# Microsoft

## Exam Questions az-500

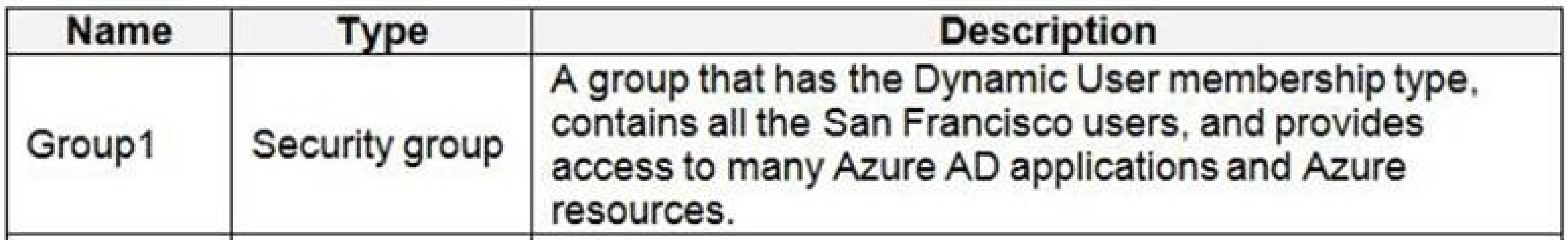
Microsoft Azure Security Technologies

**NEW QUESTION 1**
You need to meet the identity and access requirements for Group1.
What should you do?

A. Add a membership rule to Group1.
B. Delete Group1. Create a new group named Group1 that has a membership type of Office 365. Add users and devices to the group.
C. Modify the membership rule of Group1.
D. Change the membership type of Group1 to Assigne
E. Create two groups that have dynamic membership
F. Add the new groups to Group1.

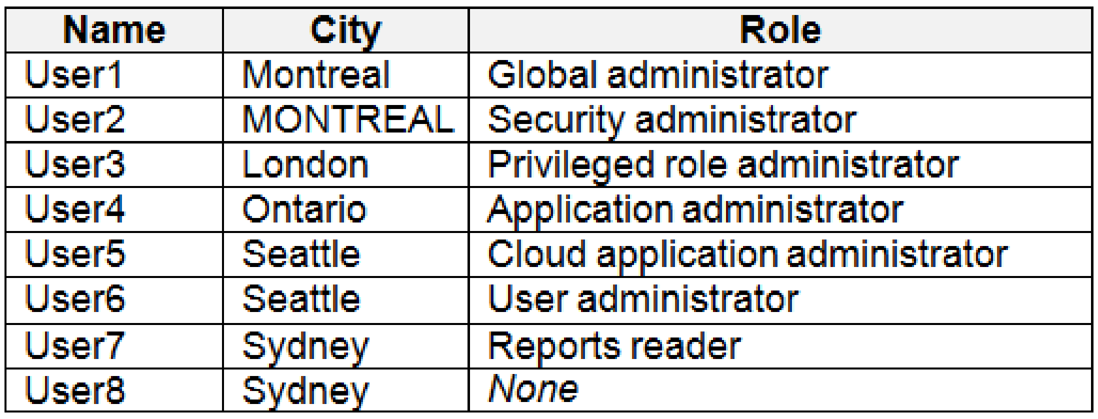
**Answer:** B

**Explanation:**
Incorrect Answers:
A, C: You can create a dynamic group for devices or for users, but you can't create a rule that contains both users and devices.
D: For assigned group you can only add individual members. Scenario:
Litware identifies the following identity and access requirements: All San Francisco users and their devices must be members of Group1. The tenant currently contain this group:



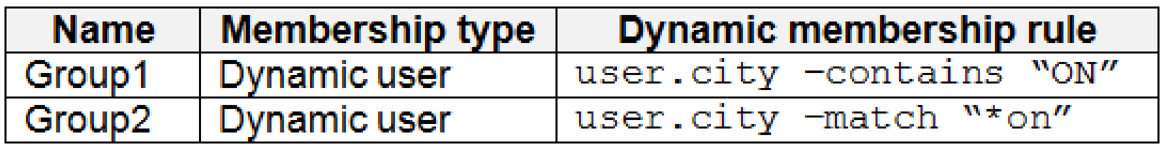
| Name | Type | Description |
|---|---|---|
| Group1 | Security group | A group that has the Dynamic User membership type, contains all the San Francisco users, and provides access to many Azure AD applications and Azure resources. |

References:
https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/groups-dynamic-membership
https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-groups-create-azure-portal
Testlet 2
This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.
To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other question on this case study.
At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next sections of the exam. After you begin a new section, you cannot return to this section.
To start the case study
To display the first question on this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.
Overview
Contoso, Ltd. is a consulting company that has a main office in Montreal and two branch offices in Seattle and New York. The company hosts its entire server infrastructure in Azure.
Contoso has two Azure subscriptions named Sub1 and Sub2. Both subscriptions are associated to an Azure Active Directory (Azure AD) tenant named contoso.com.
Technical requirements
Contoso identifies the following technical requirements:
Deploy Azure Firewall to VNetWork1 in Sub2.
Register an application named App2 in contoso.com.
Whenever possible, use the principle of least privilege.
Enable Azure AD Privileged Identity Management (PIM) for contoso.com
Contoso.com contains the users shown in the following table.



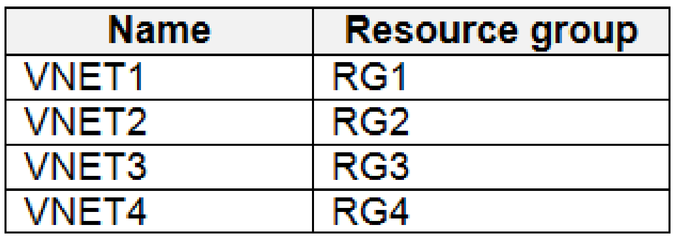
| Name | City | Role |
|---|---|---|
| User1 | Montreal | Global administrator |
| User2 | MONTREAL | Security administrator |
| User3 | London | Privileged role administrator |
| User4 | Ontario | Application administrator |
| User5 | Seattle | Cloud application administrator |
| User6 | Seattle | User administrator |
| User7 | Sydney | Reports reader |
| User8 | Sydney | *None* |

Contoso.com contains the security groups shown in the following table.



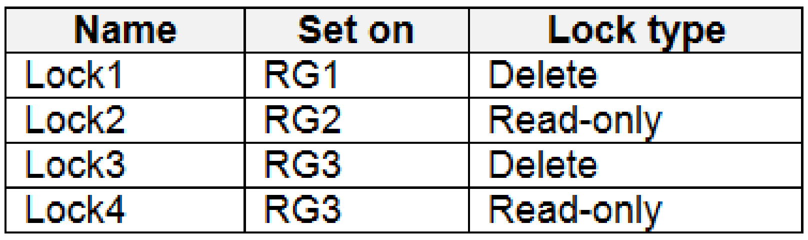
| Name | Membership type | Dynamic membership rule |
|---|---|---|
| Group1 | Dynamic user | `user.city -contains “ON”` |
| Group2 | Dynamic user | `user.city -match “*on”` |

Sub1
Sub1 contains six resource groups named RG1, RG2, RG3, RG4, RG5, and RG6.
User2 creates the virtual networks shown in the following table.



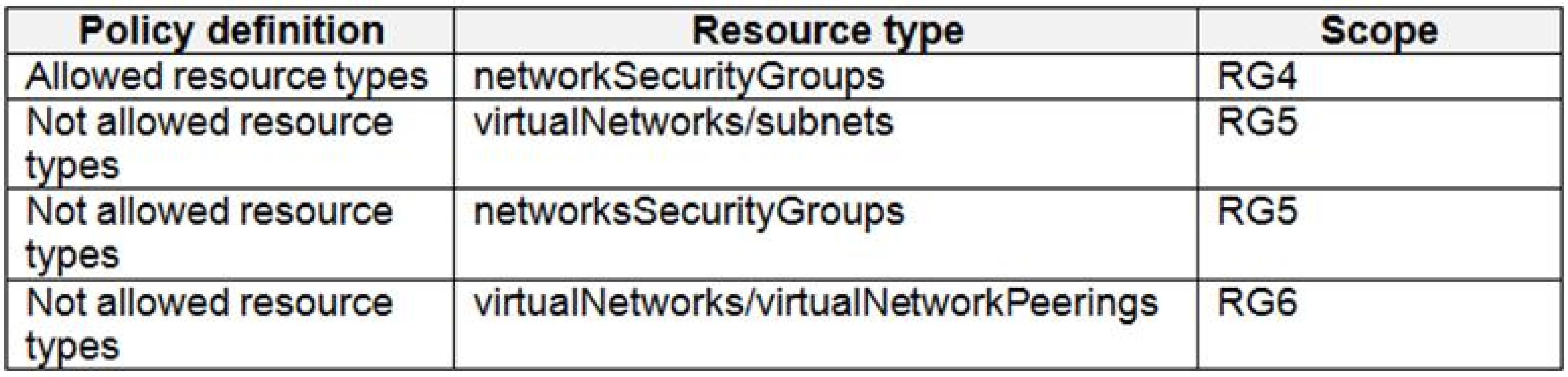
| Name | Resource group |
|---|---|
| VNET1 | RG1 |
| VNET2 | RG2 |
| VNET3 | RG3 |
| VNET4 | RG4 |

Sub1 contains the locks shown in the following table.



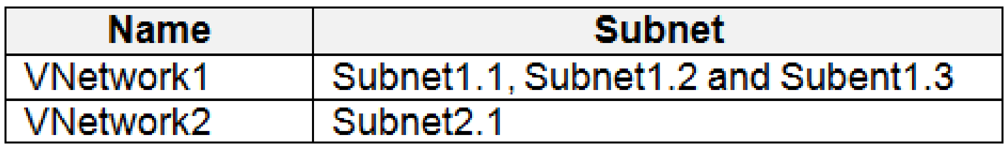
| Name | Set on | Lock type |
|---|---|---|
| Lock1 | RG1 | Delete |
| Lock2 | RG2 | Read-only |
| Lock3 | RG3 | Delete |
| Lock4 | RG3 | Read-only |

Sub1 contains the Azure policies shown in the following table.



