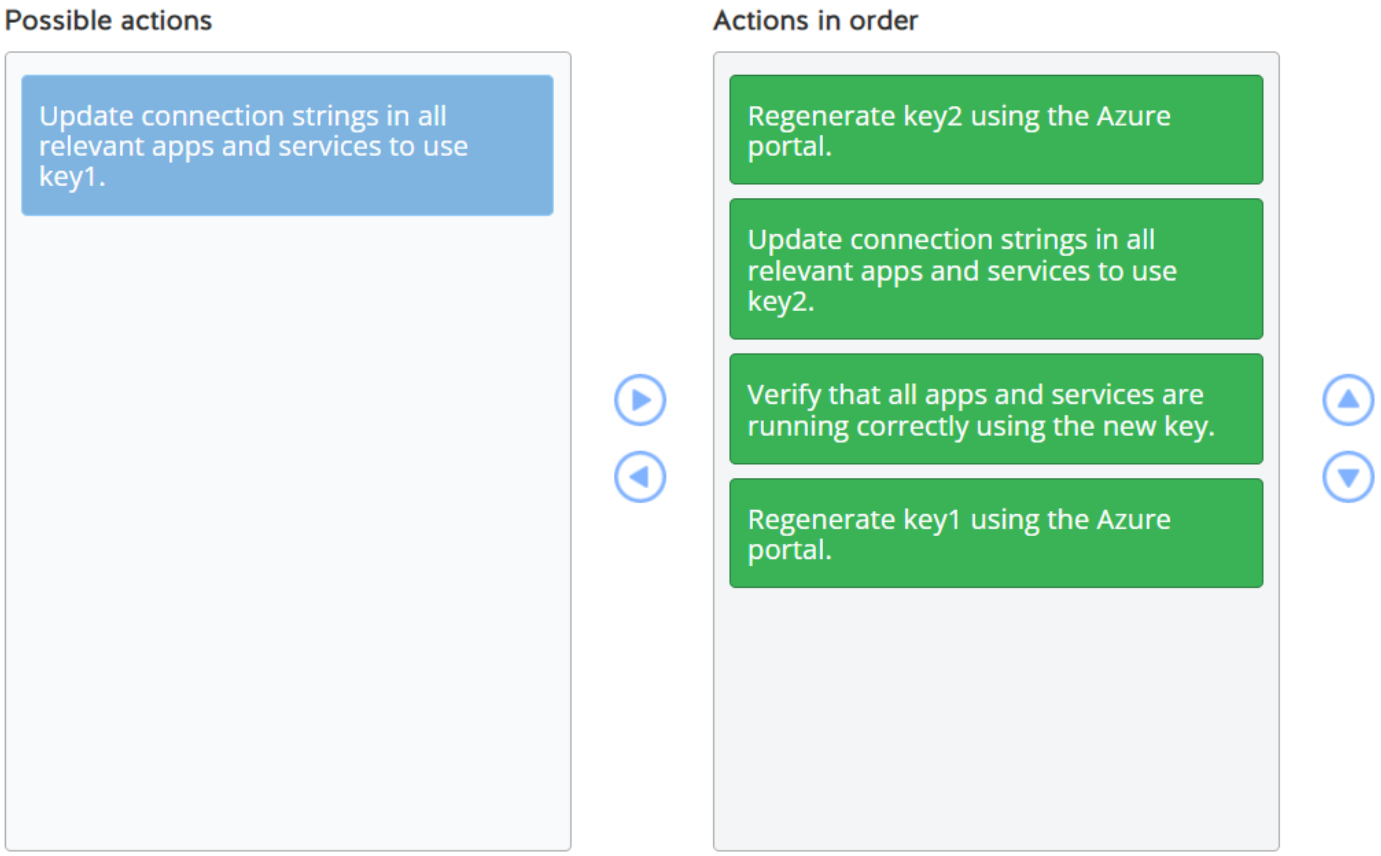


Possible actions

- Update connection strings in all relevant apps and services to use key1.
- Regenerate key1 using the Azure portal.
- Verify that all apps and services are running correctly using the new key.
- Update connection strings in all relevant apps and services to use key2.
- Regenerate key2 using the Azure portal.

Actions in order

Correct Answer: -



Possible actions

- Update connection strings in all relevant apps and services to use key1.

