



CompTIA

# CertyIQ

## Premium exam material

Get certification quickly with the CertyIQ Premium exam material.

Everything you need to prepare, learn & pass your certification exam easily. Lifetime free updates

First attempt guaranteed success.

<https://www.CertyIQ.com>

# About CertyIQ

We here at CertyIQ eventually got enough of the industry's greedy exam paid for. Our team of IT professionals comes with years of experience in the IT industry Prior to training CertyIQ we worked in test areas where we observed the horrors of the paywall exam preparation system.

The misuse of the preparation system has left our team disillusioned. And for that reason, we decided it was time to make a difference. We had to make In this way, CertyIQ was created to provide quality materials without stealing from everyday people who are trying to make a living.

## Doubt Support

We have developed a very scalable solution using which we are able to solve 400+ doubts every single day with an average rating of 4.8 out of 5.

<https://www.certyiq.com>

[Mail us on - certyiqofficial@gmail.com](mailto:certyiqofficial@gmail.com)



### Lifetime Free Updates

We provide lifetime free updates to our customers. To make life easier for our valued customers and fulfill their needs



### Free Exam PDF

You are sure to pass the exam completely free of charge



### Money Back Guarantee

We Provide 100% money back guarantee to our customer in case of any failure

John

October 19, 2022



Thanks you so much for your help. I scored 972 in my exam today. More than 90% were from your PDFs!

Dana

September 04, 2022



Thanks a lot for this updated AZ-900 Q&A. I just passed my exam and got 974, I followed both of your Az-900 videos and the 6 PDF, the PDFs are very much valid, all answers are correct. Could you please create a similar video/PDF for DP900, your content/PDF's is really awesome. The team did a really good job. Thank You 😊.

Ahamed Shibly

2 months ago



Customer support is really fast and helpful, I just finished my exam and this video along with the 6 PDF helped me pass! Definitely recommend getting the PDFs. Thank you!

October 22, 2022



Passed my exam today with 891 marks. Out of 52 questions, 51 were from certyiq PDFs including Contoso case study. Thank You certyiq team!

Henry Rome

2 months ago



These questions are real and 100 % valid. Thank you so much for your efforts, also your 4 PDFs are awesome, I passed the DP900 exam on 1 Sept. With 968 marks. Thanks a lot, buddy!

Esmaria

2 months ago



Simple easy to understand explanations. To anyone out there wanting to write AZ900, I highly recommend 6 PDF's. Thank you so much, appreciate all your hard work in having such great content. Passed my exam Today - 3 September with 942 score.



# Microsoft

(AZ-500)

Microsoft Azure Security Technologies

Total: **504 Questions**

Link: <https://certyiq.com/papers/microsoft/az-500>

### Question: 1

Your company recently created an Azure subscription.

You have been tasked with making sure that a specified user is able to implement Azure AD Privileged Identity Management (PIM).

Which of the following is the role you should assign to the user?

- A. The Global administrator role.
- B. The Security administrator role.
- C. The Password administrator role.
- D. The Compliance administrator role.

**Answer: A**

#### Explanation:

To start using PIM in your directory, you must first enable PIM.

1. Sign in to the Azure portal as a Global Administrator of your directory.

You must be a Global Administrator with an organizational account (for example, @yourdomain.com), not a Microsoft account (for example, @outlook.com), to enable PIM for a directory.

Scenario: Technical requirements include: Enable Azure AD Privileged Identity Management (PIM) for contoso.com

Reference:

<https://docs.microsoft.com/bs-latn-ba/azure/active-directory/privileged-identity-management/pim-getting-started>

### Question: 2

Note: The question is included in a number of questions that depicts the identical set-up. However, every question has a distinctive result. Establish if the solution satisfies the requirements.

Your company has an Active Directory forest with a single domain, named weylandindustries.com. They also have an Azure Active Directory (Azure AD) tenant with the same name.

You have been tasked with integrating Active Directory and the Azure AD tenant. You intend to deploy Azure AD Connect.

Your strategy for the integration must make sure that password policies and user logon limitations affect user accounts that are synced to the Azure AD tenant, and that the amount of necessary servers are reduced.

Solution: You recommend the use of pass-through authentication and seamless SSO with password hash synchronization.

Does the solution meet the goal?

- A. Yes
- B. No

**Answer: A**

#### Explanation:

Yes" - the main sign-in method is PTA fulfills the requirements and the PH sync is just for failover and for Identity protection. It is also recommended to do.

Azure AD Identity Protection requires Password Hash Sync regardless of which sign-in method you choose, to provide the Users with leaked credentials report. Organizations can fail over to Password Hash Sync if their primary sign-in method fails and it was configured before the failure event.

<https://learn.microsoft.com/en-us/azure/active-directory/hybrid/choose-ad-authn>

### Question: 3

CertyIQ

Note: The question is included in a number of questions that depicts the identical set-up. However, every question has a distinctive result. Establish if the solution satisfies the requirements.

Your company has an Active Directory forest with a single domain, named weylandindustries.com. They also have an Azure Active Directory (Azure AD) tenant with the same name.

You have been tasked with integrating Active Directory and the Azure AD tenant. You intend to deploy Azure AD Connect.

Your strategy for the integration must make sure that password policies and user logon limitations affect user accounts that are synced to the Azure AD tenant, and that the amount of necessary servers are reduced.

Solution: You recommend the use of federation with Active Directory Federation Services (AD FS).

Does the solution meet the goal?

A. Yes

B. No

**Answer: B**

**Explanation:**

A federated authentication system relies on an external trusted system to authenticate users. Some companies want to reuse their existing federated system investment with their Azure AD hybrid identity solution. The maintenance and management of the federated system falls outside the control of Azure AD. It's up to the organization by using the federated system to make sure it's deployed securely and can handle the authentication load.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta>

### Question: 4

CertyIQ

Note: The question is included in a number of questions that depicts the identical set-up. However, every question has a distinctive result. Establish if the solution satisfies the requirements.

Your company has an Active Directory forest with a single domain, named weylandindustries.com. They also have an Azure Active Directory (Azure AD) tenant with the same name.

You have been tasked with integrating Active Directory and the Azure AD tenant. You intend to deploy Azure AD Connect.

Your strategy for the integration must make sure that password policies and user logon limitations affect user accounts that are synced to the Azure AD tenant, and that the amount of necessary servers are reduced.

Solution: You recommend the use of password hash synchronization and seamless SSO.

Does the solution meet the goal?

A. Yes

B. No

**Answer: B**

**Explanation:**

password hash synchronization cannot support the password policies and user logon limitations

For this you need to implement Pass-through authentication

### Question: 5

CertyIQ

Your company has an Active Directory forest with a single domain, named weylandindustries.com. They also have an Azure Active Directory (Azure AD) tenant with the same name.

After syncing all on-premises identities to Azure AD, you are informed that users with a givenName attribute starting with LAB should not be allowed to sync to Azure AD.

Which of the following actions should you take?

- A. You should make use of the Synchronization Rules Editor to create an attribute-based filtering rule.
- B. You should configure a DNAT rule on the Firewall.
- C. You should configure a network traffic filtering rule on the Firewall.
- D. You should make use of Active Directory Users and Computers to create an attribute-based filtering rule.

**Answer: A**

**Explanation:**

Use the Synchronization Rules Editor and write attribute-based filtering rule.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-change-the-configuration>

## Question: 6

**CertyIQ**

You have been tasked with applying conditional access policies for your company's current Azure Active Directory (Azure AD).

The process involves assessing the risk events and risk levels.

Which of the following is the risk level that should be configured for users that have leaked credentials?

- A. None
- B. Low
- C. Medium
- D. High

**Answer: D**

**Explanation:**

These six types of events are categorized in to 3 levels of risks " High, Medium & Low:

Sign-in Activity	Risk Level
Users with leaked credentials	High
Sign-ins from anonymous IP addresses	Medium
Impossible travel to atypical locations	Medium
Sign-ins from infected devices	Medium
Sign-ins from IP addresses with suspicious activity	Low
Sign-ins from unfamiliar locations	Medium

Reference:

<http://www.rebeladmin.com/2018/09/step-step-guide-configure-risk-based-azure-conditional-access-policies/>

### Question: 7

CertyIQ

You have been tasked with applying conditional access policies for your company's current Azure Active Directory (Azure AD).

The process involves assessing the risk events and risk levels.

Which of the following is the risk level that should be configured for sign ins that originate from IP addresses with dubious activity?

- A. None
- B. Low
- C. Medium
- D. High

**Answer: C**

**Explanation:**

Reference:

<http://www.rebeladmin.com/2018/09/step-step-guide-configure-risk-based-azure-conditional-access-policies/>

### Question: 8

CertyIQ

You have been tasked with configuring an access review, which you plan to assigned to a new collection of reviews. You also have to make sure that the reviews can be reviewed by resource owners.

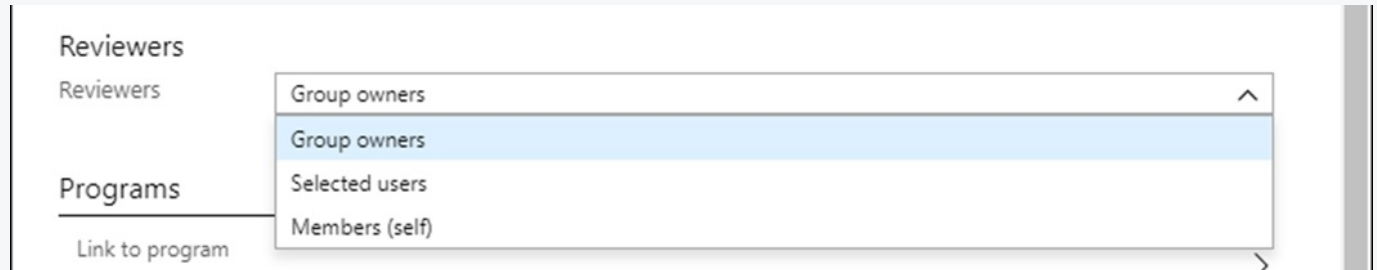
You start by creating an access review program and an access review control.  
You now need to configure the Reviewers.  
Which of the following should you set Reviewers to?

- A. Selected users.
- B. Members (Self).
- C. Group Owners.
- D. Anyone.

**Answer: C**

**Explanation:**

In the Reviewers section, select either one or more people to review all the users in scope. Or you can select to have the members review their own access. If the resource is a group, you can ask the group owners to review.



Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/governance/create-access-review> <https://docs.microsoft.com/en-us/azure/active-directory/governance/manage-programs-controls>

**Question: 9**

**CertyIQ**

Your company recently created an Azure subscription. You have, subsequently, been tasked with making sure that you are able to secure Azure AD roles by making use of Azure Active Directory (Azure AD) Privileged Identity Management (PIM).

Which of the following actions should you take FIRST?

- A. You should sign up Azure Active Directory (Azure AD) Privileged Identity Management (PIM) for Azure AD roles.
- B. You should consent to Azure Active Directory (Azure AD) Privileged Identity Management (PIM).
- C. You should discover privileged roles.
- D. You should discover resources.

**Answer: C**

**Explanation:**

C. You should discover privileged roles.

Before enabling and configuring Azure AD Privileged Identity Management (PIM), it's essential to discover and identify the privileged roles within your Azure environment. Understanding the roles and their permissions is a crucial initial step in implementing proper security measures and access controls. Once you have discovered these roles, you can proceed to configure and manage them using Azure AD PIM.

**Question: 10**

**CertyIQ**

You need to consider the underlined segment to establish whether it is accurate.

You have been tasked with creating a different subscription for each of your company's divisions. However, the subscriptions will be linked to a single Azure Active Directory (Azure AD) tenant. You want to make sure that each subscription has identical role assignments. You make use of Azure AD Privileged Identity Management (PIM). Select 'No adjustment required' if the underlined segment is accurate. If the underlined segment is inaccurate, select the accurate option.