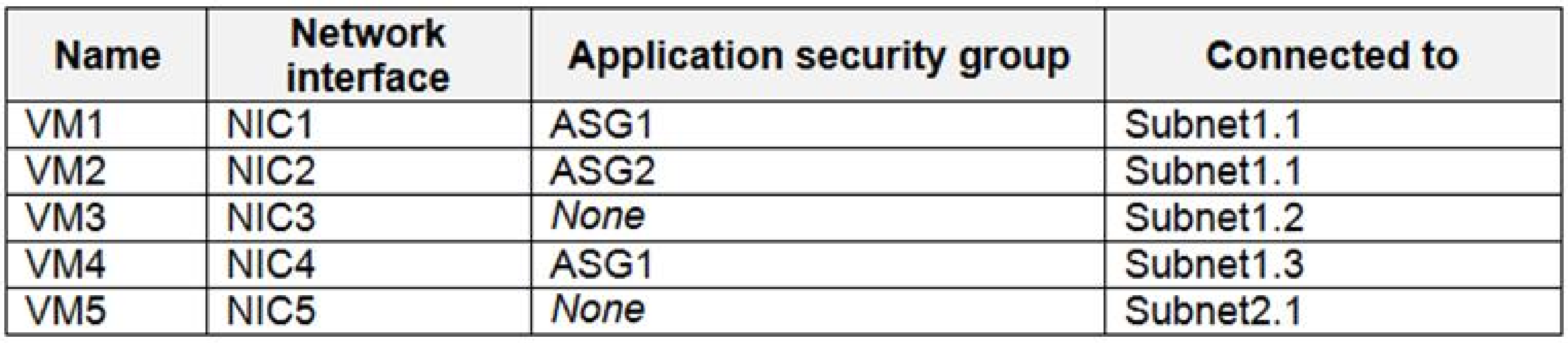
| Policy definition | Resource type | Scope |
|---|---|---|
| Allowed resource types | networkSecurityGroups | RG4 |
| Not allowed resource types | virtualNetworks/subnets | RG5 |
| Not allowed resource types | networksSecurityGroups | RG5 |
| Not allowed resource types | virtualNetworks/virtualNetworkPeerings | RG6 |

Sub2



| Name | Subnet |
|---|---|
| VNetwork1 | Subnet1.1, Subnet1.2 and Subent1.3 |
| VNetwork2 | Subnet2.1 |

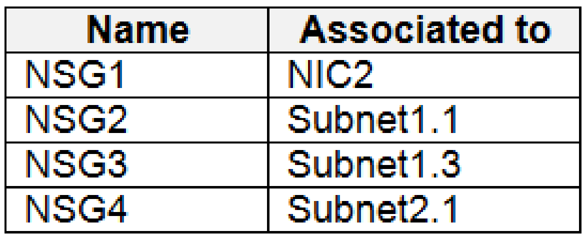
Sub2 contains the virtual machines shown in the following table.



| Name | Network interface | Application security group | Connected to |
|---|---|---|---|
| VM1 | NIC1 | ASG1 | Subnet1.1 |
| VM2 | NIC2 | ASG2 | Subnet1.1 |
| VM3 | NIC3 | *None* | Subnet1.2 |
| VM4 | NIC4 | ASG1 | Subnet1.3 |
| VM5 | NIC5 | *None* | Subnet2.1 |

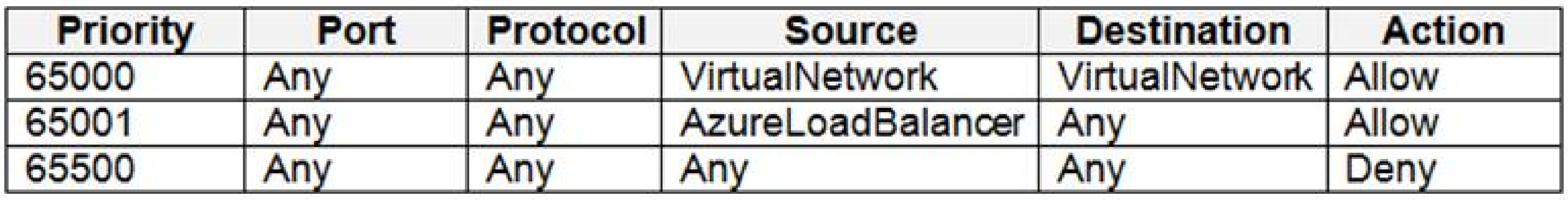
All virtual machines have the public IP addresses and the Web Server (IIS) role installed. The firewalls for each virtual machine allow ping requests and web requests.

Sub2 contains the network security groups (NSGs) shown in the following table.



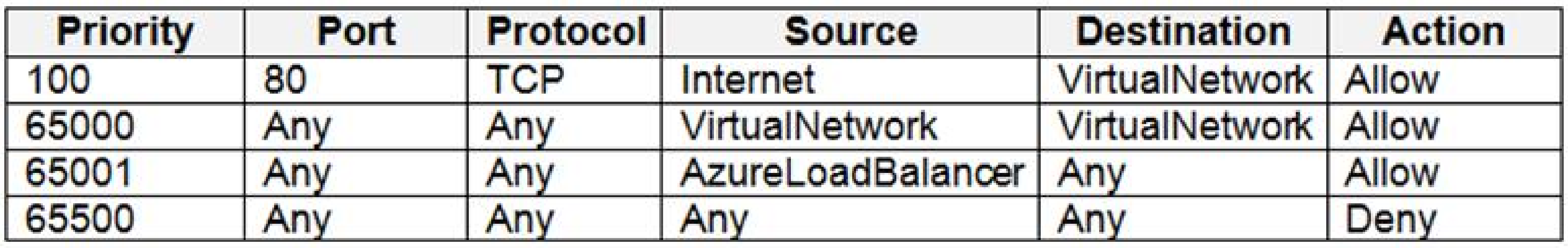
| Name | Associated to |
|---|---|
| NSG1 | NIC2 |
| NSG2 | Subnet1.1 |
| NSG3 | Subnet1.3 |
| NSG4 | Subnet2.1 |

NSG1 has the inbound security rules shown in the following table.



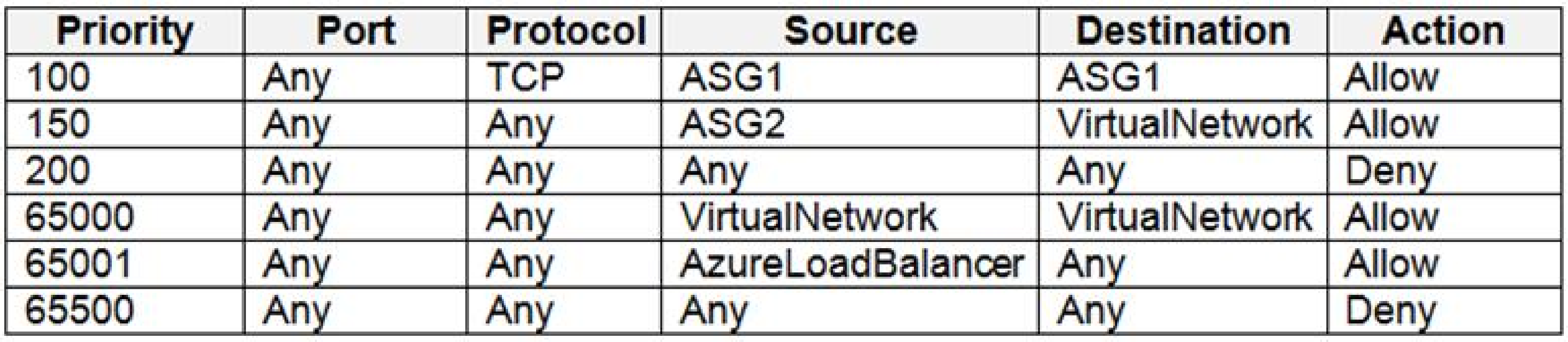
| Priority | Port | Protocol | Source | Destination | Action |
|---|---|---|---|---|---|
| 65000 | Any | Any | VirtualNetwork | VirtualNetwork | Allow |
| 65001 | Any | Any | AzureLoadBalancer | Any | Allow |
| 65500 | Any | Any | Any | Any | Deny |

NSG2 has the inbound security rules shown in the following table.



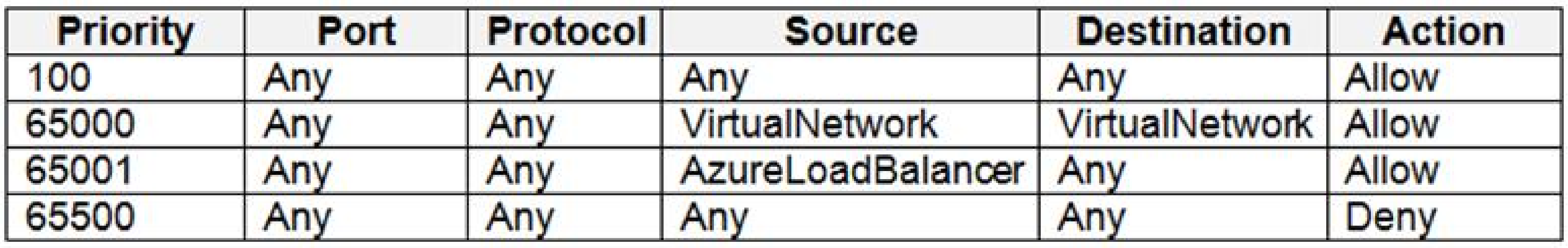
| Priority | Port | Protocol | Source | Destination | Action |
|---|---|---|---|---|---|
| 100 | 80 | TCP | Internet | VirtualNetwork | Allow |
| 65000 | Any | Any | VirtualNetwork | VirtualNetwork | Allow |
| 65001 | Any | Any | AzureLoadBalancer | Any | Allow |
| 65500 | Any | Any | Any | Any | Deny |

NSG3 has the inbound security rules shown in the following table.



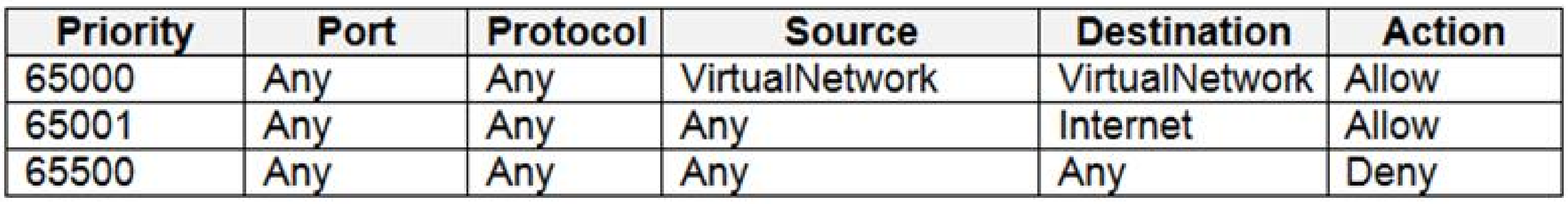
| Priority | Port | Protocol | Source | Destination | Action |
|---|---|---|---|---|---|
| 100 | Any | TCP | ASG1 | ASG1 | Allow |
| 150 | Any | Any | ASG2 | VirtualNetwork | Allow |
| 200 | Any | Any | Any | Any | Deny |
| 65000 | Any | Any | VirtualNetwork | VirtualNetwork | Allow |
| 65001 | Any | Any | AzureLoadBalancer | Any | Allow |
| 65500 | Any | Any | Any | Any | Deny |

NSG4 has the inbound security rules shown in the following table.



| Priority | Port | Protocol | Source | Destination | Action |
|---|---|---|---|---|---|
| 100 | Any | Any | Any | Any | Allow |
| 65000 | Any | Any | VirtualNetwork | VirtualNetwork | Allow |
| 65001 | Any | Any | AzureLoadBalancer | Any | Allow |
| 65500 | Any | Any | Any | Any | Deny |

NSG1, NSG2, NSG3, and NSG4 have the outbound security rules shown in the following table.



| Priority | Port | Protocol | Source | Destination | Action |
|---|---|---|---|---|---|
| 65000 | Any | Any | VirtualNetwork | VirtualNetwork | Allow |
| 65001 | Any | Any | Any | Internet | Allow |
| 65500 | Any | Any | Any | Any | Deny |

Contoso identifies the following technical requirements:
* Deploy Azure Firewall to VNetwork1 in Sub2.
* Register an application named App2 in contoso.com.
* Whenever possible, use the principle of least privilege.
* Enable Azure AD Privileged Identity Management (PIM) for contoso.com.m.