Actions in order

- Regenerate key2 using the Azure portal.
- Update connection strings in all relevant apps and services to use key2.
- Verify that all apps and services are running correctly using the new key.
- Regenerate key1 using the Azure portal.

Explanation:

You need to perform the following steps in order:

1. Regenerate key2 using the Azure portal.
2. Update connection strings in all relevant apps and services to use key2.
3. Verify that all apps and services are running correctly using the new key.
4. Regenerate key1 using the Azure portal.

You first regenerate key2 because the apps and services are currently using key1 to gain access to stored data, and you do not want to interrupt their access.

Next, you change the storage key to key2 in the apps and services and then verify that they can gain access to storage. This is important because the apps and services will not be able to use the previous primary key after it is regenerated.

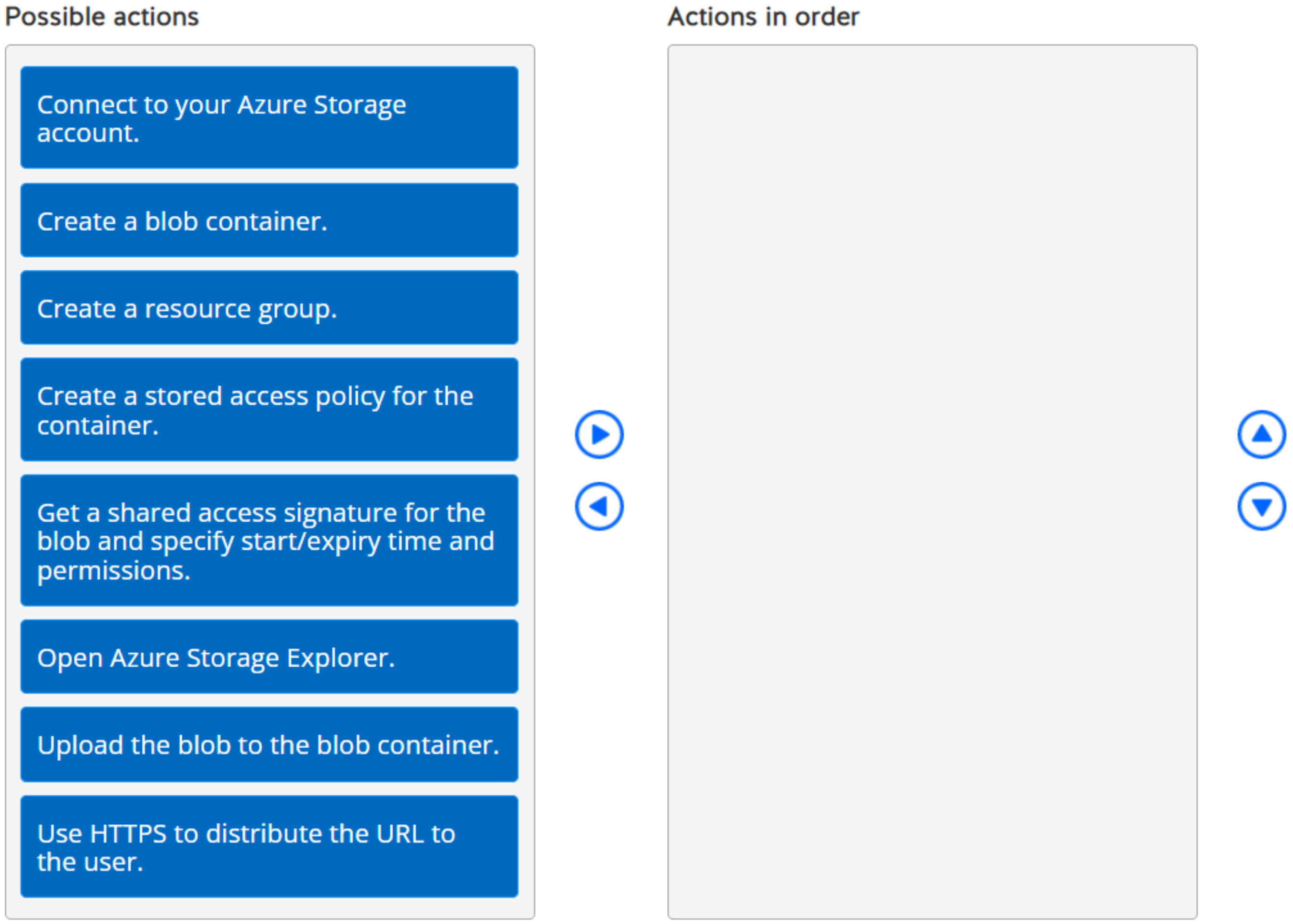
Finally, you regenerate key1.