- A. No adjustment required
- B. Azure Blueprints
- C. Conditional access policies
- D. Azure DevOps

**Answer: B**

**Explanation:**

To ensure that each subscription has identical role assignments, you should make use of Azure Blueprints. Azure Blueprints provide a declarative way to orchestrate the deployment of various Azure resources, including role assignments, policies, and resource configurations.

By creating an Azure Blueprint that defines the desired role assignments, you can apply the same blueprint to each subscription, ensuring consistent role assignments across all divisions.

### Question: 11

CertyIQ

Your company has an Azure Container Registry. You have been tasked with assigning a user a role that allows for the uploading of images to the Azure Container Registry. The role assigned should not require more privileges than necessary. Which of the following is the role you should assign?

- A. Owner
- B. Contributor
- C. AcrPush
- D. AcrPull

**Answer: C**

**Explanation:**

Reference:

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

### Question: 12

CertyIQ

Your company has an Azure Container Registry. You have been tasked with assigning a user a role that allows for the downloading of images from the Azure Container Registry. The role assigned should not require more privileges than necessary. Which of the following is the role you should assign?

- A. Reader
- B. Contributor
- C. AcrDelete
- D. AcrPull

**Answer: D**

**Explanation:**

The role assigned should not require more privileges than necessary."

Therefore, D (Acrpull) is CORRECT because it provides the least number of permissions required for downloading images from a Container Registry.

Answer A (Reader): provides at least two (2) permissions, which would be one (1) more than Acrpull allows for.

Reference:

<https://docs.microsoft.com/bs-latn-ba/azure/container-registry/container-registry-roles?tabs=azure-cli>

**Question: 13**

**CertyIQ**

Note: The question is included in a number of questions that depicts the identical set-up. However, every question has a distinctive result. Establish if the solution satisfies the requirements.

Your Company's Azure subscription includes a virtual network that has a single subnet configured.

You have created a service endpoint for the subnet, which includes an Azure virtual machine that has Ubuntu Server 18.04 installed.

You are preparing to deploy Docker containers to the virtual machine. You need to make sure that the containers can access Azure Storage resources and Azure SQL databases via the service endpoint.

You need to perform a task on the virtual machine prior to deploying containers.

Solution: You create an application security group.

Does the solution meet the goal?

A. Yes

B. No

**Answer: B**

**Explanation:**

You need to make sure that the containers can access Azure Storage resources and Azure SQL databases via the service endpoint". Since the containers are deployed inside a virtual machine the service endpoint will allow the virtual machine and anything hosted inside(applications/containers) to access Azure services directly. So since the creation of the service endpoint allows access to Azure Storage and Azure SQL databases there is no need to create an Application Security Group(ASG). B is the correct answer.

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-service-endpoints-overview>

**Question: 14**

**CertyIQ**

Note: The question is included in a number of questions that depicts the identical set-up. However, every question has a distinctive result. Establish if the solution satisfies the requirements.

Your Company's Azure subscription includes a virtual network that has a single subnet configured.

You have created a service endpoint for the subnet, which includes an Azure virtual machine that has Ubuntu Server 18.04 installed.

You are preparing to deploy Docker containers to the virtual machine. You need to make sure that the containers can access Azure Storage resources and Azure



SQL databases via the service endpoint.

You need to perform a task on the virtual machine prior to deploying containers.

Solution: You create an AKS Ingress controller.

Does the solution meet the goal?

A. Yes

B. No

**Answer: B**

**Explanation:**

Ingress Controller is used to establish a reverse proxy, so obviously answer is No

### Question: 15

CertyIQ

Note: The question is included in a number of questions that depicts the identical set-up. However, every question has a distinctive result. Establish if the solution satisfies the requirements.

Your Company's Azure subscription includes a virtual network that has a single subnet configured.

You have created a service endpoint for the subnet, which includes an Azure virtual machine that has Ubuntu Server 18.04 installed.

You are preparing to deploy Docker containers to the virtual machine. You need to make sure that the containers can access Azure Storage resources and Azure

SQL databases via the service endpoint.

You need to perform a task on the virtual machine prior to deploying containers.

Solution: You install the container network interface (CNI) plug-in.

Does the solution meet the goal?

A. Yes

B. No

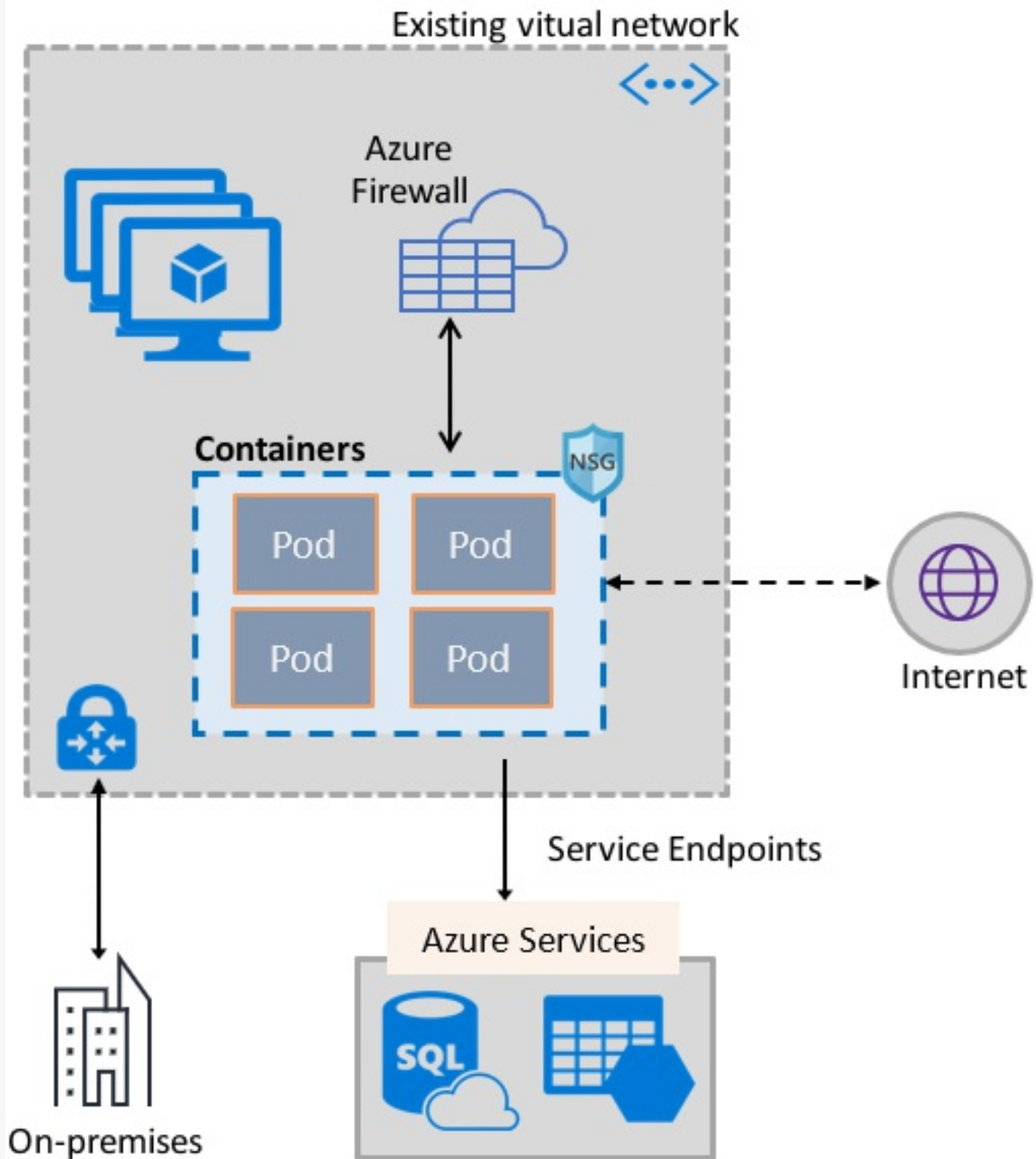
**Answer: A**

**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:



Reference:

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

### Question: 16

CertyIQ

You make use of Azure Resource Manager templates to deploy Azure virtual machines. You have been tasked with making sure that Windows features that are not in use, are automatically inactivated when instances of the virtual machines are provisioned. Which of the following actions should you take?

- A. You should make use of Azure DevOps.
- B. You should make use of Azure Automation State Configuration.
- C. You should make use of network security groups (NSG).

D. You should make use of Azure Blueprints.

**Answer: B**

**Explanation:**

You can use Azure Automation State Configuration to manage Azure VMs (both Classic and Resource Manager), on-premises VMs, Linux machines, AWS VMs, and on-premises physical machines.

Note: Azure Automation State Configuration provides a DSC pull server similar to the Windows Feature DSC-Service so that target nodes automatically receive configurations, conform to the desired state, and report back on their compliance. The built-in pull server in Azure Automation eliminates the need to set up and maintain your own pull server. Azure Automation can target virtual or physical Windows or Linux machines, in the cloud or on-premises.

Reference:

<https://docs.microsoft.com/en-us/azure/automation/automation-dsc-getting-started>

**Question: 17**

**CertyIQ**

Your company's Azure subscription includes Windows Server 2016 Azure virtual machines. You are informed that every virtual machine must have a custom antimalware virtual machine extension installed. You are writing the necessary code for a policy that will help you achieve this. Which of the following is an effect that must be included in your code?

- A. Disabled
- B. Modify
- C. AuditIfNotExists
- D. DeployIfNotExists

**Answer: D**

**Explanation:**

DeployIfNotExists executes a template deployment when the condition is met.

Reference:

<https://docs.microsoft.com/en-us/azure/governance/policy/concepts/effects>

**Question: 18**

**CertyIQ**

Your company makes use of Azure Active Directory (Azure AD) in a hybrid configuration. All users are making use of hybrid Azure AD joined Windows 10 computers.

You manage an Azure SQL database that allows for Azure AD authentication.

You need to make sure that database developers are able to connect to the SQL database via Microsoft SQL Server Management Studio (SSMS). You also need to make sure the developers use their on-premises Active Directory account for authentication. Your strategy should allow for authentication prompts to be kept to a minimum.

Which of the following is the authentication method the developers should use?

- A. Azure AD token.
- B. Azure Multi-Factor authentication.
- C. Active Directory integrated authentication.

**Answer: C**

**Explanation:**

Azure AD can be the initial Azure AD managed domain. Azure AD can also be an on-premises Active Directory Domain Services that is federated with the Azure AD.