**NEW QUESTION 2**
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have an Azure Subscription named Sub1.
You have an Azure Storage account named Sa1 in a resource group named RG1.
Users and applications access the blob service and the file service in Sa1 by using several shared access signatures (SASs) and stored access policies. You discover that unauthorized users accessed both the file service and the blob service.
You need to revoke all access to Sa1. Solution: You generate new SASs. Does this meet the goal?

A. Yes
B. No

**Answer:** B

**Explanation:**
Instead you should create a new stored access policy.
To revoke a stored access policy, you can either delete it, or rename it by changing the signed identifier. Changing the signed identifier breaks the associations between any existing signatures and the stored access policy. Deleting or renaming the stored access policy immediately affects all of the shared access signatures associated with it.
References:
https://docs.microsoft.com/en-us/rest/api/storageservices/Establishing-a-Stored-Access-Policy

**NEW QUESTION 3**
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have an Azure Subscription named Sub1.
You have an Azure Storage account named Sa1 in a resource group named RG1.
Users and applications access the blob service and the file service in Sa1 by using several shared access signatures (SASs) and stored access policies. You discover that unauthorized users accessed both the file service and the blob service.
You need to revoke all access to Sa1.
Solution: You create a new stored access policy. Does this meet the goal?

A. Yes
B. No

**Answer:** A

**Explanation:**
To revoke a stored access policy, you can either delete it, or rename it by changing the signed identifier. Changing the signed identifier breaks the associations between any existing signatures and the stored access policy. Deleting or renaming the stored access policy immediately effects all of the shared access signatures associated with it.
References:
https://docs.microsoft.com/en-us/rest/api/storageservices/Establishing-a-Stored-Access-Policy

**NEW QUESTION 4**
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a hybrid configuration of Azure Active Directory (AzureAD). You have an Azure HDInsight cluster on a virtual network.
You plan to allow users to authenticate to the cluster by using their on-premises Active Directory credentials. You need to configure the environment to support the planned authentication.
Solution: You deploy the On-premises data gateway to the on-premises network. Does this meet the goal?

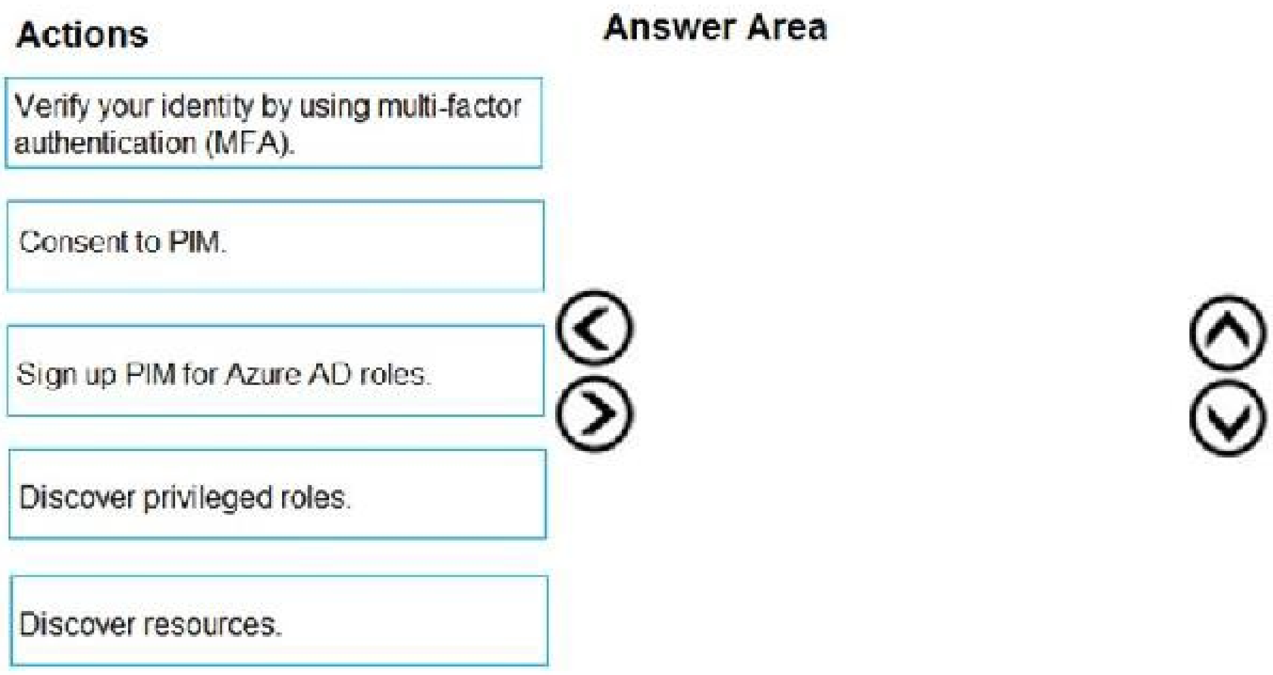
A. Yes
B. No

**Answer:** B

**Explanation:**
Instead, you connect HDInsight to your on-premises network by using Azure Virtual Networks and a VPN gateway.
- Note: To allow HDInsight and resources in the joined network to communicate by name, you must perform the following actions: Create Azure Virtual Network.
- Create a custom DNS server in the Azure Virtual Network.
- Configure the virtual network to use the custom DNS server instead of the default Azure Recursive Resolver. Configure forwarding between the custom DNS server and your on-premises DNS server.

References:
https://docs.microsoft.com/en-us/azure/hdinsight/connect-on-premises-network

**NEW QUESTION 5**
DRAG DROP
You create an Azure subscription.
You need to ensure that you can use Azure Active Directory (Azure AD) Privileged Identity Management (PIM) to secure Azure AD roles.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.
Select and Place:



Actions

Verify your identity by using multi-factor authentication (MFA).

Consent to PIM.

Sign up PIM for Azure AD roles.

Discover privileged roles.

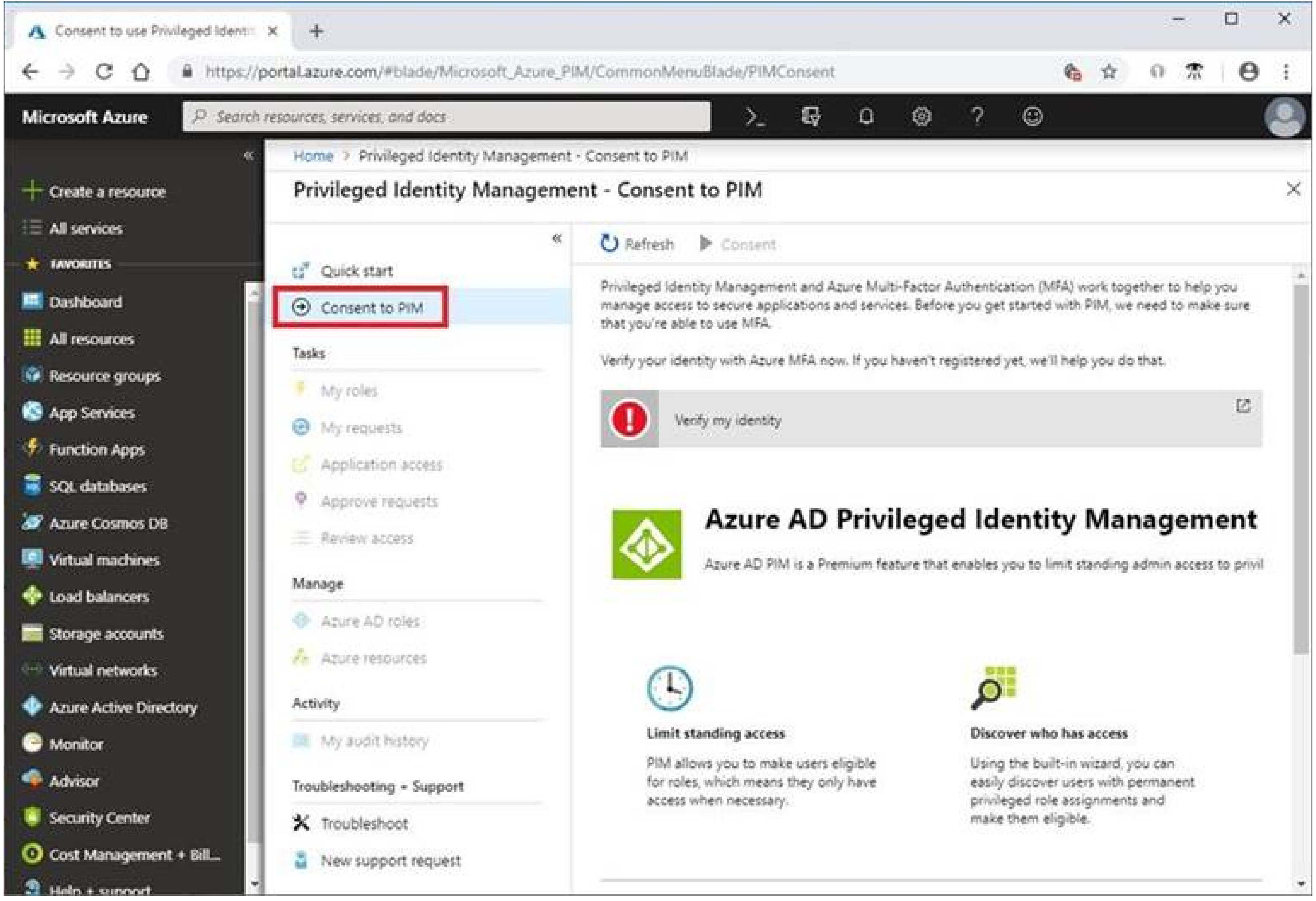
Discover resources.

Answer Area

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**
Step 1: Consent to PIM



Privileged Identity Management - Consent to PIM

Privileged Identity Management and Azure Multi-Factor Authentication (MFA) work together to help you manage access to secure applications and services. Before you get started with PIM, we need to make sure that you're able to use MFA.

Verify your identity with Azure MFA now. If you haven't registered yet, we'll help you do that.

Azure AD Privileged Identity Management

Azure AD PIM is a Premium feature that enables you to limit standing admin access to privil

Limit standing access

PIM allows you to make users eligible for roles, which means they only have access when necessary.