Question 189 CertyIQ

You need to give a user temporary read and write permissions to a blob by using an ad hoc shared access signature.

Which six actions should you perform in sequence? To answer, move the appropriate actions from the list of possible actions to the answer area and arrange them in the correct order.

Create a list in the correct order

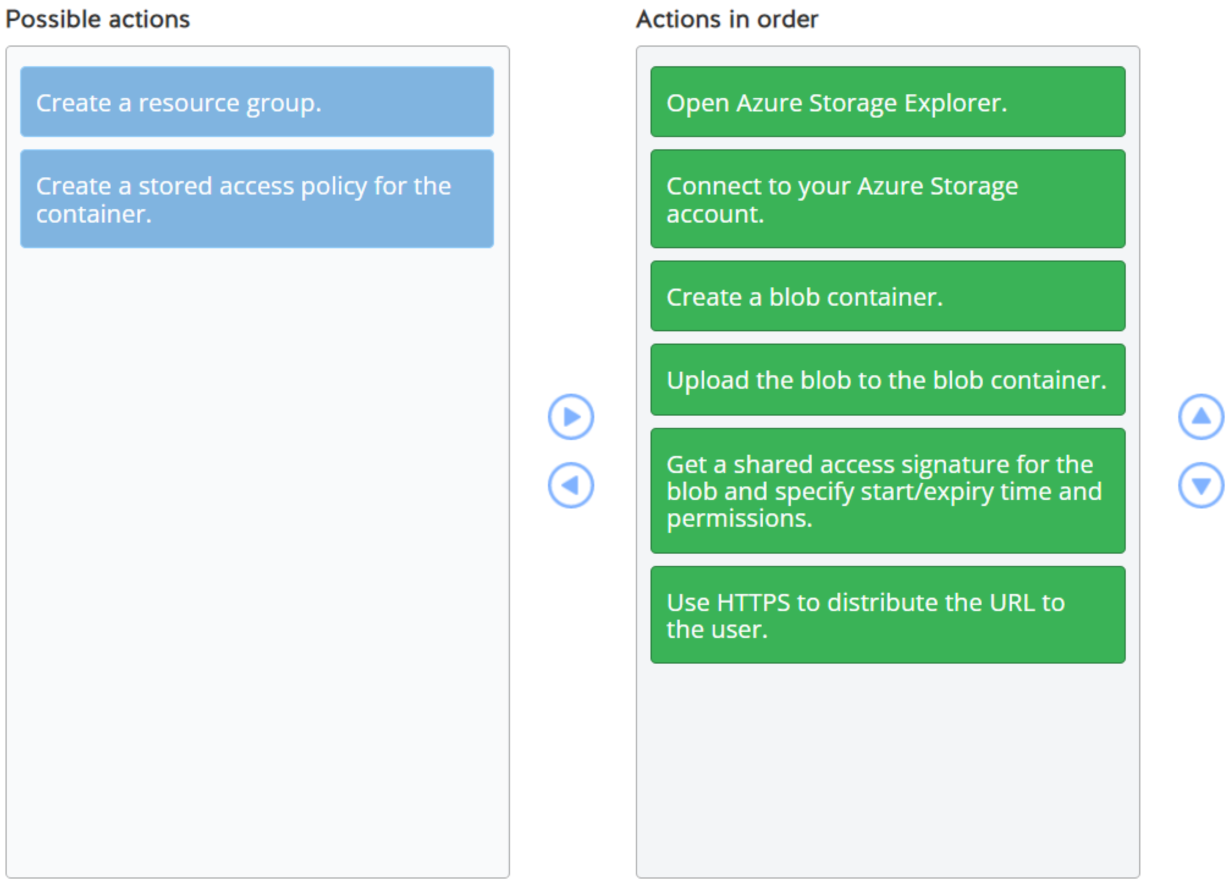


Possible actions

- Connect to your Azure Storage account.
- Create a blob container.
- Create a resource group.
- Create a stored access policy for the container.
- Get a shared access signature for the blob and specify start/expiry time and permissions.
- Open Azure Storage Explorer.
- Upload the blob to the blob container.
- Use HTTPS to distribute the URL to the user.