Using an Azure AD identity to connect using SSMS or SSDT

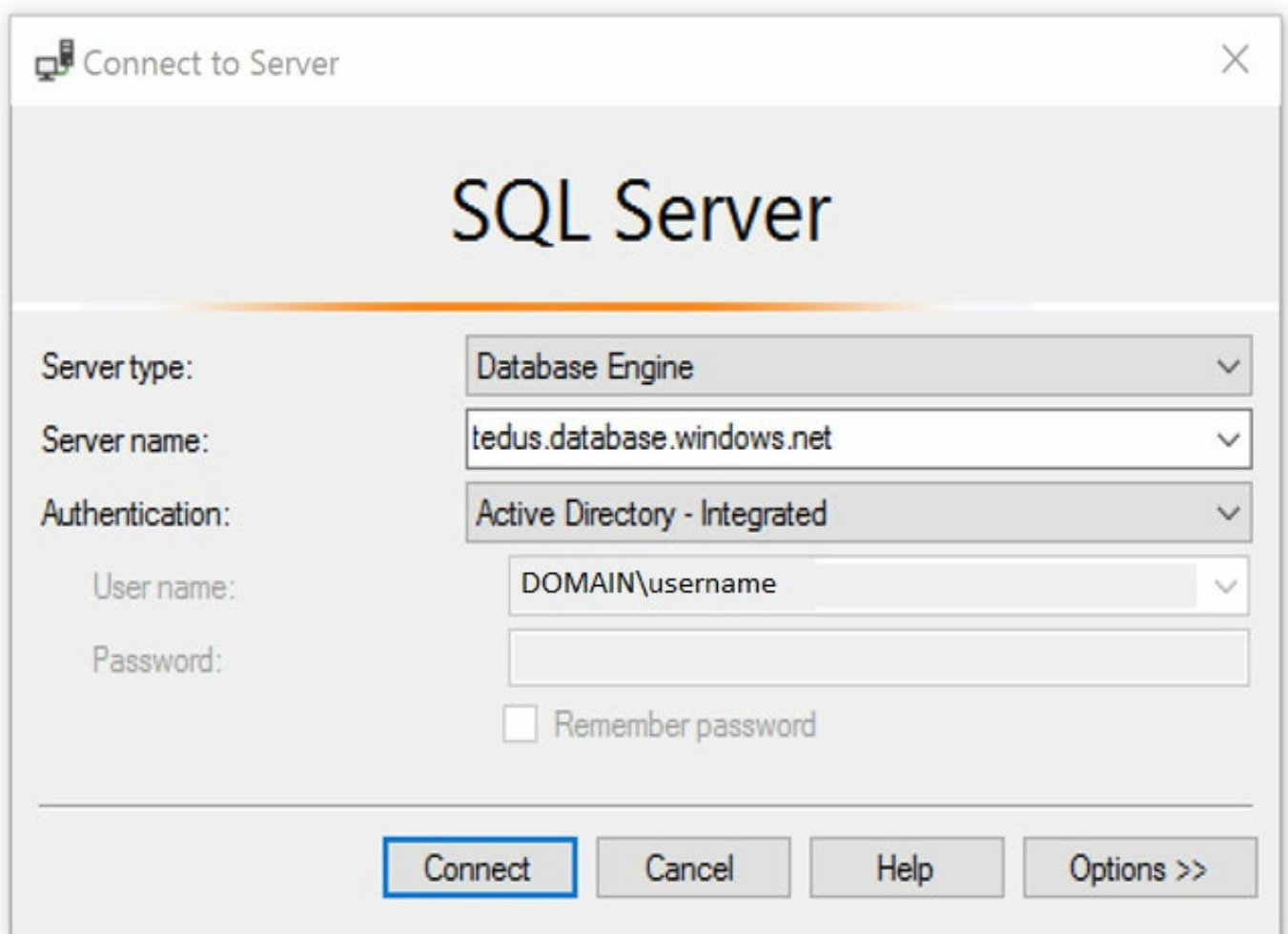
The following procedures show you how to connect to a SQL database with an Azure AD identity using SQL Server Management Studio or SQL Server Database Tools.

Active Directory integrated authentication

Use this method if you are logged in to Windows using your Azure Active Directory credentials from a federated domain.

1. Start Management Studio or Data Tools and in the Connect to Server (or Connect to Database Engine) dialog box, in the Authentication box, select Active

Directory - Integrated. No password is needed or can be entered because your existing credentials will be presented for the connection.



2. Select the Options button, and on the Connection Properties page, in the Connect to database box, type the name of the user database you want to connect to.

(The AD domain name or tenant ID option is only supported for Universal with MFA connection options, otherwise it is greyed out.)

**Question: 19**

**CertyIQ**

You have been tasked with enabling Advanced Threat Protection for an Azure SQL Database server.

Advanced Threat Protection must be configured to identify all types of threat detection.

Which of the following will happen if when a faulty SQL statement is generate in the database by an application?

- A. A Potential SQL injection alert is triggered.
- B. A Vulnerability to SQL injection alert is triggered.
- C. An Access from a potentially harmful application alert is triggered.
- D. A Brute force SQL credentials alert is triggered.

**Answer: B**

**Explanation:**

vulnerability to SQL Injection

(SQL.VM\_VulnerabilityToSqlInjection

SQL.DB\_VulnerabilityToSqlInjection

SQL.MI\_VulnerabilityToSqlInjection

SQL.DW\_VulnerabilityToSqlInjection)

An application has generated a faulty SQL statement in the database. This can indicate a possible vulnerability to SQL injection attacks. There are two possible reasons for a faulty statement. A defect in application code might have constructed the faulty SQL statement. Or, application code or stored procedures didn't sanitize user input when constructing the faulty SQL statement, which can be exploited for SQL injection. )

Reference:

<https://docs.microsoft.com/en-us/azure/sql-database/sql-database-threat-detection-overview>

**Question: 20**

**CertyIQ**

Note: The question is included in a number of questions that depicts the identical set-up. However, every question has a distinctive result. Establish if the solution satisfies the requirements.

You are in the process of creating an Azure Kubernetes Service (AKS) cluster. The Azure Kubernetes Service (AKS) cluster must be able to connect to an Azure Container Registry.

You want to make sure that Azure Kubernetes Service (AKS) cluster authenticates to the Azure Container Registry by making use of the auto-generated service principal.

Solution: You create an Azure Active Directory (Azure AD) role assignment.

Does the solution meet the goal?

- A. Yes
- B. No

**Answer: B**

**Explanation:**

1. i think its B as it wold need an RBAC role instead AAD role
2. B. NO Needs an RBAC role

**Question: 21**

**CertyIQ**

Your company has an Azure subscription that includes two virtual machines, named VirMac1 and VirMac2, which both have a status of Stopped (Deallocated).

The virtual machines belong to different resource groups, named ResGroup1 and ResGroup2.

You have also created two Azure policies that are both configured with the virtualMachines resource type. The

policy configured for ResGroup1 has a policy definition of Not allowed resource types, while the policy configured for ResGroup2 has a policy definition of Allowed resource types. You then create a Read-only resource lock on VirMac1, as well as a Read-only resource lock on ResGroup2. Which of the following is TRUE with regards to the scenario? (Choose all that apply.)

- A. You will be able to start VirMac1.
- B. You will NOT be able to start VirMac1.
- C. You will be able to create a virtual machine in ResGroup2.
- D. You will NOT be able to create a virtual machine in ResGroup2.

**Answer: BD**

**Explanation:**

When you will create a virtual machine in ResGroup2 it will give you error

"The selected resource group is read only"

## Question: 22

CertyIQ

You have been tasked with delegate administrative access to your company's Azure key vault. You have to make sure that a specific user can set advanced access policies for the key vault. You also have to make sure that access is assigned based on the principle of least privilege. Which of the following options should you use to achieve your goal?

- A. Azure Information Protection B. RBAC
- C. Azure AD Privileged Identity Management (PIM)
- D. Azure DevOps

**Answer:**

**Explanation:**

**Correction in Question as both Option A & B displayed in same row.**

You have been tasked with delegate administrative access to your company's Azure key vault.

You have to make sure that a specific user can set advanced access policies for the key vault. You also have to make sure that access is assigned based on the principle of least privilege.

Which of the following options should you use to achieve your goal?

A. Azure Information Protection

**B. RBAC**

C. Azure AD Privileged Identity Management (PIM)

D. Azure DevOps

-----  
**Correct Answer: B**

**Explanation:**

The answer is B, because PIM is where you can manage, control, and monitor the access.

The management plane uses RBAC - this is where you manage Key Vault itself which implies creating and deleting key vaults, retrieving Key Vault properties, and updating access policies.

<https://docs.microsoft.com/en-us/azure/key-vault/general/security-features#access-model-overview>

### Question: 23

CertyIQ

You have been tasked with delegate administrative access to your company's Azure key vault. You have to make sure that a specific user is able to add and delete certificates in the key vault. You also have to make sure that access is assigned based on the principle of least privilege. Which of the following options should you use to achieve your goal?

- A. A key vault access policy
- B. Azure policy
- C. Azure AD Privileged Identity Management (PIM)
- D. Azure DevOps

**Answer: A**

**Explanation:**

These operations are done on the key vault's data plane. The suitable built-in role would be a Key Vault Certificates Officer - able to perform any action on the certificates of a key vault, except manage permissions.

Reference:

<https://docs.microsoft.com/en-us/azure/key-vault/key-vault-secure-your-key-vault>

### Question: 24

CertyIQ

You have an Azure virtual machine that runs Windows Server R2. You plan to deploy and configure an Azure Key vault, and enable Azure Disk Encryption for the virtual machine. Which of the following is TRUE with regards to Azure Disk Encryption for a Windows VM?

- A. It is supported for basic tier VMs.
- B. It is supported for standard tier VMs.
- C. It is supported for VMs configured with software-based RAID systems.
- D. It is supported for VMs configured with Storage Spaces Direct (S2D).

**Answer: B**

**Explanation:**

Windows VMs are available in a range of sizes. Azure Disk Encryption is supported on Generation 1 and Generation 2 VMs. Azure Disk Encryption is also available for VMs with premium storage.

Azure Disk Encryption is not available on Basic, A-series VMs, or on virtual machines with a less than 2 GB of memory. For more exceptions, see Azure Disk Encryption: Unsupported scenarios.

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-machines/windows/disk-encryption-windows>

**Question: 25****CertyIQ**

You have an Azure virtual machine that runs Ubuntu 16.04-DAILY-LTS.  
You plan to deploy and configure an Azure Key vault, and enable Azure Disk Encryption for the virtual machine.  
Which of the following is TRUE with regards to Azure Disk Encryption for a Linux VM?

- A. It is NOT supported for basic tier VMs.
- B. It is NOT supported for standard tier VMs.
- C. OS drive encryption for Linux virtual machine scale sets is supported.
- D. Custom image encryption is supported.

**Answer: A****Explanation:**

"Azure Disk Encryption does not work for the following Linux scenarios, features, and technology:

Encrypting basic tier VM or VMs created through the classic VM creation method."

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-machines/linux/disk-encryption-linux>

**Question: 26****CertyIQ**

You need to consider the underlined segment to establish whether it is accurate.  
You have configured an Azure Kubernetes Service (AKS) cluster in your testing environment.  
You are currently preparing to deploy the cluster to the production environment.  
After disabling HTTP application routing, you want to replace it with an application routing solution that allows for reverse proxy and TLS termination for AKS services via a solitary IP address.  
You must create an AKS Ingress controller.  
Select 'No adjustment required' if the underlined segment is accurate. If the underlined segment is inaccurate, select the accurate option.

- A. No adjustment required.
- B. a network security group
- C. an application security group
- D. an Azure Basic Load Balancer

**Answer: A****Explanation:**

An ingress controller is a piece of software that provides reverse proxy, configurable traffic routing, and TLS termination for Kubernetes services.

Reference:

<https://docs.microsoft.com/en-us/azure/aks/ingress-tls>

**Question: 27****CertyIQ**

You want to gather logs from a large number of Windows Server 2016 computers using Azure Log Analytics.  
You are configuring an Azure Resource Manager template to deploy the Microsoft Monitoring Agent to all the servers automatically.



Which of the following should be included in the template? (Choose all that apply.)

- A. WorkspaceID
- B. AzureADApplicationID
- C. WorkspaceKey
- D. StorageAccountKey

**Answer: AC**

**Explanation:**

Reference:

<https://blogs.technet.microsoft.com/manageabilityguys/2015/11/19/enabling-the-microsoft-monitoring-agent-in-windows-json-templates/>

### Question: 28

**CertyIQ**

Note: The question is included in a number of questions that depicts the identical set-up. However, every question has a distinctive result. Establish if the solution satisfies the requirements.

Your company has Azure subscription linked to their Azure Active Directory (Azure AD) tenant.

As a Global administrator for the tenant, part of your responsibilities involves managing Azure Security Center settings.