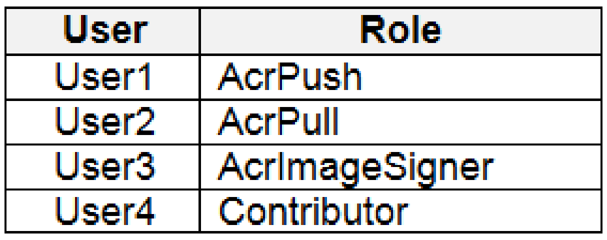
Discover who has access

Using the built-in wizard, you can easily discover users with permanent privileged role assignments and make them eligible.

Step: 2 Verify your identity by using multi-factor authentication (MFA)
Click Verify my identity to verify your identity with Azure MFA. You'll be asked to pick an account.
Step 3: Sign up PIM for Azure AD roles

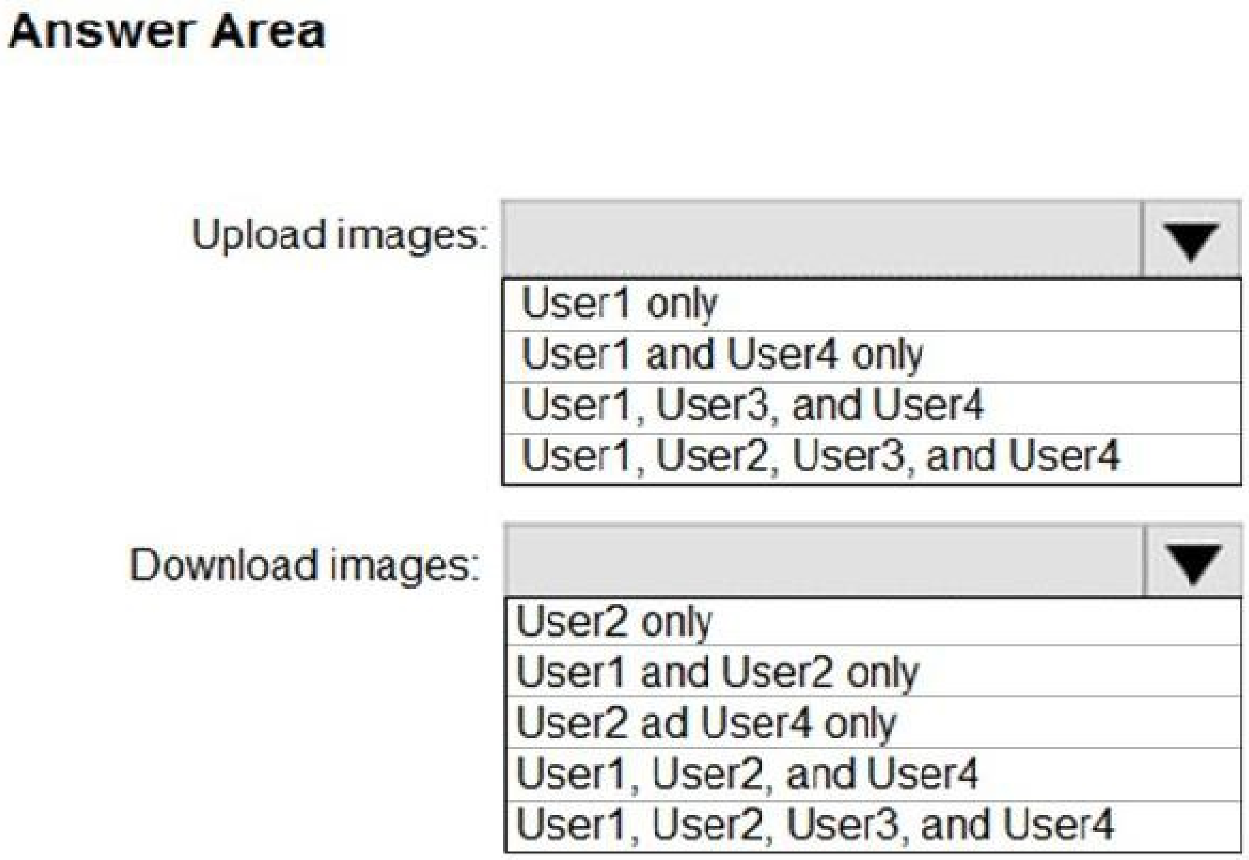
Once you have enabled PIM for your directory, you'll need to sign up PIM to manage Azure AD roles.
References:
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-getting-started

**NEW QUESTION 6**
HOTSPOT
You have an Azure Container Registry named Registry1.
You add role assignment for Registry1 as shown in the following table.



| User | Role |
|---|---|
| User1 | AcrPush |
| User2 | AcrPull |
| User3 | AcrImageSigner |
| User4 | Contributor |

Which users can upload images to Registry1 and download images from Registry1? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Hot Area:



**Answer Area**

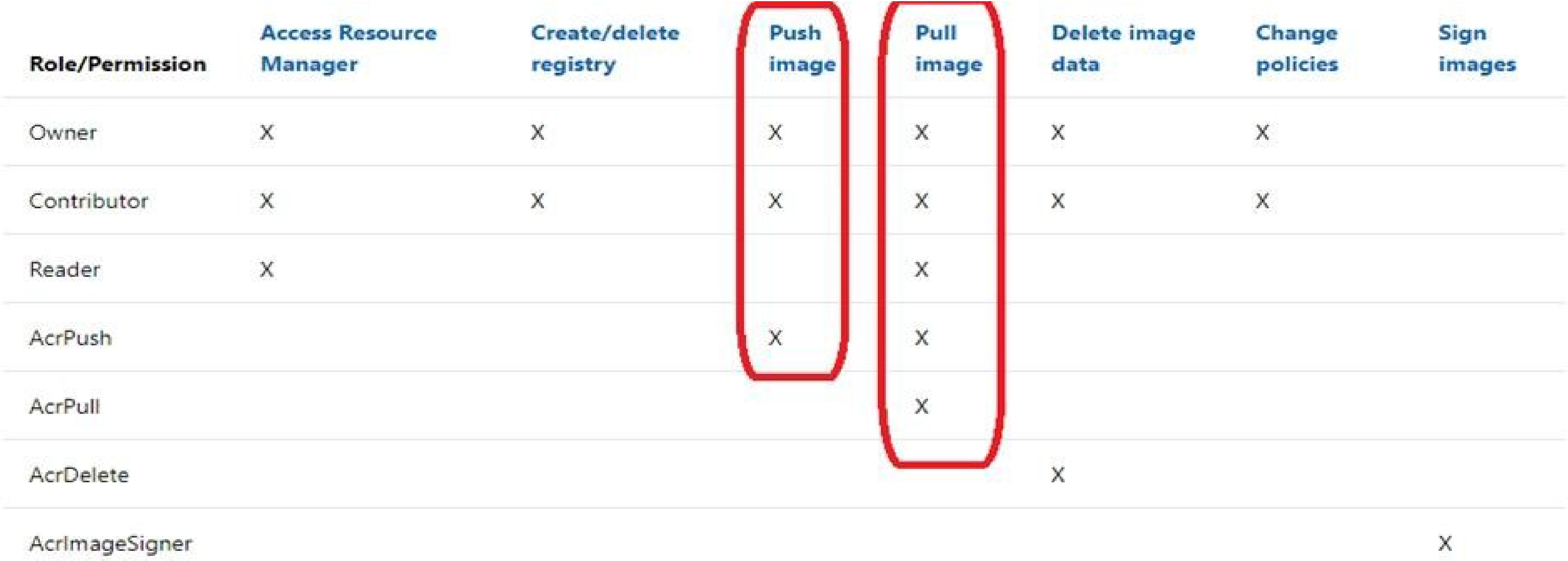
Upload images: ▼
- User1 only
- User1 and User4 only
- User1, User3, and User4
- User1, User2, User3, and User4

Download images: ▼
- User2 only
- User1 and User2 only
- User2 ad User4 only
- User1, User2, and User4
- User1, User2, User3, and User4

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**
Box 1: User1 and User4 only
Owner, Contributor and AcrPush can push images.
Box 2: User1, User2, and User4
All, except AcrImagineSigner, can download/pull images.



| Role/Permission | Access Resource Manager | Create/delete registry | Push image | Pull image | Delete image data | Change policies | Sign images |
|---|---|---|---|---|---|---|---|
| Owner | X | X | X | X | X | X | |
| Contributor | X | X | X | X | X | X | |
| Reader | X | | | X | | | |
| AcrPush | | | X | X | | | |
| AcrPull | | | | X | | | |
| AcrDelete | | | | | X | | |
| AcrImageSigner | | | | | | | X |

References:
https://docs.microsoft.com/bs-latn-ba/azure/container-registry/container-registry-roles

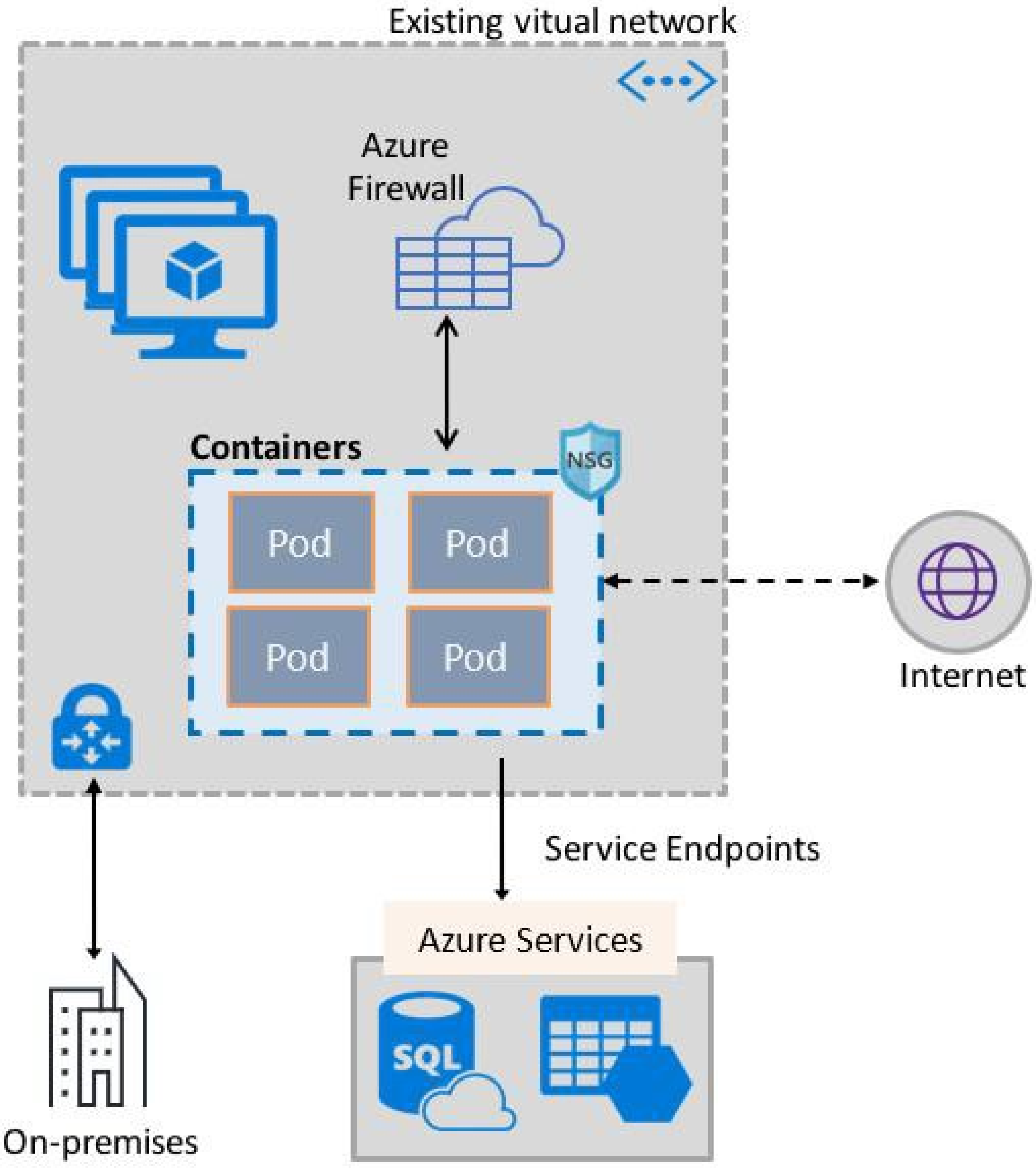
**NEW QUESTION 7**

You have an Azure subscription named Sub1. Sub1 contains a virtual network named VNet1 that contains one subnet named Subnet1.
You create a service endpoint for Subnet1.
Subnet1 contains an Azure virtual machine named VM1 that runs Ubuntu Server 18.04.
You need to deploy Docker containers to VM1. The containers must be able to access Azure Storage resources and Azure SQL databases by using the service endpoint.