Actions in order

Correct Answer: -



Possible actions

- Create a resource group.
- Create a stored access policy for the container.

Actions in order

- Open Azure Storage Explorer.
- Connect to your Azure Storage account.
- Create a blob container.
- Upload the blob to the blob container.
- Get a shared access signature for the blob and specify start/expiry time and permissions.
- Use HTTPS to distribute the URL to the user.

Explanation:

You need to perform the following steps in order:

1. Open Azure Storage Explorer.

2. Connect to your Azure Storage account.

3. Create a blob container.

4. Upload the blob to the blob container.

5. Get a shared access signature for the blob and specify start/expiry time and permissions.

6. Use HTTPS to distribute the URL to the user.

You use Azure Storage Explorer to manage your storage account as well as to upload and download blobs, files, and other resources. After you open Azure Storage Explorer, you connect to your storage account

Next, you create a blob container for the blob you will grant access to, and then you upload the blob. Blobs are always uploaded to a container so they can be more easily organized.

You generate a shared access signature for the blob simply by right-clicking, selecting Get Shared Access Signature, and then specifying the start/expiry time and permissions. Finally, you use HTTPS to distribute the shared access signature to the user. Using HTTP can leave your blob vulnerable to improper access because the shared access signature token could be intercepted during communication.

You should not create a resource group. You already have a storage account, so that means that you also already have a resource group. It is not necessary to create another resource group.

You should not create a stored access policy for the container. In this scenario, you are creating an ad hoc shared access signature, and the start time, expiry time, and permissions are specified in the shared access signature URI. With a stored access policy, the start time, expiry time, and permissions are defined in the policy. A shared access signature that is associated with the policy inherits those constraints.

Case Study

Question 190

CertyIQ

Instructions

This case study contains 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.

Note: You cannot go back or review questions of this type on the actual certification exam.

You have an Azure resource group named RG1. RG1 contains a Linux virtual machine (VM) named VM

You need to automate the deployment of 20 additional Linux VMs. The new VMs should be based upon

VMT's configuration.

Solution From the virtual machine's Export Template settings blade, you click Deploy and edit the parameters.

Does this solution meet the goal?

A. Yes

B. No

Explanation:

The solution meets the goal. Every deployment in Azure is described in a template in JavaScript Object Notation (JSON) format. You can access the underlying template from the Export Template settings blade of the VM resource, and can then deploy multiple new instances of a resource by modifying the template parameters.

Question 191 CertyIQ

Instructions

This case study contains 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.

Note: You cannot go back or review questions of this type on the actual certification exam.

You have an Azure resource group named RG1. RG1 contains a Linux virtual machine (VM) named VM1.

You need to automate the deployment of 20 additional Linux VMs. The new VMs should be based upon VMTS configuration.

Solution: You store the Linux VM properties in a template and deploy the additional VMs by editing the template parameter values for each additional VM.

Does this solution meet the goal?

A. Yes

B. No

Explanation:

The solution meets the goal.

The Templates blade in the Azure portal enables you to store JavaScript Object Notation (JSON) documents that automate Azure resource deployment.

In this case, you could store the Linux VM properties in a template and deploy the 20 additional VMs simply by editing the template parameter values for each additional VM.

Question 192 CertyIQ

Instructions

This case study contains 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.

Note: You cannot go back or review questions of this type on the actual certification exam.

You have an Azure resource group named RG1. RG1 contains a Linux virtual machine (VM) named VM1.

You need to automate the deployment of 20 additional Linux VMs. The new VMs should be based upon VMT's configuration.

Solution: From the resource group's Policies blade, you click Assign policy.

Does this solution meet the goal?

A. Yes

B. No

Explanation:

This solution does not meet the goal. To automate the deployment of the 20 additional VMs, you should access the virtual machine's underlying JavaScript Object Notation (JSON) template and deploy the new resources by using the template and custom deployment parameters. By contrast, Azure Policy is a governance product that makes it easier for Azure administrators to constrain deployments to meet organizational requirements. For example, you could deploy an Azure policy that requires all resource deployments to occur within only company-authorized geographic locations.