You are currently preparing to create a custom sensitivity label.

Solution: You start by altering the pricing tier of the Security Center.

Does the solution meet the goal?

- A. Yes
- B. No

**Answer: B**

**Explanation:**

No - First you have to create a custom sensitive information type.

### Question: 29

**CertyIQ**

Note: The question is included in a number of questions that depicts the identical set-up. However, every question has a distinctive result. Establish if the solution satisfies the requirements.

Your company has Azure subscription linked to their Azure Active Directory (Azure AD) tenant.

As a Global administrator for the tenant, part of your responsibilities involves managing Azure Security Center settings.

You are currently preparing to create a custom sensitivity label.

Solution: You start by integrating Security Center and Microsoft Cloud App Security.

Does the solution meet the goal?

- A. Yes
- B. No

**Answer: B**

**Explanation:**

Must create Custom Information type first for description of the sensitive Label

### Question: 30

CertyIQ

Note: The question is included in a number of questions that depicts the identical set-up. However, every question has a distinctive result. Establish if the solution satisfies the requirements.

Your company has Azure subscription linked to their Azure Active Directory (Azure AD) tenant.

As a Global administrator for the tenant, part of your responsibilities involves managing Azure Security Center settings.

You are currently preparing to create a custom sensitivity label.

Solution: You start by creating a custom sensitive information type.

Does the solution meet the goal?

- A. Yes
- B. No

**Answer: A**

**Explanation:**

create Custom Information type first for description of the sensitive Label.

Reference:

<https://docs.microsoft.com/en-us/office365/securitycompliance/customize-a-built-in-sensitive-information-type>

### Question: 31

CertyIQ

You have a sneaking suspicion that there are users trying to sign in to resources which are inaccessible to them. You decide to create an Azure Log Analytics query to confirm your suspicions. The query will detect unsuccessful user sign-in attempts from the last few days.

You want to make sure that the results only show users who had failed to sign-in more than five times.

Which of the following should be included in your query?

- A. The EventID and CountIf() parameters.
- B. The ActivityID and CountIf() parameters.
- C. The EventID and Count() parameters.
- D. The ActivityID and Count() parameters.

**Answer: C**

**Explanation:**

KUSTO Query

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

Reference:

<https://docs.microsoft.com/en-us/azure/azure-monitor/log-query/examples>

### Question: 32

CertyIQ

Your company uses Azure DevOps with branch policies configured. Which of the following is TRUE with regards to branch policies? (Choose all that apply.)

- A. It enforces your team's change management standards.
- B. It controls who can read and update the code in a branch.
- C. It enforces your team's code quality.
- D. It places a branch into a read-only state.

**Answer: AC**

#### Explanation:

Branch policies help teams protect their important branches of development. Policies enforce your team's code quality and change management standards.

Reference:

<https://docs.microsoft.com/en-us/azure/devops/repos/git/branch-policies?view=azure-devops&viewFallbackFrom=vsts>

### Question: 33

CertyIQ

After creating a new Azure subscription, you are tasked with making sure that custom alert rules can be created in Azure Security Center.

You have created an Azure Storage account.

Which of the following is the action you should take?

- A. You should make sure that Azure Active Directory (Azure AD) Identity Protection is removed.
- B. You should create a DLP policy.
- C. You should create an Azure Log Analytics workspace.
- D. You should make sure that Security Center has the necessary tier configured.

**Answer: C**

#### Explanation:

C: You need write permission in the workspace that you select to store your custom alert.

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/security-center-custom-alert>

### Question: 34

CertyIQ

Your company's Azure subscription includes an Azure Log Analytics workspace.

Your company has a hundred on-premises servers that run either Windows Server 2012 R2 or Windows Server 2016, and is linked to the Azure Log Analytics workspace. The Azure Log Analytics workspace is set up to gather performance counters associated with security from these linked servers.

You have been tasked with configuring alerts according to the information gathered by the Azure Log Analytics workspace.

You have to make sure that alert rules allow for dimensions, and that alert creation time should be kept to a minimum. Furthermore, a single alert notification must be created when the alert is created and when the alert is sorted out.

You need to make use of the necessary signal type when creating the alert rules.

Which of the following is the option you should use?

- A. You should make use of the Activity log signal type.
- B. You should make use of the Application Log signal type.
- C. You should make use of the Metric signal type.
- D. You should make use of the Audit Log signal type.

**Answer: C**

**Explanation:**

Metric alerts in Azure Monitor provide a way to get notified when one of your metrics cross a threshold. Metric alerts work on a range of multi-dimensional platform metrics, custom metrics, Application Insights standard and custom metrics.

Note: Signals are emitted by the target resource and can be of several types. Metric, Activity log, Application Insights, and Log.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-monitor/platform/alerts-metric>

**Question: 35**

**CertyIQ**

Your company's Azure subscription includes a hundred virtual machines that have Azure Diagnostics enabled. You have been tasked with retrieving the identity of the user that removed a virtual machine fifteen days ago. You have already accessed Azure Monitor.

Which of the following options should you use?

- A. Application Log
- B. Metrics
- C. Activity Log
- D. Logs

**Answer: C**

**Explanation:**

Azure activity logs provide insight into the operations that were performed on resources in your subscription. Activity logs were previously known as audit logs or operational logs, because they report control-plane events for your subscriptions.

Reference:

<https://docs.microsoft.com/en-us/azure/security/azure-log-audit>

**Question: 36**

**CertyIQ**

Your company's Azure subscription includes a hundred virtual machines that have Azure Diagnostics enabled. You have been tasked with analyzing the security events of a Windows Server 2016 virtual machine. You have already accessed Azure Monitor.

Which of the following options should you use?

- A. Application Log
- B. Metrics
- C. Activity Log
- D. Logs

**Answer: D**

**Explanation:**

Log Integration collects Azure diagnostics from your Windows virtual machines, Azure activity logs, Azure Security Center alerts, and Azure resource provider logs. This integration provides a unified dashboard for all your assets, whether they're on-premises or in the cloud, so that you can aggregate, correlate, analyze, and alert for security events.

Reference:

<https://docs.microsoft.com/en-us/azure/security/azure-log-audit>

**Question: 37**

**CertyIQ**

You have been tasked with making sure that you are able to modify the operating system security configurations via Azure Security Center. To achieve your goal, you need to have the correct pricing tier for Azure Security Center in place. Which of the following is the pricing tier required?

- A. Advanced
- B. Premium
- C. Standard
- D. Free

**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 threat protection capabilities, which use 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. In addition, standard tier adds vulnerability scanning for your virtual machines.

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/security-center-pricing>

**Question: 38**

**CertyIQ**

Note: The question is included in a number of questions that depicts the identical set-up. However, every question has a distinctive result. Establish if the solution satisfies the requirements.

Your company's Azure subscription is linked to their Azure Active Directory (Azure AD) tenant.

After an internally developed application is registered in Azure AD, you are tasked with making sure that the application has the ability to access Azure Key Vault secrets on application the users' behalf.

Solution: You configure a delegated permission with admin consent.

Does the solution meet the goal?

A. Yes

B. No

**Answer: A**

**Explanation:**

Delegated permissions - Your client application needs to access the web API as the signed-in user, but with access limited by the selected permission. This type of permission can be granted by a user unless the permission requires administrator consent.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-configure-app-access-web-apis>

### Question: 39

CertyIQ

Note: The question is included in a number of questions that depicts the identical set-up. However, every question has a distinctive result. Establish if the solution satisfies the requirements.

Your company's Azure subscription is linked to their Azure Active Directory (Azure AD) tenant.

After an internally developed application is registered in Azure AD, you are tasked with making sure that the application has the ability to access Azure Key Vault secrets on application the users' behalf.

Solution: You configure a delegated permission with no admin consent.

Does the solution meet the goal?

A. Yes

B. No

**Answer: A**

**Explanation:**

Delegated permissions - Your client application needs to access the web API as the signed-in user, but with access limited by the selected permission. This type of permission can be granted by a user unless the permission requires administrator consent.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-configure-app-access-web-apis>

### Question: 40

CertyIQ

You need to consider the underlined segment to establish whether it is accurate.

Your Azure Active Directory Azure (Azure AD) tenant has an Azure subscription linked to it.

Your developer has created a mobile application that obtains Azure AD access tokens using the OAuth 2 implicit grant type.

The mobile application must be registered in Azure AD.

You require a redirect URI from the developer for registration purposes.

Select 'No adjustment required' if the underlined segment is accurate. If the underlined segment is inaccurate, select the accurate option.

A. No adjustment required

B. a secret

C. a login hint

D. a client ID

**Answer: D**

**Explanation:**

1. As per Microsoft's documentation, a Client ID is REQUIRED, while a Redirect URI is only RECOMMENDED  
<https://docs.microsoft.com/en-us/azure/active-directory/develop/v2-oauth2-implicit-grant-flow>
2. CLIENT ID

**Question: 41**

**CertyIQ**

You are in the process of configuring an Azure policy via the Azure portal.  
Your policy will include an effect that will need a managed identity for it to be assigned.  
Which of the following is the effect in question?

- A. AuditIfNotExist
- B. Disabled
- C. DeployIfNotExist
- D. EnforceOPAConstraint

**Answer: C**

**Explanation:**

When Azure Policy runs the template in the deployIfNotExists policy definition, it does so using a managed identity.

Reference:

<https://docs.microsoft.com/bs-latn-ba/azure/governance/policy/how-to/remediate-resources>

**Question: 42**

**CertyIQ**

You have been tasked with creating an Azure key vault using PowerShell. You have been informed that objects deleted from the key vault must be kept for a set period of 90 days.  
Which two of the following parameters must be used in conjunction to meet the requirement? (Choose two.)

- A. EnabledForDeployment
- B. EnablePurgeProtection
- C. EnabledForTemplateDeployment
- D. EnableSoftDelete

**Answer: BD**

**Explanation:**

- EnablePurgeProtection an EnableSoftDelete

Reference:

<https://docs.microsoft.com/en-us/powershell/module/azurerm.keyvault/new-azurermkeyvault>  
<https://docs.microsoft.com/en-us/azure/key-vault/key-vault-ovw-soft-delete>

**Question: 43**

**CertyIQ**

DRAG DROP -

Your company has an Azure SQL database that has Always Encrypted enabled.

You are required to make the relevant information available to application developers to allow them to access data in the database.

Which two of the following options should be made available? Answer by dragging the correct options from the list to the answer area.

Select and Place:

## Options

## Answer

The column encryption key

A DLP policy

A shared access signature (SAS)

A key vault access policy

The column master key

Answer:



# Options

# Answer

The column encryption key

A DLP policy

A shared access signature (SAS)

A key vault access policy

The column master key

The column encryption key

The column master key

## Explanation:

Always Encrypted uses two types of keys: column encryption keys and column master keys. A column encryption key is used to encrypt data in an encrypted column. A column master key is a key-protecting key that encrypts one or more column encryption keys.

## Reference:

<https://docs.microsoft.com/en-us/sql/relational-databases/security/encryption/always-encrypted-database-engine>

## Question: 44

CertyIQ

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

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

You have an Azure subscription 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: B**

**Explanation:**

Creating a new (additional) stored access policy will have no effect on the existing policy or the SAS's linked to it.

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.

Reference:

<https://docs.microsoft.com/en-us/rest/api/storageservices/Establishing-a-Stored-Access-Policy>

**Question: 45****CertyIQ**

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

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

You have a hybrid configuration of Azure Active Directory (Azure AD).

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.

Reference:

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

**Question: 46****CertyIQ**

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

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

You have a hybrid configuration of Azure Active Directory (Azure AD).

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 create a site-to-site VPN between the virtual network and the on-premises network.  
Does this meet the goal?