A. Create an application security group and a network security group (NSG).
B. Edit the docker-compose.yml file.
C. Install the container network interface (CNI) plug-in.

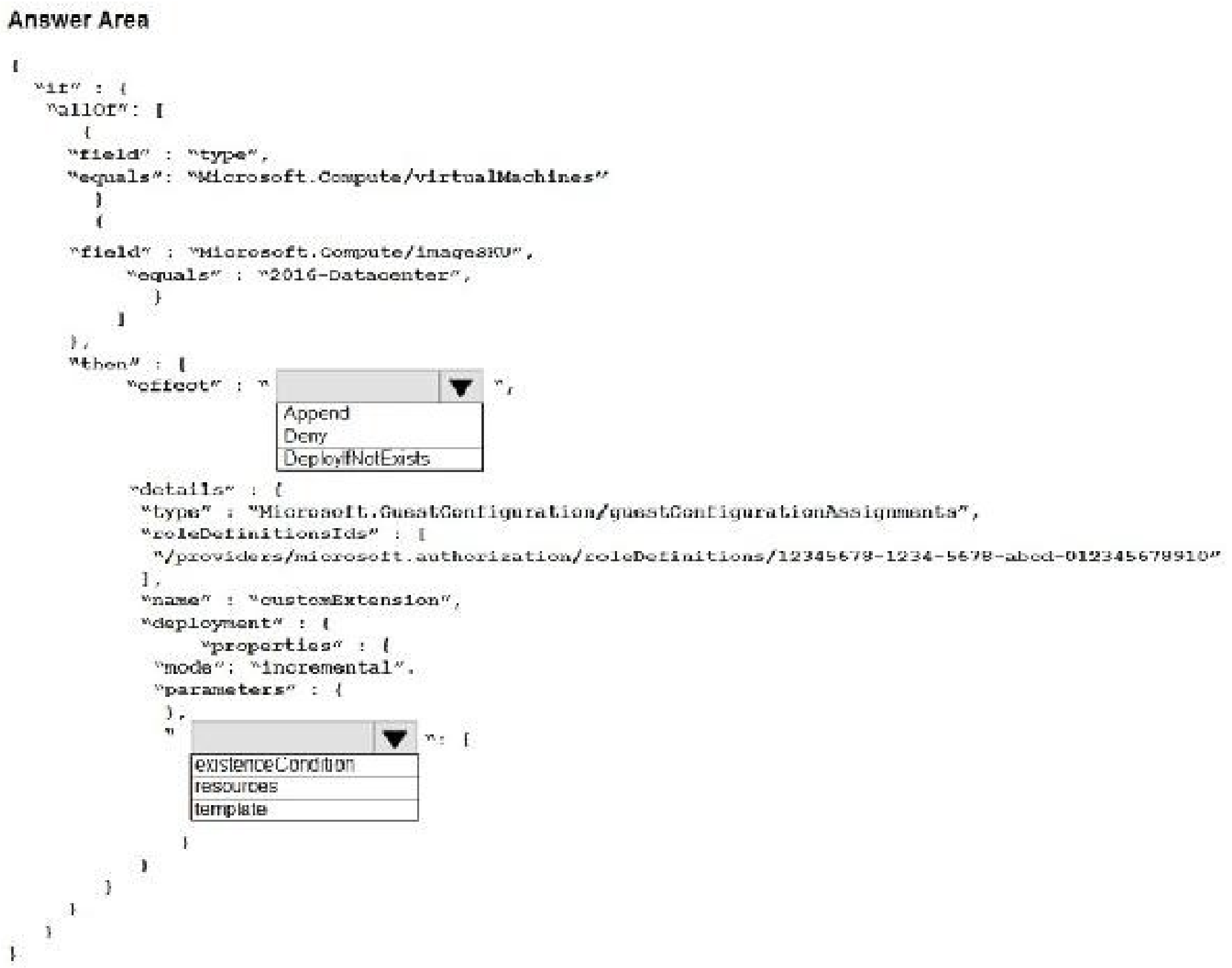
**Answer:** C

**Explanation:**
The Azure Virtual Network container network interface (CNI) plug-in installs in an Azure Virtual Machine. The plug-in supports both Linux and Windows platform.
The plug-in assigns IP addresses from a virtual network to containers brought up in the virtual machine, attaching them to the virtual network, and connecting them directly to other containers and virtual network resources. The plug-in doesn't rely on overlay networks, or routes, for connectivity, and provides the same performance as virtual machines.
The following picture shows how the plug-in provides Azure Virtual Network capabilities to Pods:



References:
https://docs.microsoft.com/en-us/azure/virtual-network/container-networking-overview

**NEW QUESTION 8**
HOTSPOT
You have an Azure subscription. The subscription contains Azure virtual machines that run Windows Server 2016.
You need to implement a policy to ensure that each virtual machine has a custom antimalware virtual machine extension installed. How should you complete the policy? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Hot Area:



Answer Area

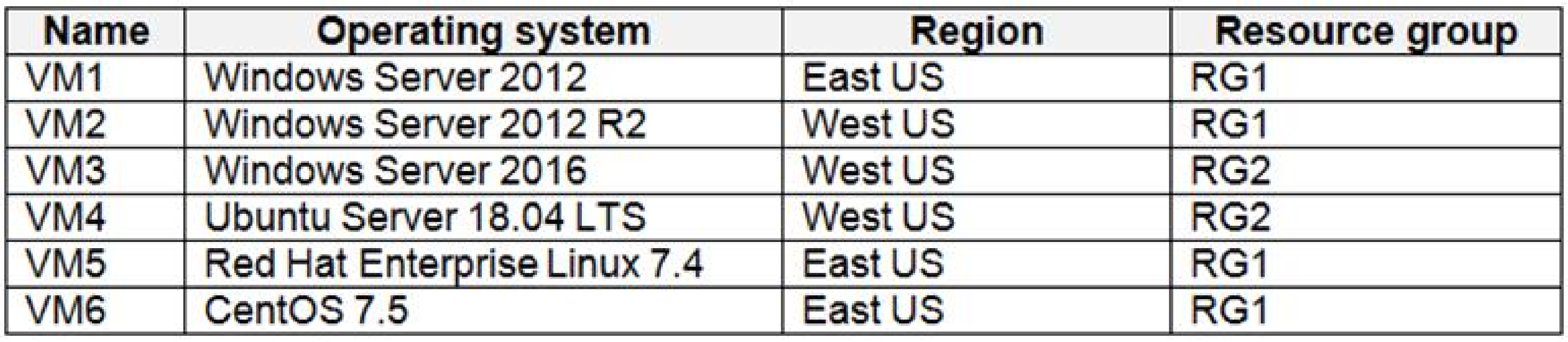
```
{
  "if" : {
   "allOf": [
      {
    "field" : "type",
    "equals": "Microsoft.Compute/virtualMachines"
       }
       {
    "field" : "Microsoft.Compute/imageSKU",
         "equals" : "2016-Datacenter",
            }
       ]
    },
    "then" : {
         "effect" : "                ▼ ",
                     Append
                     Deny
                     DeployIfNotExists
         "details" : {
          "type" : "Microsoft.GuestConfiguration/guestConfigurationAssignments",
          "roleDefinitionsIds" : [
           "/providers/microsoft.authorization/roleDefinitions/12345678-1234-5678-abcd-012345678910"
          ],
          "name" : "customExtension",
          "deployment" : {
               "properties" : {
           "mode": "incremental",
           "parameters" : {
            },
            "              ▼ ": [
              existenceCondition
              resources
              template
             }
          }
        }
     }
   }
 }
```

A. Mastered
B. Not Mastered

**Answer:** A

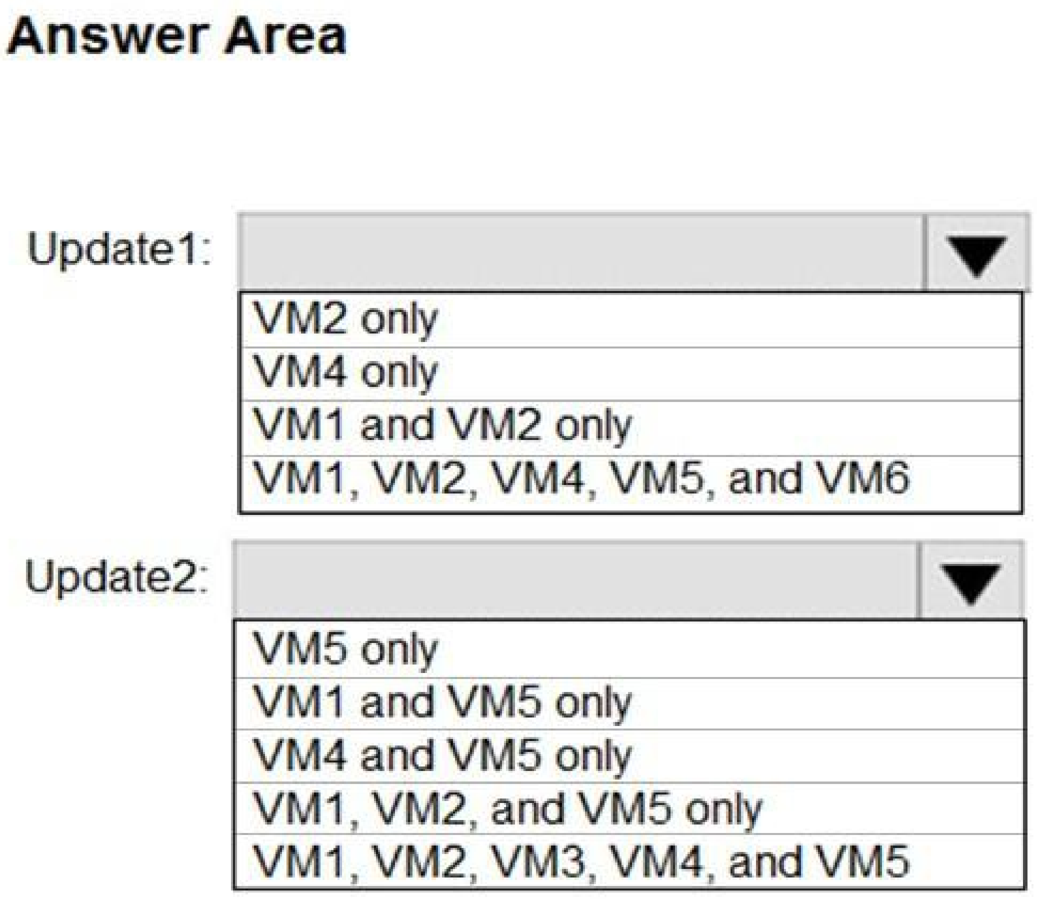
**Explanation:**
Box 1: DeployIfNotExists
DeployIfNotExists executes a template deployment when the condition is met.
Box 2: Template
The details property of the DeployIfNotExists effects has all the subproperties that define the related resources to match and the template deployment to execute.
Deployment [required]
This property should include the full template deployment as it would be passed to the Microsoft.Resources/deployment References:
https://docs.microsoft.com/en-us/azure/governance/policy/concepts/effects