Question 193 CertyIQ

Instructions

This case study contains 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.

Note: You cannot go back or review questions of this type on the actual certification exam.

You want to install an internet-facing web application named WebApp1 on multiple Azure virtual machines (VMs). The VMs must run Windows Server 2019. Connections to WebApp1 must be spread across all the VMs. The VMs must be located in separate datacenters in the same region. The Service Level Agreement (SLA) percentage of connectivity must be the highest possible.

Solution: Create three VMs (each in a different availability zone) and create and configure a standard Stock Keeping Unit (SKU) load balancer.

Does this solution meet the goal?

A. Yes

B. No

Explanation:

This solution meets the goal. You need to deploy two or more VMs to different availability zones in the same region to acquire an SLA connectivity percentage of 99.99. This is the highest possible percentage in Azure. An availability zone is made up of one or more datacenters. You also need to create and configure a standard SKU load balancer. This includes creating a zone-redundant standard IP address. This IP address will be replicated across the three zones. Only a standard SKU load balancer offers this feature, the basic SKU does not.

The load balancer will be zone-redundant because the attached IP address is zone-redundant. The load balancer distributes inbound flows to the VMs. This assures connectivity as long as a VM in a single zone has connectivity. A standard load balancer has an SLA of 99.99% when connected to two or more healthy VMs.

Question 194 CertyIQ

Instructions

This case study contains 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.

Note: You cannot go back or review questions of this type on the actual certification exam.

You want to install an internet-facing web application named WebApp1 on multiple Azure virtual machines (VMs). The VMs must run Windows Server 2019. Connections to WebApp1 must be spread across all the VMs. The VMs must be located in separate datacenters in the same region. The Service Level Agreement (SLA) connectivity percentage must be the highest possible.

Solution: Create an availability set with three VMs, three fault domains, and three update domains, and create a basic load balancer.

Does this solution meet the goal?

A. Yes

B. No

Explanation:

This solution does not meet the goal. When you deploy two or more VMs in the same availability set, you will have a guaranteed SLA percentage of 99.95%. This is lower than the maximum of 99.99 percent for VMs deployed into different availability zones. Also, when you deploy VMs in an availability set, the VMs are not deployed into different datacenters. When you create a basic load balancer, you will not get an SLA. Only standard load balancers offer SLAS.

Question 195 CertyIQ

Instructions

This case study contains 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.

Note: You cannot go back or review questions of this type on the actual certification exam.

You want to install an internet-facing web application named WebApp1 on multiple Azure virtual machines (VMs). The VMs must run Windows Server 2019. Connections to WebApp1 must be spread across all the VMs. The VMs must be located in separate datacenters in the same region. The Service Level Agreement (SLA) connectivity percentage must be the highest possible.

Solution: Create three VMs in a single virtual network (VNet), with each VM in a different availability zone, and use Azure Front Door.

Does this solution meet the goal?

A. Yes

B. No

Explanation:

This solution does not meet the goal. Azure Front Door can perform load balancing only at the global level. In this scenario, you need to load balance traffic within a single VNet in a single region. You need to use a load balancer or an application gateway to spread the connections across the VMs.

Question 196 CertyIQ

Instructions

This case study contains 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.

Note: You cannot go back or review questions of this type on the actual certification exam.

You want to install an internet-facing web application named WebApp1 on multiple Azure virtual machines (VMs) The VMs must run Windows Server 2019 Connections to WebApp1 must be spread across all the VMs. The VMs must be located in separate datacenters in the same region. The Service Level Agreement (SLA) connectivity percentage must be the highest possible.

Solution: Create three VMs, set the availability zone to 1, and create a zone-redundant load balancer.

Does this solution meet the goal?

A. Yes

B. No

Explanation:

This solution does not meet the goal. To deploy the VMs to different datacenters inside a region, each VM must be deployed to a different availability zone (1, 2, and 3). This is also required for the highest possible SLA percentage of 99.99.