- A. Yes
- B. No

**Answer: B**

**Explanation:**

AI: Creating a site-to-site VPN between the virtual network and the on-premises network will establish a secure connection between the two networks, but it alone does not enable users to authenticate to the Azure HDInsight cluster using their on-premises Active Directory credentials.

To support the planned authentication, you need to use Azure AD Domain Services to synchronize on-premises Active Directory with Azure AD. This synchronization will allow users to authenticate to the Azure HDInsight cluster using their on-premises Active Directory credentials.

Therefore, the given solution alone does not meet the goal.

#### Question: 47

CertyIQ

Your network contains an Active Directory forest named contoso.com. The forest contains a single domain. You have an Azure subscription named Sub1 that is associated to an Azure Active Directory (Azure AD) tenant named contoso.com.

You plan to deploy Azure AD Connect and to integrate Active Directory and the Azure AD tenant.

You need to recommend an integration solution that meets the following requirements:

- Ensures that password policies and user logon restrictions apply to user accounts that are synced to the tenant
- Minimizes the number of servers required for the solution.

Which authentication method should you include in the recommendation?

- A. federated identity with Active Directory Federation Services (AD FS)
- B. password hash synchronization with seamless single sign-on (SSO)
- C. pass-through authentication with seamless single sign-on (SSO)

**Answer: C**

**Explanation:**

1. C. pass-through authentication with seamless single sign-on (SSO)
2. Companies with a security requirement to immediately enforce on-premises user account states, password policies, and sign-in hours might use this authentication method (PTA). <https://learn.microsoft.com/en-us/azure/active-directory/hybrid/choose-ad-authn>

#### Question: 48

CertyIQ

Your network contains an on-premises Active Directory domain named corp.contoso.com.

You have an Azure subscription named Sub1 that is associated to an Azure Active Directory (Azure AD) tenant named contoso.com.

You sync all on-premises identities to Azure AD.

You need to prevent users who have a givenName attribute that starts with TEST from being synced to Azure AD.

The solution must minimize administrative effort.

What should you use?

- A. Synchronization Rules Editor
- B. Web Service Configuration Tool

- C. the Azure AD Connect wizard
- D. Active Directory Users and Computers

**Answer: A**

**Explanation:**

Use the Synchronization Rules Editor and write attribute-based filtering rule.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-change-the-configuration>

**Question: 49**

**CertyIQ**

DRAG DROP -

You are implementing conditional access policies.

You must evaluate the existing Azure Active Directory (Azure AD) risk events and risk levels to configure and implement the policies.

You need to identify the risk level of the following risk events:

- Users with leaked credentials
- Impossible travel to atypical locations
- Sign-ins from IP addresses with suspicious activity

Which level should you identify for each risk event? To answer, drag the appropriate levels to the correct risk events. Each level may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:

**Levels**

**Answer Area**

High

Impossible travel to atypical locations:

Low

Users with leaked credentials:

Medium

Sign-ins from IP addresses with suspicious activity:

**Answer:**

**Levels**

**Answer Area**

High

Impossible travel to atypical locations:

Medium

Low

Users with leaked credentials:

High

Medium

Sign-ins from IP addresses with suspicious activity:

Medium

**Explanation:**

MEDIUM

high

medium

### Question: 50

CertyIQ

HOTSPOT -

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

Name	Member of	Mobile phone	Multi-factor authentication (MFA) status
User1	Group1	123 555 7890	Disabled
User2	Group1, Group2	None	Enabled
User3	Group1	123 555 7891	Required

You create and enforce an Azure AD Identity Protection user risk policy that has the following settings:

- Assignment: Include Group1, Exclude Group2
- Conditions: Sign-in risk of Medium and above
- Access: Allow access, Require password change

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

NOTE: Each correct selection is worth one point.

Hot Area:

## Answer Area

### Statements

Yes

No

If User1 signs in from an unfamiliar location, he must change his password.

☐☐

If User2 signs in from an anonymous IP address, she must change her password.

☐☐

If User3 signs in from a computer containing malware that is communicating with known bot servers, he must change his password.

☐☐

Answer:

## Answer Area

### Statements

Yes

No

If User1 signs in from an unfamiliar location, he must change his password.

☒☐

If User2 signs in from an anonymous IP address, she must change her password.

☐☒

If User3 signs in from a computer containing malware that is communicating with known bot servers, he must change his password.

☐☒

**Explanation:**

Box 1: Yes -

User1 is member of Group1. Sign in from unfamiliar location is risk level Medium.

Box 2 no

"When organizations both include and exclude a user or group the user or group is excluded from the policy, as an exclude action overrides an include in policy."

Box 3: No -

Sign-ins from IP addresses with suspicious activity is low.

**Question: 51**

**CertyIQ**

DRAG DROP -

You need to configure an access review. The review will be assigned to a new collection of reviews and reviewed by resource owners.

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**

**Answer Area**

Create an access review program.

Set Reviewers to Selected users.

Create an access review audit.

Create an access review control.

Set Reviewers to Group owners.

Set Reviewers to Members.



**Answer:**



## Actions

Create an access review program.

Set Reviewers to Selected users.

Create an access review audit.

Create an access review control.

Set Reviewers to Group owners.

Set Reviewers to Members.

## Answer Area

Create an access review program.

Create an access review control.

Set Reviewers to Group owners.



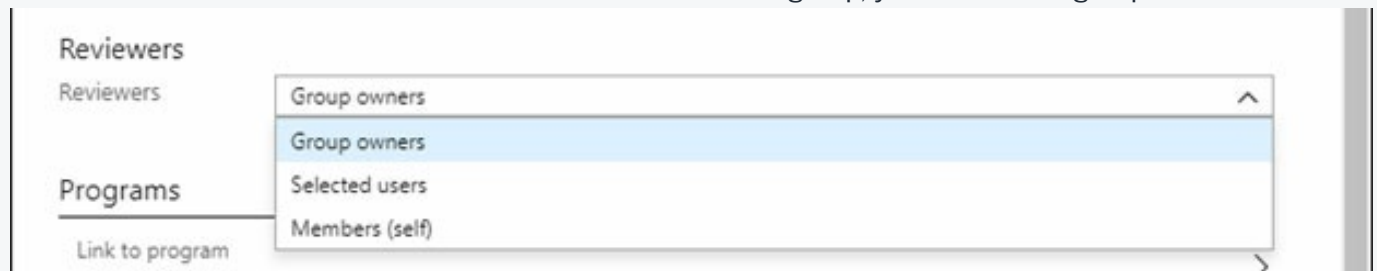
### Explanation:

Step 1: Create an access review program

Step 2: Create an access review control

Step 3: Set Reviewers to Group owners

In the Reviewers section, select either one or more people to review all the users in scope. Or you can select to have the members review their own access. If the resource is a group, you can ask the group owners to review.



### Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/governance/create-access-review> <https://docs.microsoft.com/en-us/azure/active-directory/governance/manage-programs-controls>

### Question: 52

CertyIQ

#### HOTSPOT -

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

Name	Role	Sign in frequency
User1	Password administrator	Signs in every work day
User2	Password administrator	Signs in bi-weekly
User3	Global administrator, Password administrator	Signs in every month

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

# Create an access review

Access reviews allow reviewers to attest to whether users still need to be in a role.

Review name \*

Review1

Description ⓘ

Start date \*

11/12/2020

Frequency

One time

Duration (in days) ⓘ

1

End ⓘ

Never

End by

Occurrences

Number of times

0

End date \*

12/12/2020

Users

Scope

Everyone

Review role membership (permanent and eligible) \*

Password Administrator

Reviewers

Reviewers

Members (self)

## ^ Upon completion settings

Auto apply results to resource ⓘ 

Enable

Disable

If reviewers don't respond ⓘ 

Take recommendations

## ∨ Advanced settings

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

NOTE: Each correct selection is worth one point.

Hot Area:



## Answer Area

User3 can perform Review1 for  
[answer choice].

▼
User3 only
User1 and User2 only
User1, User2, and User3

If User2 fails to complete Review1 by  
December 12, 2020, [answer choice].

▼
The Password administrator role will be revoked from User2
User2 will retain the Password administrator role
User3 will receive a confirmation request

### Answer:

#### Answer Area

User3 can perform Review1 for  
[answer choice].

▼
User3 only
User1 and User2 only
User1, User2, and User3

If User2 fails to complete Review1 by  
December 12, 2020, [answer choice].

▼
The Password administrator role will be revoked from User2
User2 will retain the Password administrator role
User3 will receive a confirmation request

### Explanation:

Box 1: User3 only -

Use the Members (self) option to have the users review their own role assignments.

Box 2: User3 will receive a confirmation request

Use the Should reviewer not respond list to specify what happens for users that are not reviewed by the reviewer within the review period. This setting does not impact users who have been reviewed by the reviewers manually. If the final reviewer's decision is Deny, then the user's access will be removed.

No change - Leave user's access unchanged

Remove access - Remove user's access

Approve access - Approve user's access

Take recommendations - Take the system's recommendation on denying or approving the user's continued access

Reference:

<https://docs.microsoft.com/bs-latn-ba/azure/active-directory/privileged-identity-management/pim-how-to-st art-security-review>

## Question: 53

CertyIQ

You have an Azure subscription named Sub1 that is associated to an Azure Active Directory (Azure AD) tenant named contoso.com.

An administrator named Admin1 has access to the following identities:

- An OpenID-enabled user account
- A Hotmail account
- An account in contoso.com
- An account in an Azure AD tenant named fabrikam.com

You plan to use Azure Account Center to transfer the ownership of Sub1 to Admin1.

To which accounts can you transfer the ownership of Sub1?

A. contoso.com only

- B. contoso.com, fabrikam.com, and Hotmail only
- C. contoso.com and fabrikam.com only
- D. contoso.com, fabrikam.com, Hotmail, and OpenID-enabled user account

Answer: C

Explanation:

When you transfer billing ownership of your subscription to an account in another Azure AD tenant, you can move the subscription to the new account's tenant. If you do so, all users, groups, or service principals who had role based access (RBAC) to manage subscriptions and its resources lose their access. Only the user in the new account who accepts your transfer request will have access to manage the resources.

Reference:

<https://docs.microsoft.com/en-us/azure/billing/billing-subscription-transfer> <https://docs.microsoft.com/en-us/azure/billing/billing-subscription-transfer#transferring-subscription-to-an-account-in-another-azure-ad-tenant>

Question: 54



HOTSPOT -  
Your company has two offices in Seattle and New York. Each office connects to the Internet by using a NAT device. The offices use the IP addresses shown in the following table.

Location	IP address space	Public NAT segment
Seattle	10.10.0.0/16	190.15.1.0/24
New York	172.16.0.0/16	194.25.2.0/24

The company has an Azure Active Directory (Azure AD) tenant named contoso.com. The tenant contains the users shown in the following table.

Name	Multi-factor authentication (MFA) status
User1	Enabled
User2	Enforced

The MFA service settings are configured as shown in the exhibit. (Click the Exhibit tab.)

## trusted ips [\(learn more\)](#)

☒ Skip multi-factor authentication for requests from federated users on my intranet

Skip multi-factor authentication for requests from following range of IP address subnets

10.10.0.0/16  
194.25.2.0/24

## verification options [\(learn more\)](#)

Methods available to users:

- ☒ Call to phone
- ☒ Text message to phone
- ☐ Notification through mobile app
- ☐ Verification code from mobile app or hardware token

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

NOTE: Each correct selection is worth one point.