**NEW QUESTION 9**
HOTSPOT
You have Azure virtual machines that have Update Management enabled. The virtual machines are configured as shown in the following table.



| Name | Operating system | Region | Resource group |
|---|---|---|---|
| VM1 | Windows Server 2012 | East US | RG1 |
| VM2 | Windows Server 2012 R2 | West US | RG1 |
| VM3 | Windows Server 2016 | West US | RG2 |
| VM4 | Ubuntu Server 18.04 LTS | West US | RG2 |
| VM5 | Red Hat Enterprise Linux 7.4 | East US | RG1 |
| VM6 | CentOS 7.5 | East US | RG1 |

You schedule two update deployments named Update1 and Update2. Update1 updates VM3. Update2 updates VM6.
Which additional virtual machines can be updated by using Update1 and Update2? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Hot Area:



Answer Area

Update1:

VM2 only
VM4 only
VM1 and VM2 only
VM1, VM2, VM4, VM5, and VM6

Update2:

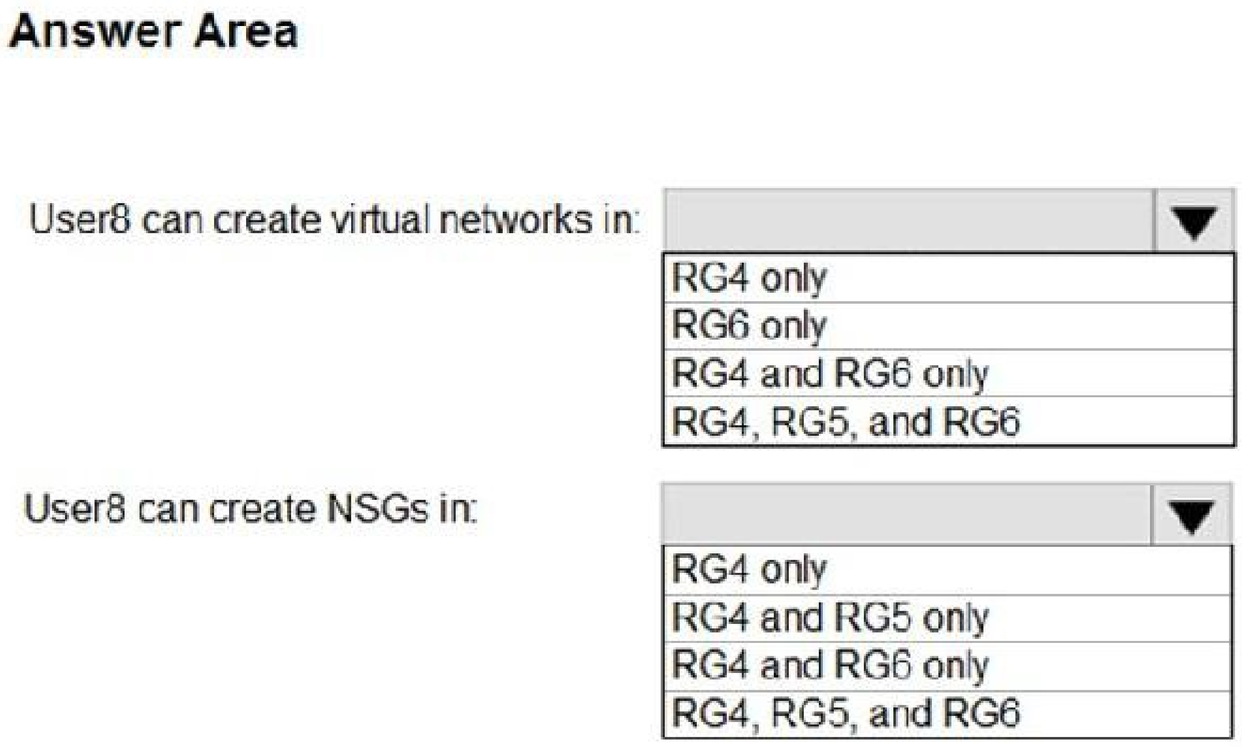
VM5 only
VM1 and VM5 only
VM4 and VM5 only
VM1, VM2, and VM5 only
VM1, VM2, VM3, VM4, and VM5

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**
Update1: VM1 and VM2 only
VM3: Windows Server 2016 West US RG2
Update2: VM4 and VM5 only VM6: CentOS 7.5 East US RG1
For Linux, the machine must have access to an update repository. The update repository can be private or public. References:
https://docs.microsoft.com/en-us/azure/automation/automation-update-management

**NEW QUESTION 10**
HOTSPOT
You assign User8 the Owner role for RG4, RG5, and RG6.
In which resource groups can User8 create virtual networks and NSGs? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Hot Area:



Answer Area

User8 can create virtual networks in:

RG4 only
RG6 only
RG4 and RG6 only
RG4, RG5, and RG6

User8 can create NSGs in:

RG4 only
RG4 and RG5 only
RG4 and RG6 only
RG4, RG5, and RG6

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**
Box 1: RG4 only
Virtual Networks are not allowed for Rg5 and Rg6.
Box 2: Rg4,Rg5, and Rg6 Scenario:
Contoso has two Azure subscriptions named Sub1 and Sub2.

Sub1 contains six resource groups named RG1, RG2, RG3, RG4, RG5, and RG6. You assign User8 the Owner role for RG4, RG5, and RG6
User8 city Sidney, Role:None
Note: A network security group (NSG) contains a list of security rules that allow or deny network traffic to resources connected to Azure Virtual Networks (VNet). NSGs can be associated to subnets, individual VMs (classic), or individual network interfaces (NIC) attached to VMs (Resource Manager).
References:
https://docs.microsoft.com/en-us/azure/governance/policy/overview

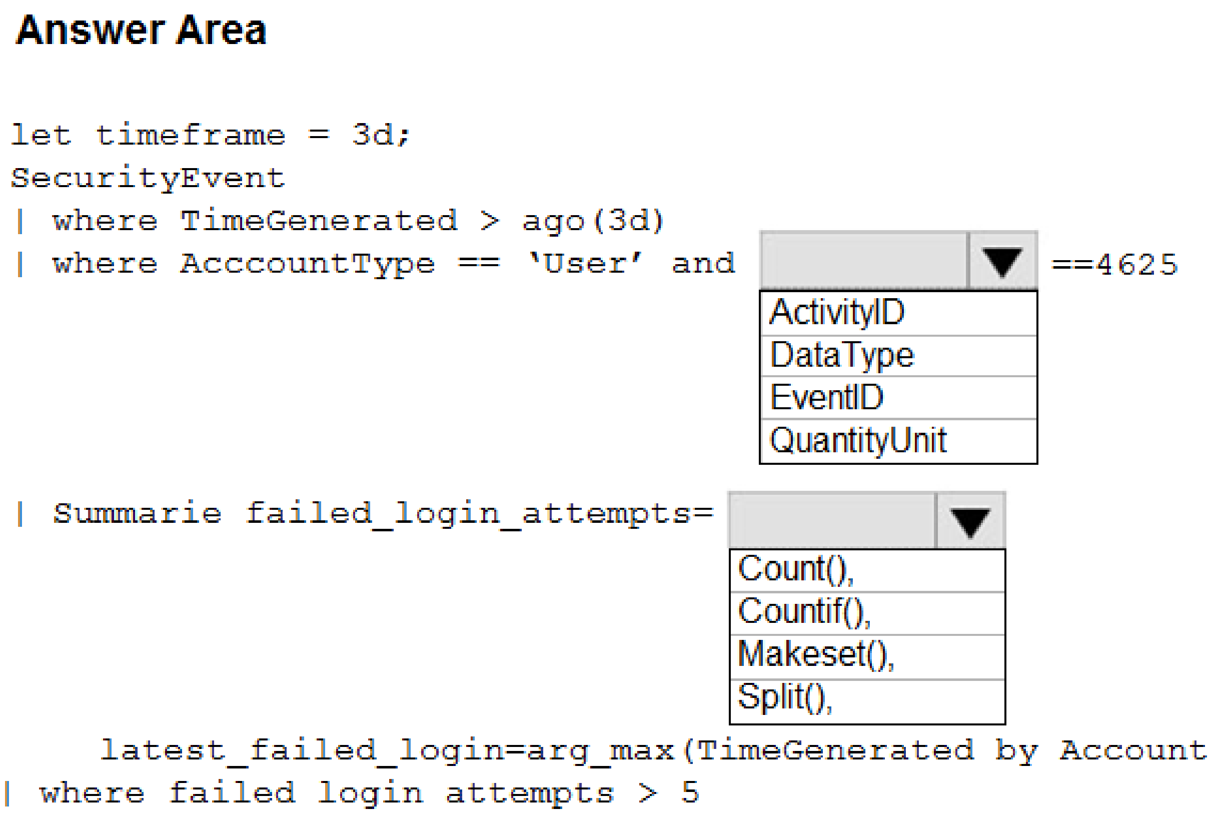
**NEW QUESTION 10**
You need to ensure that you can meet the security operations requirements.
What should you do first?

A. Turn on Auto Provisioning in Security Center.
B. Integrate Security Center and Microsoft Cloud App Security.
C. Upgrade the pricing tier of Security Center to Standard.
D. Modify the Security Center workspace configuration.