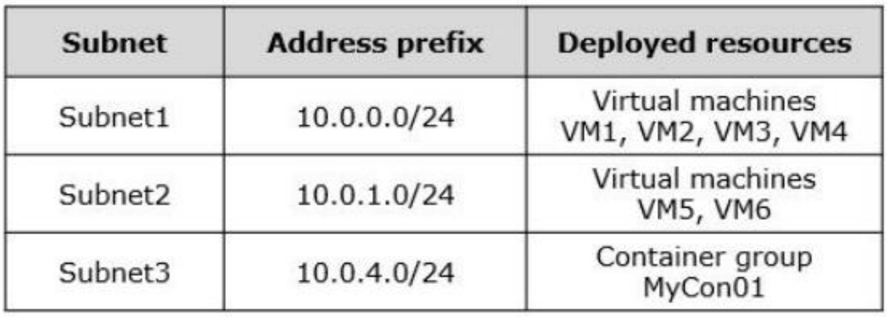
Question 197 CertyIQ

Instructions

This case study contains 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.

Note: You cannot go back or review questions of this type on the actual certification exam.

Exhibit: -



Subnet	Address prefix	Deployed resources
Subnet1	10.0.0.0/24	Virtual machines VM1, VM2, VM3, VM4
Subnet2	10.0.1.0/24	Virtual machines VM5, VM6
Subnet3	10.0.4.0/24	Container group MyCon01

Your company has an Azure subscription. This includes a virtual network (VNet) named VNet1 with the subnets shown in the exhibit.

The company is deploying a new Azure container group on VNet1. The container instances need to communicate with VM5 and VM6.

You need to determine an appropriate location for deploying the container group.

Solution: You create the container group on Subnet2.

Does this solution meet the goal?

A. Yes

B. No

Explanation:

This solution does not meet the goal. You cannot deploy a container group on a subnet that already contains resources such as virtual machines (VMs).

You can deploy a container group on a subnet that already hosts a container group, a subnet that does not host any resources, or you can recreate a new subnet when you create the container group

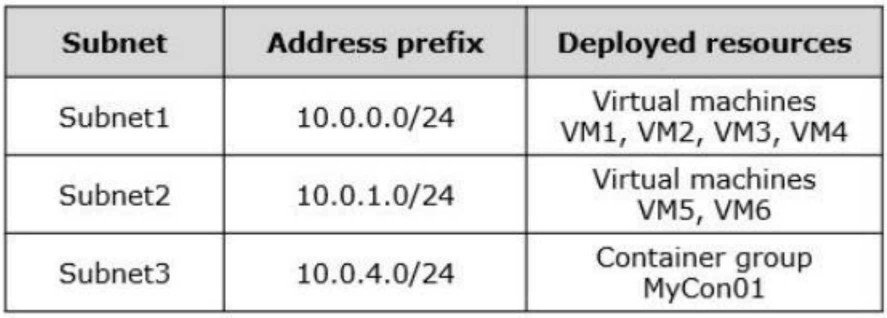
Question 198 CertyIQ

Instructions

This case study contains 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.

Note: You cannot go back or review questions of this type on the actual certification exam.

Exhibit: -



Subnet	Address prefix	Deployed resources
Subnet1	10.0.0.0/24	Virtual machines VM1, VM2, VM3, VM4
Subnet2	10.0.1.0/24	Virtual machines VM5, VM6
Subnet3	10.0.4.0/24	Container group MyCon01

Your company has an Azure subscription. This includes a virtual network (VNet) named VNet1 with the subnets shown in the exhibit.

The company is deploying a new Azure container group on VNet1. The container instances need to communicate with VM5 and VM6.

You need to determine an appropriate location for deploying the container group.

Solution: You create the container group on Subnet3.

Does this solution meet the goal?

A. Yes

B. No

Explanation:

The solution meets the goal. You can deploy a container group on a subnet that already hosts a container group, a subnet that does not host any resources, or you can recreate a new subnet when you create the container group.