Hot Area:

### Answer Area

	Yes	No
If User1 signs in to Azure from a device that uses an IP address of 134.18.14.10, User1 must be authenticated by using a phone.	<input type="radio"/>	<input type="radio"/>
If User2 signs in to Azure from a device in the Seattle office, User2 must be authenticated by using the Microsoft Authenticator app.	<input type="radio"/>	<input type="radio"/>
If User2 signs in to Azure from a device in the New York office, User2 must be authenticated by using a phone	<input type="radio"/>	<input type="radio"/>

Answer:

### Answer Area

	Yes	No
If User1 signs in to Azure from a device that uses an IP address of 134.18.14.10, User1 must be authenticated by using a phone.	<input checked="" type="radio"/>	<input type="radio"/>
If User2 signs in to Azure from a device in the Seattle office, User2 must be authenticated by using the Microsoft Authenticator app.	<input type="radio"/>	<input checked="" type="radio"/>
If User2 signs in to Azure from a device in the New York office, User2 must be authenticated by using a phone	<input type="radio"/>	<input checked="" type="radio"/>

**Explanation:**

Box 1: Yes -

Box 2: No -

Use of Microsoft Authenticator is not required. Either a text or phone call is required for MFA.

Note: Microsoft Authenticator is a multifactor app for mobile devices that generates time-based codes used during the Two-Step Verification process.

Box 3: No -

The New York IP address subnet is included in the "skip multi-factor authentication for request.

Reference:

<https://www.cayosoft.com/difference-enabling-enforcing-mfa/>

**Question: 55****CertyIQ**

Your company plans to create separate subscriptions for each department. Each subscription will be associated to the same Azure Active Directory (Azure AD) tenant.

You need to configure each subscription to have the same role assignments.

What should you use?

- A. Azure Security Center
- B. Azure Policy
- C. Azure AD Privileged Identity Management (PIM)
- D. Azure Blueprints

**Answer: D****Explanation:**

Just as a blueprint allows an engineer or an architect to sketch a project's design parameters, Azure Blueprints enables cloud architects and central information technology groups to define a repeatable set of Azure resources that implements and adheres to an organization's standards, patterns, and requirements. Blueprints are a declarative way to orchestrate the deployment of various resource templates and other artifacts such as:

- ⇒ Role Assignments
- ⇒ Policy Assignments
- ⇒ Azure Resource Manager templates
- ⇒ Resource Groups

Reference:

<https://docs.microsoft.com/en-us/azure/governance/blueprints/overview>

**Question: 56****CertyIQ**

HOTSPOT -

You have an Azure Container Registry named Registry1.

You add role assignments 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 and User4 only

User1, User2, and User4

User1, User2, User3, and User4

Answer:



## 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 and User4 only

User1, User2, and User4

User1, User2, User3, and User4

### 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		
AcrImagineSigner							X

Reference:

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

### Question: 57

CertyIQ

You have an Azure subscription.

You create an Azure web app named Contoso1812 that uses an S1 App Service plan.

You plan to -

create a CNAME DNS record for `www.contoso.com` that points to `Contoso1812`.

You need to ensure that users can access `Contoso1812` by using the `https://www.contoso.com` URL.

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

NOTE: Each correct selection is worth one point.

- A. Turn on the system-assigned managed identity for `Contoso1812`.
- B. Add a hostname to `Contoso1812`.
- C. Scale out the App Service plan of `Contoso1812`.
- D. Add a deployment slot to `Contoso1812`.
- E. Scale up the App Service plan of `Contoso1812`.
- F. Upload a PFX file to `Contoso1812`.

**Answer: BF**

**Explanation:**

B: You can configure Azure DNS to host a custom domain for your web apps. For example, you can create an Azure web app and have your users access it using either `www.contoso.com` or `contoso.com` as a fully qualified domain name (FQDN).

To do this, you have to create three records:

A root "A" record pointing to `contoso.com`

A root "TXT" record for verification

A "CNAME" record for the `www` name that points to the A record

F: To use HTTPS, you need to upload a PFX file to the Azure Web App. The PFX file will contain the SSL certificate required for HTTPS.

Reference:

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

## Question: 58

CertyIQ

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

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

You have an Azure subscription 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 lock on `sa1`.

Does this meet the goal?

- A. Yes
- B. No

**Answer: B**

**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 affects all of the shared access signatures

associated with it.

Reference:

<https://docs.microsoft.com/en-us/rest/api/storageservices/Establishing-a-Stored-Access-Policy>

### Question: 59

CertyIQ

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

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

You have a hybrid configuration of Azure Active Directory (Azure AD).

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 Azure Active Directory Domain Services (Azure AD DS) to the Azure subscription.

Does this meet the goal?

A. Yes

B. No

**Answer: A**

**Explanation:**

Azure Active Directory Domain Services

Azure AD DS provides a managed domain that's fully compatible with Windows Server Active Directory.

Microsoft takes care of managing, patching, and monitoring the domain in a highly available (HA) setup. You can deploy your cluster without worrying about maintaining domain controllers.

Users, groups, and passwords are synchronized from Azure AD. The one-way sync from your Azure AD instance to Azure AD DS enables users to sign in to the cluster by using the same corporate credentials.

### Question: 60

CertyIQ

Your network contains an Active Directory forest named contoso.com. You have an Azure Active Directory (Azure AD) tenant named contoso.com.

You plan to configure synchronization by using the Express Settings installation option in Azure AD Connect.

You need to identify which roles and groups are required to perform the planned configuration. The solution must use the principle of least privilege.

Which two roles and groups should you identify? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. the Domain Admins group in Active Directory

B. the Security administrator role in Azure AD

C. the Global administrator role in Azure AD

D. the User administrator role in Azure AD

E. the Enterprise Admins group in Active Directory

**Answer: CE**

**Explanation:**



C. the Global administrator role in Azure AD

E. the Enterprise Admins group in active directory

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/reference-connect-accounts-permissions>

### Question: 61

CertyIQ

DRAG DROP -

You create an Azure subscription with Azure AD Premium P2.

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

Discover privileged roles.

Sign up PIM for Azure AD roles.

Consent to PIM.

Discover resources.

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

#### Answer Area

Answer:

#### Actions

Discover privileged roles.

Sign up PIM for Azure AD roles.

Consent to PIM.

Discover resources.

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

#### Answer Area

Sign up PIM for Azure AD roles.

Discover privileged roles.

Consent to PIM.

Explanation:

Sign up PIM for Azure AD roles: This action involves enabling Azure AD PIM for your subscription and assigning users to the appropriate Azure AD roles that will have access to privileged operations.

Discover privileged roles: After signing up for Azure AD roles, you need to identify the roles in Azure AD that are considered privileged. This step involves identifying the roles that require additional security and oversight.

Consent to PIM: Once the privileged roles are discovered, you need to provide consent to enable PIM for these roles. This step ensures that PIM can manage and enforce the security controls for these roles.

### Question: 62

CertyIQ

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

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

You have a hybrid configuration of Azure Active Directory (Azure AD).

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 an Azure AD Application Proxy.

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.

Reference:

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

### Question: 63

CertyIQ

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

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

You have an Azure subscription 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 regenerate the Azure storage account access keys.

Does this meet the goal?

- A. Yes
- B. No

Answer: A

Explanation:

Generating new storage account keys will invalidate all SAS's that were based on the previous keys.

Question: 64

CertyIQ

HOTSPOT -

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

Name	Member of	Multi-factor authentication (MFA) status
User1	None	Disabled
User2	Group1	Disabled
User3	Group1	Enforced

Azure AD Privileged Identity Management (PIM) is used in contoso.com.

In PIM, the Password Administrator role has the following settings:

- Maximum activation duration (hours): 2
- Send email notifying admins of activation: Disable
- Require incident/request ticket number during activation: Disable
- Require Azure Multi-Factor Authentication for activation: Enable
- Require approval to activate this role: Enable
- Selected approver: Group1

You assign users the Password Administrator role as shown in the following table.

Name	Assignment type
User1	Active
User2	Eligible
User3	Eligible

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
When User1 signs in, the user is assigned the Password Administrator role automatically.	<input type="radio"/>	<input type="radio"/>
User2 can request to activate the Password Administrator role.	<input type="radio"/>	<input type="radio"/>
If User3 wants to activate the Password Administrator role, the user can approve their own request.	<input type="radio"/>	<input type="radio"/>

Answer:

## Answer Area

Statements	Yes	No
When User1 signs in, the user is assigned the Password Administrator role automatically.	<input checked="" type="radio"/>	<input type="radio"/>
User2 can request to activate the Password Administrator role.	<input checked="" type="radio"/>	<input type="radio"/>
If User3 wants to activate the Password Administrator role, the user can approve their own request.	<input type="radio"/>	<input checked="" type="radio"/>

### Explanation:

Box 1: Yes -

Active assignments don't require the member to perform any action to use the role. Members assigned as active have the privileges assigned to the role at all times.

Box 2: Yes -

While Multi-Factor Authentication is disabled for User2 and the setting Require Azure Multi-Factor Authentication for activation is enabled, User2 can request the role but will need to enable MFA to use the role.

Note: Eligible assignments require the member of the role to perform an action to use the role. Actions might include performing a multi-factor authentication (MFA) check, providing a business justification, or requesting approval from designated approvers.

Box 3: No -

User3 is Group1, which is a Selected Approver Group, however, self-approval is not allowed and someone else from group is required to approve the request.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-resource-roles-assign-roles>

## Question: 65

CertyIQ

You have a hybrid configuration of Azure Active Directory (Azure AD) that has Single Sign-On (SSO) enabled. You have an Azure SQL Database instance that is configured to support Azure AD authentication.

Database developers must connect to the database instance from the domain joined device and authenticate by using their on-premises Active Directory account.

You need to ensure that developers can connect to the instance by using Microsoft SQL Server Management Studio. The solution must minimize authentication prompts.

Which authentication method should you recommend?

- A. Active Directory - Password
- B. Active Directory - Universal with MFA support
- C. SQL Server Authentication
- D. Active Directory - Integrated

**Answer: D**

### Explanation:

Active Directory - Integrated -

Azure Active Directory Authentication is a mechanism of connecting to Microsoft Azure SQL Database by using identities in Azure Active Directory (Azure AD).

Use this method for connecting to SQL Database if you are logged in to Windows using your Azure Active Directory credentials from a federated domain.

Reference:

<https://docs.microsoft.com/en-us/sql/ssms/f1-help/connect-to-server-database-engine?view=sql-server-2017>  
<https://docs.microsoft.com/en-us/azure/sql-database/sql-database-aad-authentication-configure>

### Question: 66

CertyIQ

You plan to use Azure Resource Manager templates to perform multiple deployments of identically configured Azure virtual machines. The password for the administrator account of each deployment is stored as a secret in different Azure key vaults.

You need to identify a method to dynamically construct a resource ID that will designate the key vault containing the appropriate secret during each deployment.

The name of the key vault and the name of the secret will be provided as inline parameters.

What should you use to construct the resource ID?

- A. a key vault access policy
- B. a linked template
- C. a parameters file
- D. an automation account

**Answer: B**

**Explanation:**

You can't dynamically generate the resource ID in the parameters file because template expressions aren't allowed in the parameters file.

In your parent template, you add the nested template and pass in a parameter that contains the dynamically generated resource ID. The following image shows how a parameter in the linked template references the secret.

### Question: 67

CertyIQ

HOTSPOT -

You create a new Azure subscription that is associated to a new Azure Active Directory (Azure AD) tenant.

You create one active conditional access policy named Portal Policy. Portal Policy is used to provide access to the Microsoft Azure Management cloud app.

The Conditions settings for Portal Policy are configured as shown in the Conditions exhibit. (Click the Conditions tab.)

# Portal Policy

Conditional access policy

 Delete

Control user access based on conditional access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Name \*  

Portal Policy

Assignments

Users and groups ⓘ  
All users

Cloud apps or actions ⓘ  
1 app included

Conditions ⓘ  
1 condition selected

Access controls

Grant ⓘ  
1 control selected

Session ⓘ  
0 controls selected

Control user access based on signals from conditions like risk, device platform, location, client apps, or device state. [Learn more](#)

User risk ⓘ  
Not configured

Sign-in risk ⓘ  
Not configured

Device platforms ⓘ  
Not configured

Locations ⓘ  
1 included

Client apps ⓘ  
Not configured

Device state (Preview) ⓘ  
Not configured

Control user access based on their physical location. [Learn more](#)

Configure ⓘ  

Yes No

Include Exclude  

☐ Any location  
☐ All trusted locations  
☒ Selected locations

Select  
Contoso  
Contoso ...