**Answer:** C

**Explanation:**
The Standard tier extends the capabilities of the Free tier to workloads running in private and other public clouds, providing unified security management and threat protection across your hybrid cloud workloads. The Standard tier also adds advanced threat detection capabilities, which uses built-in behavioral analytics and machine learning to identify attacks and zero-day exploits, access and application controls to reduce exposure to network attacks and malware, and more.
Scenario: Security Operations Requirements
Litware must be able to customize the operating system security configurations in Azure Security Center. References:
https://docs.microsoft.com/en-us/azure/security-center/security-center-pricing
Question Set 3

**NEW QUESTION 12**
HOTSPOT
You suspect that users are attempting to sign in to resources to which they have no access.
You need to create an Azure Log Analytics query to identify failed user sign-in attempts from the last three days. The results must only show users who had more than five failed sign-in attempts.
How should you configure the query? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Hot Area:



**Answer Area**

```
let timeframe = 3d;
SecurityEvent
| where TimeGenerated > ago(3d)
| where AcccountType == 'User' and [          ▼] ==4625

| Summarie failed_login_attempts= [          ▼]

    latest_failed_login=arg_max(TimeGenerated by Account
| where failed login attempts > 5
```

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**
The following example identifies user accounts that failed to log in more than five times in the last day, and when they last attempted to log in. let timeframe = 1d;
SecurityEvent
| where TimeGenerated > ago(1d)
| where AccountType == 'User' and EventID == 4625 // 4625 - failed log in
| summarize failed_login_attempts=count(), latest_failed_login=arg_max(TimeGenerated, Account) by Account
| where failed_login_attempts > 5
| project-away Account1
References:
https://docs.microsoft.com/en-us/azure/azure-monitor/log-query/examples

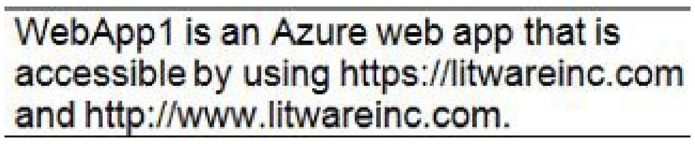
**NEW QUESTION 13**
You need to configure WebApp1 to meet the data and application requirements.
Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Upload a public certificate.
B. Turn on the HTTPS Only protocol setting.
C. Set the Minimum TLS Version protocol setting to 1.2.
D. Change the pricing tier of the App Service plan.
E. Turn on the Incoming client certificates protocol setting.

**Answer:** AC

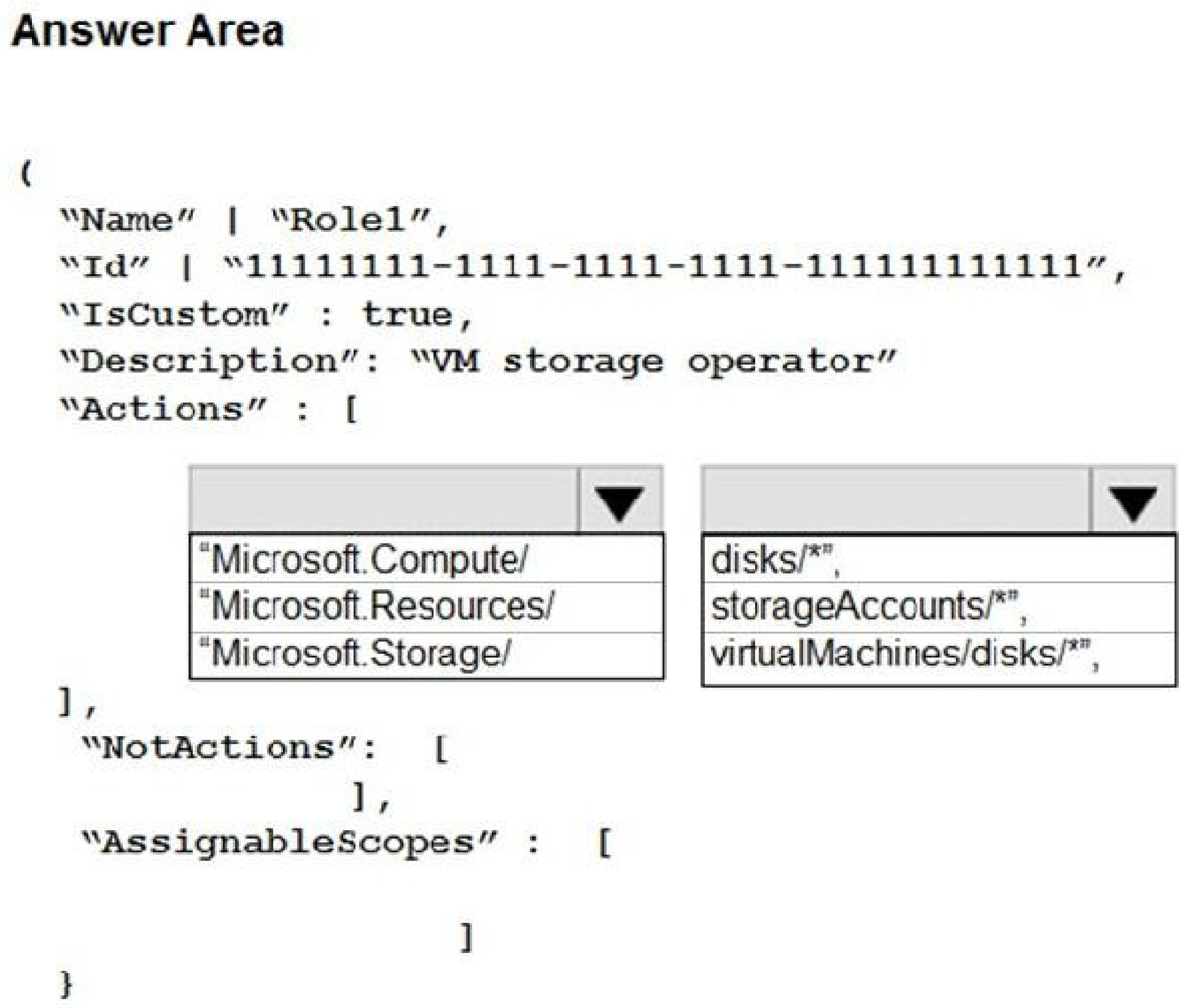
**Explanation:**
A: To configure Certificates for use in Azure Websites Applications you need to upload a public Certificate.
C: Over time, multiple versions of TLS have been released to mitigate different vulnerabilities. TLS 1.2 is the most current version available for apps running on Azure App Service.
Incorrect Answers:
B: We need support the http url as well.
Note:



WebApp1 is an Azure web app that is accessible by using https://litwareinc.com and http://www.litwareinc.com.

References:
https://docs.microsoft.com/en-us/azure/app-service/app-service-web-configure-tls-mutual-auth
https://azure.microsoft.com/en-us/updates/app-service-and-functions-hosted-apps-can-now-update-tls-versions/

**NEW QUESTION 16**
HOTSPOT
You need to create Role1 to meet the platform protection requirements.
How should you complete the role definition of Role1? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Hot Area:



Answer Area

```
(
  "Name" | "Role1",
  "Id" | "11111111-1111-1111-1111-111111111111",
  "IsCustom" : true,
  "Description": "VM storage operator"
  "Actions" : [
          [                    ▼] [                    ▼]
  ],
   "NotActions":  [
                ],
   "AssignableScopes" :  [

                    ]
  }
```

"Microsoft.Compute/
"Microsoft.Resources/
"Microsoft.Storage/

disks/*",
storageAccounts/*",
virtualMachines/disks/*",

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**
Scenario: A new custom RBAC role named Role1 must be used to delegate the administration of the managed disks in Resource Group1. Role1 must be available only for Resource Group1.
Azure RBAC template managed disks "Microsoft.Storage/" References:
https://blogs.msdn.microsoft.com/azureedu/2017/02/11/new-managed-disk-storage-option-for-your-azure-vms/

**NEW QUESTION 18**
From the Azure portal, you are configuring an Azure policy.
You plan to assign policies that use the DeployIfNotExist, AuditIfNotExist, Append, and Deny effects. Which effect requires a managed identity for the assignment?

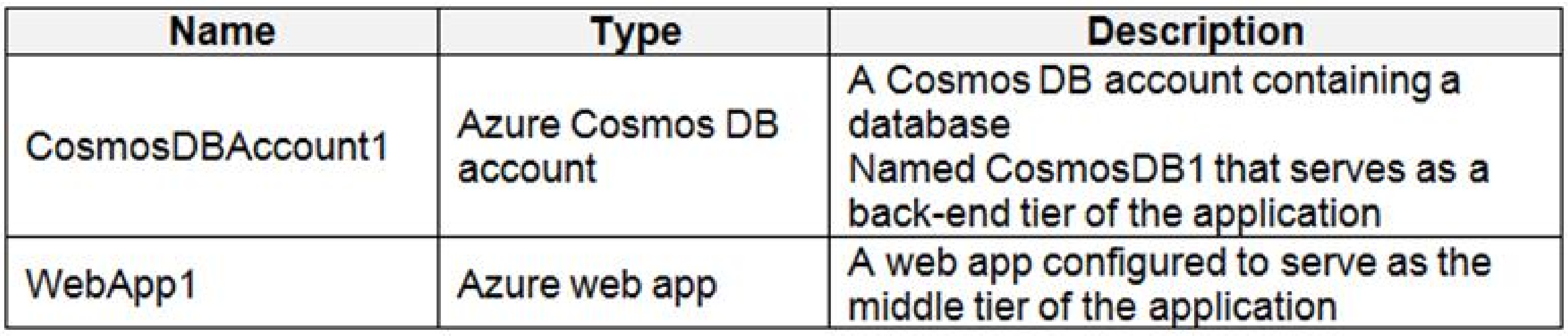
A. AuditIfNotExist

B. Append
C. DeployIfNotExist
D. Deny

**Answer:** C

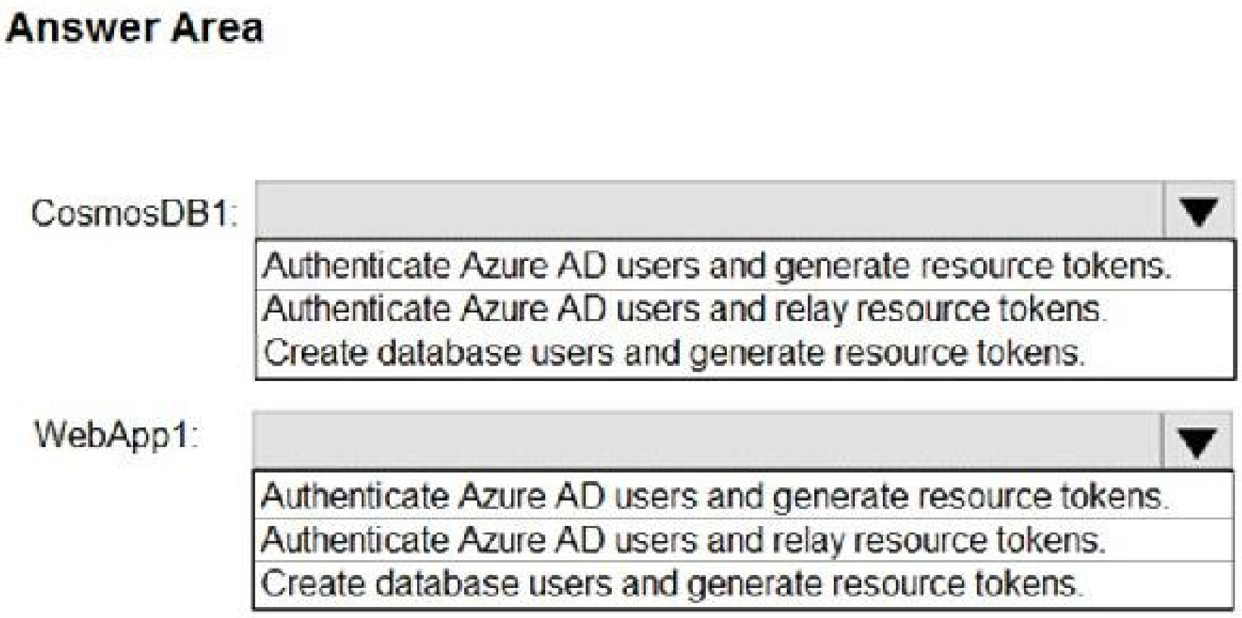
**Explanation:**
When Azure Policy runs the template in the deployIfNotExists policy definition, it does so using a managed identity.
References:
https://docs.microsoft.com/bs-latn-ba/azure/governance/policy/how-to/remediate-resources