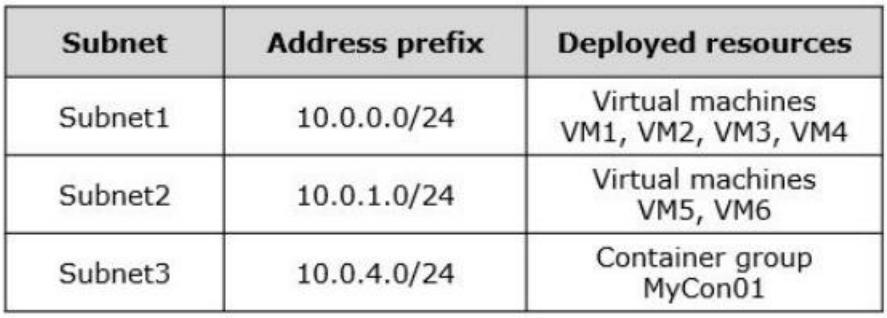
Question 199 CertyIQ

Instructions

This case study contains 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.

Note: You cannot go back or review questions of this type on the actual certification exam.

Exhibit: -



Subnet	Address prefix	Deployed resources
Subnet1	10.0.0.0/24	Virtual machines VM1, VM2, VM3, VM4
Subnet2	10.0.1.0/24	Virtual machines VM5, VM6
Subnet3	10.0.4.0/24	Container group MyCon01

Your company has an Azure subscription. This includes a virtual network (VNet) named VNet! with the subnets shown in the exhibit.

The company is deploying a new Azure container group on VNet1. The container instances need to communicate with VM5 and VM6.

You need to determine an appropriate location for deploying the container group.

Solution: You create a new subnet to host the container group when you create the container group.

Does this solution meet the goal?

A. Yes

B. No

Explanation:

The solution meets the goal. You can deploy a container group on a subnet that already hosts a container group, a subnet that does not host any resources, or you can recreate a new subnet when you create the container group.

Question 200 CertyIQ

Instructions

This case study contains 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.

Note: You cannot go back or review questions of this type on the actual certification exam.

You deploy an Azure web app named MyApp. MyApps runs in a Free pricing tier service plan named MyPlan. During testing, you discover that MyApp stops after 60 minutes and that it cannot be restarted until the next day.

You need to ensure that MyApp can run eight hours each day during the testing period. You want to keep the additional costs incurred to a minimum.

Solution: You change the pricing tier for MyPlan to Shared D1.

Does this solution meet the goal?

A. Yes

B. No

Explanation:

This solution does not meet the goal. The problem is that the Free pricing tier supports no more than 60 minutes of CPU time per day. You should not change the pricing tier for MyPlan to Shared D1. This plan allows only 240 minutes of CPU time per day.

You should change the pricing tier for MyPlan to Basic B1. This is the least expensive plan that supports 24 hour CPU time.

Question 201 CertyIQ

Instructions

This case study contains 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.

Note: You cannot go back or review questions of this type on the actual certification exam.

You deploy an Azure web app named MyApp. MyApps runs in a Free pricing tier service plan named MyPlan. During testing, you discover that MyApp stops after 60 minutes and that it cannot be restarted until the next day.

You need to ensure that MyApp can run eight hours each day during the testing period. You want to keep the additional costs incurred to a minimum.

Solution: You change the pricing tier for MyPlan to Basic B1.

Does this solution meet the goal?

A. Yes

B. No

Explanation:

This solution does meet the goal. You should change the pricing tier for MyPlan to Basic B1. This is the least expensive plan that supports 24-hour CPU time.

Question 202 CertyIQ

Instructions

This case study contains 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.

Note: You cannot go back or review questions of this type on the actual certification exam.

You deploy an Azure web app named MyApp. MyApps runs in a Free pricing tier service plan named MyPlan. During testing, you discover that MyApp stops after 60 minutes and that it cannot be restarted until the next day.

You need to ensure that MyApp can run eight hours each day during the testing period. You want to keep the additional costs incurred to a minimum.

Solution: You change the pricing tier for MyPlan to Standard 51.

Does this solution meet the goal?

A. Yes

B. No

Explanation:

This solution does not meet the goal. The problem is that the Free pricing tier supports no more than 60 minutes of CPU time per day. You should not change the pricing tier for MyPlan to Standard S1. This meets the run time requirement but it is not the least expensive solution.

You should change the pricing tier for MyPlan to Basic B1. This is the least expensive plan that supports 24 hour CPU time.

End of Part 5

We hope to see you again...

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

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

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

Connect with us @ LinkedIn Telegram

Contact us for other dumps: -

contact.certyiqofficial@gmail.com

For any other enquiry, please drop us a mail at

enquiry.certyiqofficial@gmail.com