The Grant settings for Portal Policy are configured as shown in the Grant exhibit. (Click the Grant tab.)



## Portal Policy

Conditional access policy



Delete

Control user access based on conditional access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Name \*

Portal Policy

### Assignments

Users and groups ⓘ

All users



Cloud apps or actions ⓘ

1 app included



Conditions ⓘ

1 condition selected



### Access controls

Grant ⓘ

1 control selected



Session ⓘ

0 controls selected



## Grant



Control user access enforcement to block or grant access. [Learn more](#)

☐ Block access

☒ Grant access

☒ Require multi-factor authentication ⓘ

☐ Require device to be marked as compliant ⓘ

☐ Require Hybrid Azure AD joined device ⓘ

☐ Require approved client app ⓘ  
[See list of approved client apps](#)

☐ Require app protection policy (preview) ⓘ  
[See list of policy protected client apps](#)

☐ Require password change (Preview) ⓘ

### For multiple controls

☒ Require all the selected controls

☐ Require one of the selected controls

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

NOTE: Each correct selection is worth one point.

Hot Area:

## Answer area

### Statements

Yes

No

Users from the Contoso named location must use multi-factor authentication (MFA) to access the Azure portal.

☐☐

Users from the Contoso named location must use multi-factor authentication (MFA) to access the web services hosted in the Azure subscription.

☐☐

Users external to the Contoso named location must use multi-factor authentication (MFA) to access the Azure portal.

☐☐

Answer:

## Answer area

### Statements

Yes

No

Users from the Contoso named location must use multi-factor authentication (MFA) to access the Azure portal.

☒☐

Users from the Contoso named location must use multi-factor authentication (MFA) to access the web services hosted in the Azure subscription.

☐☒

Users external to the Contoso named location must use multi-factor authentication (MFA) to access the Azure portal.

☐☒

### Explanation:

Box 1: Yes -

The Contoso location is included in the policy and MFA is required.

Box 2: No -

The policy applies to the Azure portal and Azure management endpoints. The policy does not apply to web services host in Azure.

Box 3: No -

The policy applies only to users in the Contoso location. The policy does not apply to users external to the Contoso location.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition>

## Question: 68

CertyIQ

HOTSPOT -

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

Name	Member of	Multi-factor authentication (MFA) status
User1	Group1, Group2	Disabled
User2	Group2	Disabled

The tenant contains the named locations shown in the following table.



Name	IP address range	Trusted location
Seattle	193.77.10.0/24	Yes
Boston	154.12.18.0/24	No

You create the conditional access policies for a cloud app named App1 as shown in the following table.

Name	Include	Exclude	Condition	Grant
Policy1	Group1	Group2	Locations: Boston	Block access
Policy2	Group1	None	Locations: Any location	Grant access, Require multi-factor authentication
Policy3	Group2	Group1	Locations: Boston	Block access
Policy4	User2	None	Locations: Any location	Grant access, Require multi-factor authentication

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

NOTE: Each correct selection is worth one point.

Hot Area:

### Answer Area

Statements	Yes	No
User1 can access App1 from an IP address of 154.12.18.10.	<input type="radio"/>	<input type="radio"/>
User2 can access App1 from an IP address of 193.77.10.15.	<input type="radio"/>	<input type="radio"/>
User2 can access App1 from an IP address of 154.12.18.34.	<input type="radio"/>	<input type="radio"/>

Answer:

### Answer Area

Statements	Yes	No
User1 can access App1 from an IP address of 154.12.18.10.	<input checked="" type="radio"/>	<input type="radio"/>
User2 can access App1 from an IP address of 193.77.10.15.	<input checked="" type="radio"/>	<input type="radio"/>
User2 can access App1 from an IP address of 154.12.18.34.	<input type="radio"/>	<input checked="" type="radio"/>

Explanation:

User1 can access - Remember, exclusions take precedence. Policy1 won't apply since group2 is excluded, policy2 allows, policy3 won't apply since group1 is excluded, policy4 won't apply.

User2 can access - there are no policies blocking the Seattle range

User2 cannot access - policy1 won't apply since group2 is excluded, policy2 allows, but policy3 blocks access for group2.

Question: 69

HOTSPOT -

You have an Azure subscription named Sub 1 that is associated to an Azure Active Directory (Azure AD) tenant named contoso.com. The tenant contains the users shown in the following table.

Name	Role
User1	Global administrator
User2	Security administrator
User3	Security reader
User4	License administrator

Each user is assigned an Azure AD Premium P2 license. You plan to onboard and configure Azure AD Identity Protection. Which users can onboard Azure AD Identity Protection, remediate users, and configure policies? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point. Hot Area:

Answer Area

Users who can onboard Azure AD Identity Protection:

User1 only

User1 and User2 only

User1,User2, and User3 only

User1,User2, User3, and User4 only

Users who can remediate users and configure policies:

User1 and User2 only

User1 and User3 only

User1, User2, and User3 only

User1, User2, User3, and User4

Answer:

Answer Area

Users who can onboard Azure AD Identity Protection:

User1 only

User1 and User2 only

User1,User2, and User3 only

User1,User2, User3, and User4 only

Users who can remediate users and configure policies:

User1 and User2 only

User1 and User3 only

User1, User2, and User3 only

User1, User2, User3, and User4

**Explanation:**

Global Administrator and Security Administrator have full access to Identity Protection. However only Global Administrator can onboard Identity Protection.

Security Administrator has full access so it can remediate and configure policies. It can't reset user password tho.

Security Reader can view all Identity Protection reports and Overview blade. It can't configure policies.

<https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/overview-identity-protection#permissions>

- Users who can onboard Azure AD Protection - User1 only
- Users who can remediate users and configure policies - User1 and User2 only

**Question: 70****CertyIQ**

HOTSPOT -

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

Name	Member of
User1	Group1
User2	Group2
User3	Group1, Group2

From Azure AD Privileged Identity Management (PIM), you configure the settings for the Security Administrator role as shown in the following exhibit.

**Assignment**☒ Allow permanent eligible assignment

Expire eligible assignments after

3 Months

☒ Allow permanent active assignment

Expire active assignments after

1 Month

☐ Require Azure Multi-Factor Authentication on active assignment☒ Require justification on active assignment**Activation**

Activation maximum duration (hours)



5

☐ Require Azure Multi-Factor Authentication on activation☐ Require justification on activation☐ Require ticket information on activation☐ Require approval to activate

Select approvers

*No member or group selected*

From PIM, you assign the Security Administrator role to the following groups:

- Group1: Active assignment type, permanently assigned
- Group2: Eligible assignment type, permanently eligible

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

NOTE: Each correct selection is worth one point.

Hot Area:

## Answer Area

Statements	Yes	No
User1 can only activate the Security Administrator role in five hours.	<input type="radio"/>	<input type="radio"/>
If User2 activates the Security Administrator role, the user will be assigned the role immediately.	<input type="radio"/>	<input type="radio"/>
User3 can activate the Security Administrator role.	<input type="radio"/>	<input type="radio"/>

Answer:

### Answer Area

Statements	Yes	No
User1 can only activate the Security Administrator role in five hours.	<input type="radio"/>	<input checked="" type="radio"/>
If User2 activates the Security Administrator role, the user will be assigned the role immediately.	<input checked="" type="radio"/>	<input type="radio"/>
User3 can activate the Security Administrator role.	<input type="radio"/>	<input checked="" type="radio"/>

#### Explanation:

Box 1: No -

User1 is a member of Group1. Group1: Active assignment type, permanently assigned

Box 2: Yes -

Active Type: A role assignment that doesn't require a user to perform any action to use the role. Users assigned as active have the privileges assigned to the role

Box 3: No -

User3 is member of Group1 and Group2.

Group1: Active assignment type, permanently assigned

Group2: Eligible assignment type, permanently eligible

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure> <https://docs.microsoft.com/bs-cyrl-ba/azure/active-directory/privileged-identity-management/pim-resource-roles-configure-role-settings>

## Question: 71

CertyIQ

HOTSPOT -

Your company has an Azure subscription named Subscription1 that contains the users shown in the following table.



Name	Role
User1	Global administrator
User2	Billing administrator
User3	Owner
User4	Account Admin

The company is sold to a new owner.

The company needs to transfer ownership of Subscription1.

Which user can transfer the ownership and which tool should the user use? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

## Answer Area

User:

▼

User1
User2
User3
User4

Tool:

▼

Azure Account Center
Azure Cloud Shell
Azure PowerShell
Azure Security Center

Answer:

## Answer Area

User:

	▼
User1	
User2	
User3	
User4	

Tool:

	▼
Azure Account Center	
Azure Cloud Shell	
Azure PowerShell	
Azure Security Center	

### Explanation:

Box 1; User2 -

Billing Administrator -

Select Transfer billing ownership for the subscription that you want to transfer.

Enter the email address of a user who's a billing administrator of the account that will be the new owner for the subscription.

Box 2: Azure Account Center -

Azure Account Center can be used.

Reference:

<https://docs.microsoft.com/en-us/azure/billing/billing-subscription-transfer#transfer-billing-ownership-of-an-azure-subscription>

### Question: 72

CertyIQ

SIMULATION -

The developers at your company plan to create a web app named App12345678 and to publish the app to <https://www.contoso.com>.

You need to perform the following tasks:

- Ensure that App12345678 is registered to Azure Active Directory (Azure AD).
- Generate a password for App12345678.

To complete this task, sign in to the Azure portal.

### Answer:

See the explanation below.

### Explanation:


Step 1: Register the Application

1. Sign in to your Azure Account through the Azure portal.

2. Select Azure Active Directory.
3. Select App registrations.
4. Select New registration.
5. Name the application 12345678. Select a supported account type, which determines who can use the application. Under Redirect URI, select Web for the type of application you want to create. Enter the URI: `https://www.contoso.com`, where the access token is sent to.

[Dashboard](#) > [Microsoft - App registrations](#) > Register an application

## Register an application

 If you are building an application for external users that will be distributed by Microsoft, you must register as a first party application to meet all security, privacy, and compliance policies. [Read our decision guide](#)

**\* Name**

The user-facing display name for this application (this can be changed later).

**Supported account types**

Who can use this application or access this API?

☒ Accounts in this organizational directory only (Microsoft)

☐ Accounts in any organizational directory

☐ Accounts in any organizational directory and personal Microsoft accounts (e.g. Skype, Xbox, Outlook.com)

[Help me choose...](#)

**Redirect URI (optional)**

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

[By proceeding, you agree to the Microsoft Platform Policies](#)

**Register**

6. Click Register

Step 2: Create a new application secret

If you choose not to use a certificate, you can create a new application secret.

7. Select Certificates & secrets.

8. Select Client secrets -> New client secret.

9. Provide a description of the secret, and a duration. When done, select Add.

After saving the client secret, the value of the client secret is displayed. Copy this value because you aren't able to retrieve the key later. You provide the key value with the application ID to sign in as the application. Store the key value where your application can retrieve it.

Reference:



### Question: 73

CertyIQ

#### SIMULATION -

You need to create a new Azure Active Directory (Azure AD) directory named 12345678.onmicrosoft.com and a user named User1 in the new directory.

To complete this task, sign in to the Azure portal.