**NEW QUESTION 20**
HOTSPOT
You have an Azure subscription named Sub1 that is associated to an Azure Active Directory (Azure AD) tenant named contoso.com. You plan to implement an application that will consist of the resources shown in the following table.



| Name | Type | Description |
|---|---|---|
| CosmosDBAccount1 | Azure Cosmos DB account | A Cosmos DB account containing a database Named CosmosDB1 that serves as a back-end tier of the application |
| WebApp1 | Azure web app | A web app configured to serve as the middle tier of the application |

Users will authenticate by using their Azure AD user account and access the Cosmos DB account by using resource tokens. You need to identify which tasks will be implemented in CosmosDB1 and WebApp1.
Which task should you identify for each resource? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Hot Area:



Answer Area

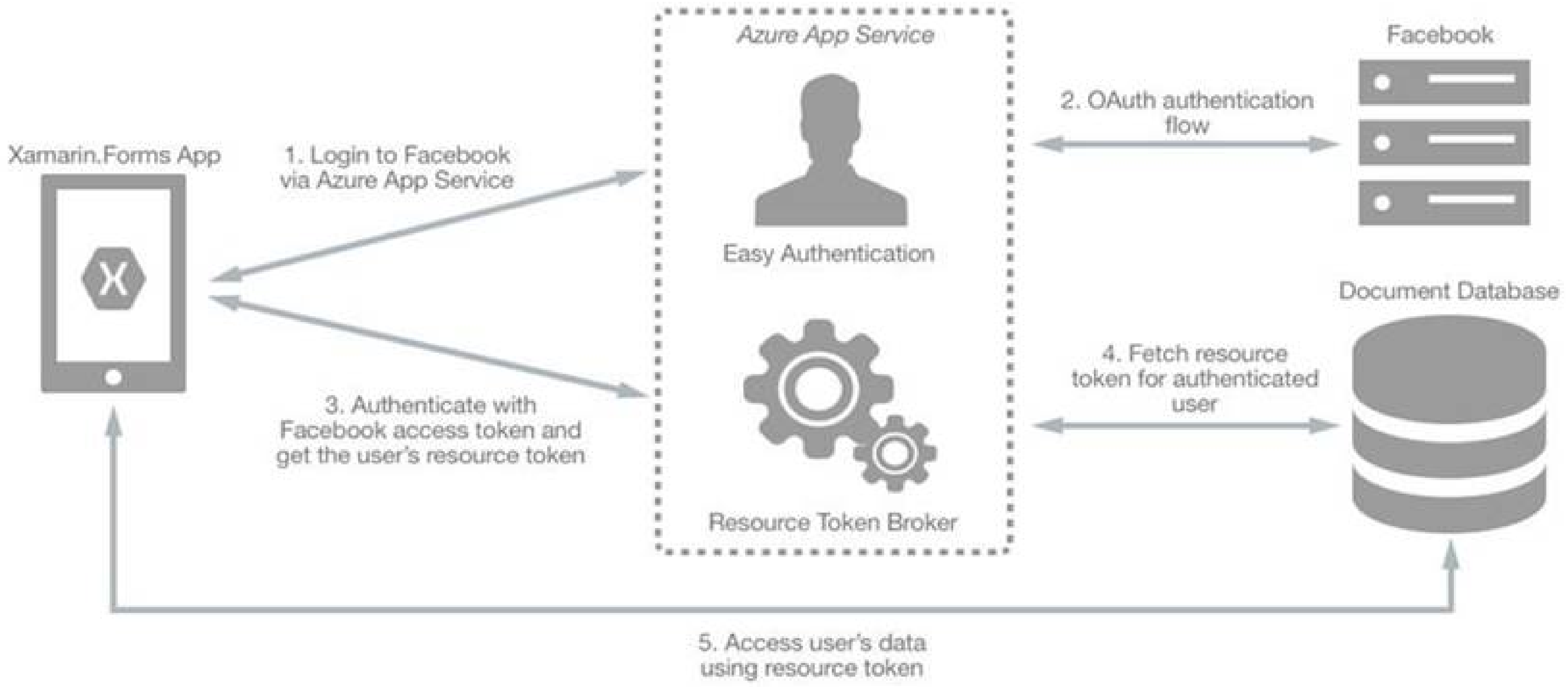
CosmosDB1:
- Authenticate Azure AD users and generate resource tokens.
- Authenticate Azure AD users and relay resource tokens.
- Create database users and generate resource tokens.

WebApp1:
- Authenticate Azure AD users and generate resource tokens.
- Authenticate Azure AD users and relay resource tokens.
- Create database users and generate resource tokens.

A. Mastered
B. Not Mastered

**Answer:** A

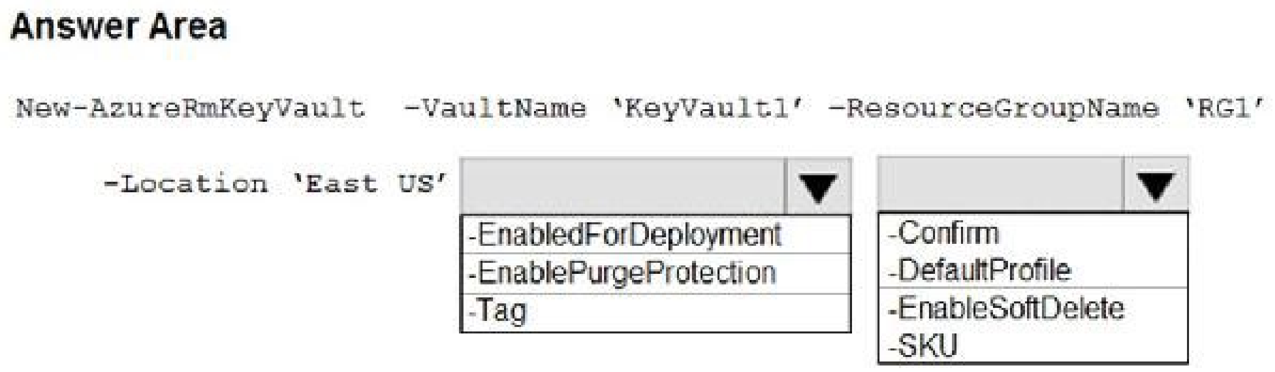
**Explanation:**
CosmosDB1: Create database users and generate resource tokens.
Azure Cosmos DB resource tokens provide a safe mechanism for allowing clients to read, write, and delete specific resources in an Azure Cosmos DB account according to the granted permissions.
WebApp1: Authenticate Azure AD users and relay resource tokens
A typical approach to requesting, generating, and delivering resource tokens to a mobile application is to use a resource token broker. The following diagram shows a high-level overview of how the sample application uses a resource token broker to manage access to the document database data:


Azure App Service
Facebook
2. OAuth authentication flow
Xamarin.Forms App
1. Login to Facebook via Azure App Service
Easy Authentication
Document Database
4. Fetch resource token for authenticated user
3. Authenticate with Facebook access token and get the user's resource token
Resource Token Broker
5. Access user's data using resource token

References:
https://docs.microsoft.com/en-us/xamarin/xamarin-forms/data-cloud/cosmosdb/authentication

**NEW QUESTION 23**

HOTSPOT
You need to create an Azure key vault. The solution must ensure that any object deleted from the key vault be retained for 90 days.
How should you complete the command? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Hot Area:



Answer Area

```
New-AzureRmKeyVault  -VaultName 'KeyVault1' -ResourceGroupName 'RG1'
    -Location 'East US'
```

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**
Box 1: -EnablePurgeProtection
If specified, protection against immediate deletion is enabled for this vault; requires soft delete to be enabled as well.
Box 2: -EnableSoftDelete
Specifies that the soft-delete functionality is enabled for this key vault. When soft-delete is enabled, for a grace period, you can recover this key vault and its contents after it is deleted.
References:
https://docs.microsoft.com/en-us/powershell/module/azurerm.keyvault/new-azurermkeyvault

**NEW QUESTION 24**

You have an Azure subscription that contains an Azure key vault named Vault1.
In Vault1, you create a secret named Secret1.
An application developer registers an application in Azure Active Directory (Azure AD). You need to ensure that the application can use Secret1.
What should you do?

A. In Azure AD, create a role.
B. In Azure Key Vault, create a key.
C. In Azure Key Vault, create an access policy.
D. In Azure AD, enable Azure AD Application Proxy.

**Answer:** A

**Explanation:**
Azure Key Vault provides a way to securely store credentials and other keys and secrets, but your code needs to authenticate to Key Vault to retrieve them.
Managed identities for Azure resources overview makes solving this problem simpler, by giving Azure services an automatically managed identity in Azure Active Directory (Azure AD). You can use this identity to authenticate to any service that supports Azure AD authentication, including Key Vault, without having any credentials in your code.
Example: How a system-assigned managed identity works with an Azure VM
After the VM has an identity, use the service principal information to grant the VM access to Azure resources. To call Azure Resource Manager, use role-based access control (RBAC) in Azure AD to assign the appropriate role to the VM service principal. To call Key Vault, grant your code access to the specific secret or

key in Key Vault.
References:
https://docs.microsoft.com/en-us/azure/key-vault/quick-create-net
https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/overview

**NEW QUESTION 28**
Your company uses Azure DevOps.
You need to recommend a method to validate whether the code meets the company’s quality standards and code review standards. What should you recommend implementing in Azure DevOps?

A. branch folders
B. branch permissions
C. branch policies
D. branch locking

**Answer:** C

**Explanation:**
Branch policies help teams protect their important branches of development. Policies enforce your team's code quality and change management standards.
References:
https://docs.microsoft.com/en-us/azure/devops/repos/git/branch-policies?view=azure-devops&viewFallbackFrom=vsts

**NEW QUESTION 30**
......