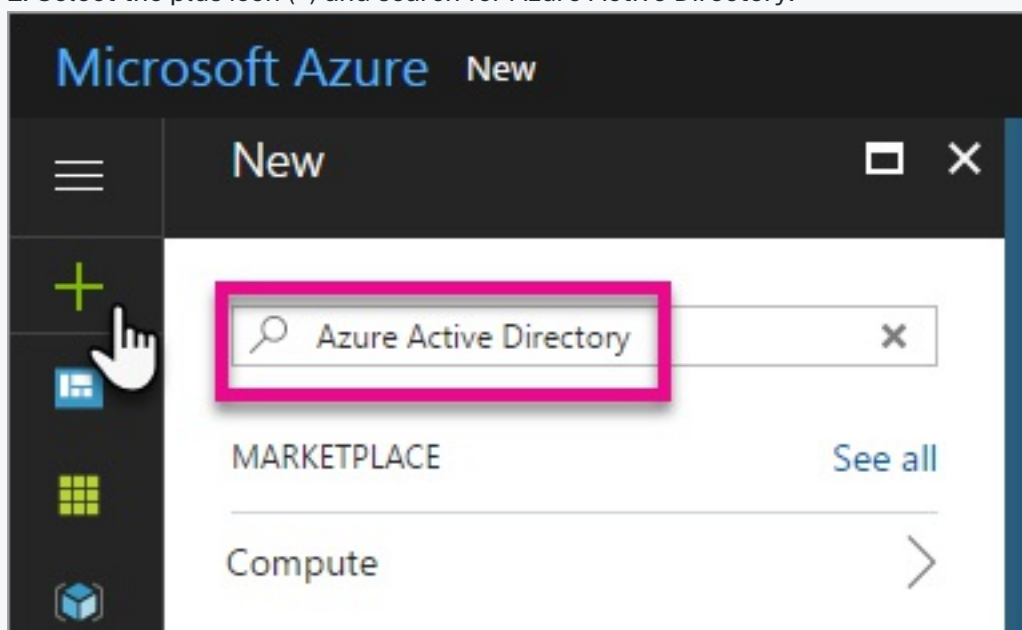
#### Answer:

See the explanation below.

#### Explanation:

Step 1: Create an Azure Active Directory tenant

1. Browse to the Azure portal and sign in with an account that has an Azure subscription.
2. Select the plus icon (+) and search for Azure Active Directory.



3. Select Azure Active Directory in the search results.




4. Select Create.
5. Provide an Organization name and an Initial domain name (12345678). Then select Create. Your directory is created.

## Create directory

\* Organization name ⓘ  
Contoso Direct ✓

\* Initial domain name ⓘ  
contosodirect ✓  
contosodirect.onmicrosoft.com

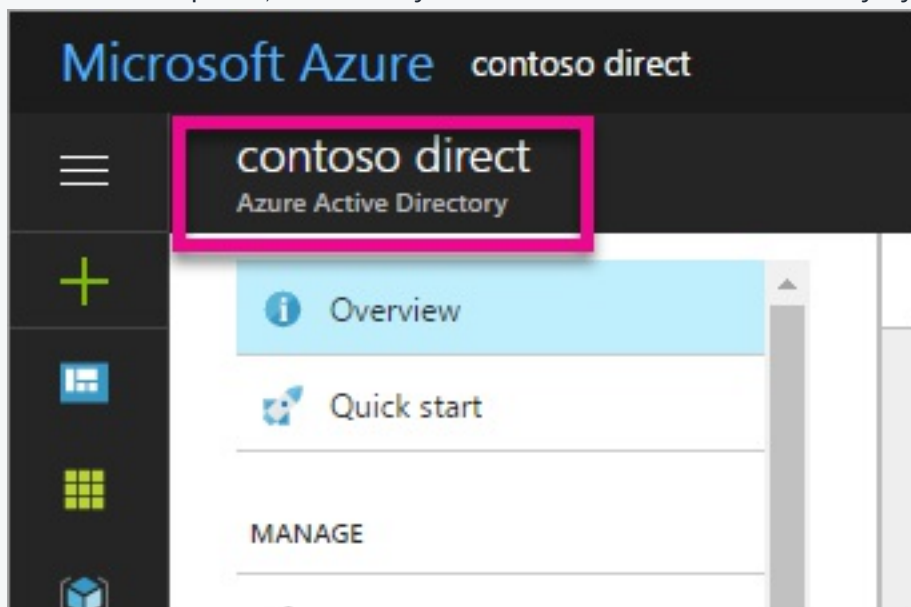
Country or region ⓘ  
United States ▼

 Directory creation will take about one minute.

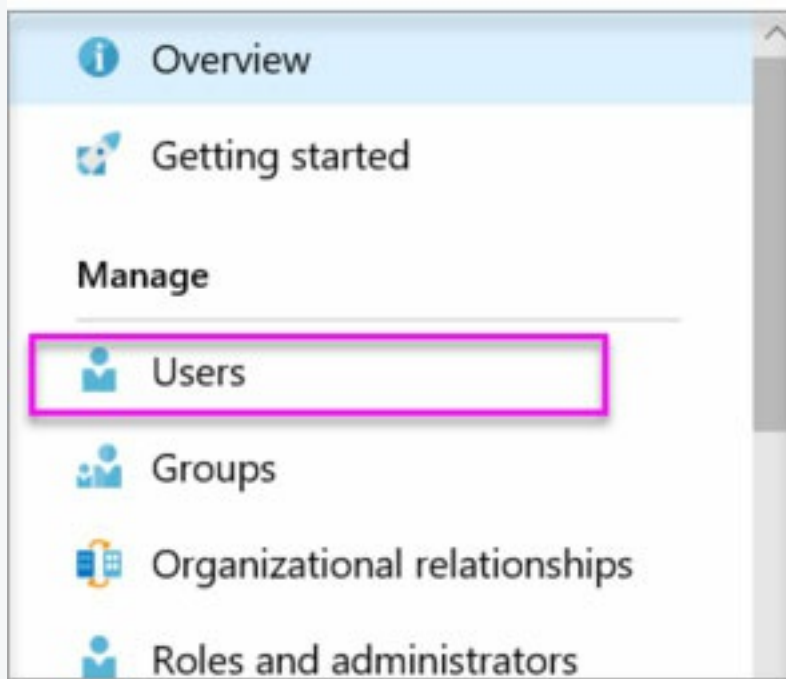
6. After directory creation is complete, select the information box to manage your new directory. Next, you're going to add tenant users.

Step 2: Create an Azure Active Directory tenant user

7. In the Azure portal, make sure you are on the Azure Active Directory fly out.



8. Under Manage, select Users.



9. Select All users and then select + New user.

10. Provide a Name and User name (user1) for the regular user tenant. You can also show the temporary password. When you're done, select Create.

Name: user1 -

User name: [email protected]

User

contoso direct

\*

Name ⓘ

PBI Embed

1

✓

\*

User name ⓘ

pbiembed@contosodirect.onmicrosoft.com

2

✓

Profile ⓘ

Not configured

>

Properties ⓘ

Default

>

Groups ⓘ

0 groups selected

>

Directory role ⓘ

User

3

>

Password

.....

☐ Show Password

Reference:

<https://docs.microsoft.com/en-us/power-bi/developer/create-an-azure-active-directory-tenant>

#### Question: 74

CertyIQ

HOTSPOT -

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

Name	Member of	Multi-factor authentication (MFA) status
User1	Group1, Group2	Enabled
User2	Group1	Disabled
User3	Group1	Disabled

You create and enforce an Azure AD Identity Protection sign-in risk policy that has the following settings:

- Assignments: Include Group1, exclude Group2
- Conditions: Sign-in risk level: Medium and above
- Access: Allow access, Require multi-factor authentication

You need to identify what occurs when the users sign in to Azure AD.

What should you identify for each user? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

## Answer Area

When User1 signs in from an anonymous IP address, the user will:

	▼
Be blocked	
Be prompted for MFA	
Sign in by using a username and password only	

When User2 signs in from an unfamiliar location, the user will:

	▼
Be blocked	
Be prompted for MFA	
Sign in by using a username and password only	

When User3 signs in from an infected device, the user will:

	▼
Be blocked	
Be prompted for MFA	
Sign in by using a username and password only	

Answer:

## Answer Area

When User1 signs in from an anonymous IP address, the user will:

	▼
Be blocked	
Be prompted for MFA	
Sign in by using a username and password only	

When User2 signs in from an unfamiliar location, the user will:

	▼
Be blocked	
Be prompted for MFA	
Sign in by using a username and password only	

When User3 signs in from an infected device, the user will:

	▼
Be blocked	
Be prompted for MFA	
Sign in by using a username and password only	

Explanation:

Reference:

<http://www.rebeladmin.com/2018/09/step-step-guide-configure-risk-based-azure-conditional-access-policies/> <https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-policies> <https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks>

**Question: 75****HOTSPOT -**

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

Name	Multi-factor authentication (MFA) status
User1	Disabled
User2	Disabled
User3	Enforced

In Azure AD Privileged Identity Management (PIM), the Role settings for the Contributor role are configured as shown in the exhibit. (Click the Exhibit tab.)

**Role settings****Assignment**

☐ Allow permanent eligible assignment

Expire eligible assignments after

3 Months



☐ Allow permanent active assignment

Expire active assignments after

1 Month



☒ Require Multi-Factor Authentication on active assignment

☒ Require justification on active assignment

**Activation**

Activation maximum duration (hours)



8

☒ Require Multi-Factor Authentication on activation

☒ Require justification on activation

☐ Require ticket information on activation

☐ Require approval to activate

\* Select approvers

No member or group selected



You assign users the Contributor role on May 1, 2019 as shown in the following table.



Name	Assignment type
User1	Eligible
User2	Active
User3	Active

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

NOTE: Each correct selection is worth one point.

Hot Area:

## Answer Area

Statements	Yes	No
On May 15, 2019, User1 can activate the Contributor role.	<input type="radio"/>	<input type="radio"/>
On May 15, 2019, User2 can use the Contributor role.	<input type="radio"/>	<input type="radio"/>
On June 15, 2019, User3 can activate the Contributor role.	<input type="radio"/>	<input type="radio"/>

Answer:

## Answer Area

Statements	Yes	No
On May 15, 2019, User1 can activate the Contributor role.	<input checked="" type="radio"/>	<input type="radio"/>
On May 15, 2019, User2 can use the Contributor role.	<input checked="" type="radio"/>	<input type="radio"/>
On June 15, 2019, User3 can activate the Contributor role.	<input type="radio"/>	<input checked="" type="radio"/>

Explanation:

YES, YES, NO.

MFA Disabled/Enabled means nothing, its there to trick you. That is for 0365 only "Basic" MFA which wouldn't be in use at this point since in order to use PIM you must have EMS E5 licenses/P2 AD so those MFA enable/disable settings are ignored. They would just get an MFA enrollment wizard/prompt to setup their phone first.



Question: 76



HOTSPOT -

You work at a company named Contoso, Ltd. that has the offices shown in the following table.

Name	IP address space
Boston	180.15.10.0/24
Seattle	132.32.15.0/24

Contoso has an Azure Active Directory (Azure AD) tenant named contoso.com. All contoso.com users have Azure Multi-Factor Authentication (MFA) enabled. The tenant contains the users shown in the following table.

Name	User device	Last sign-in	During last sign-in, user selected Don't ask again for 14 days
User1	Device1	June 1	Yes
User2	Device2	June 3	No

The multi-factor authentication settings for contoso.com are configured as shown in the following exhibit.

# multi-factor authentication

## users service settings

### app passwords [\(learn more\)](#)

- ☒ Allow users to create app passwords to sign in to non-browser apps
- ☐ Do not allow users to create app passwords to sign in to non-browser apps

### trusted ips [\(learn more\)](#)

- ☐ Skip multi-factor authentication for requests from federated users on my intranet

Skip multi-factor authentication for requests from following range of IP address subnets

180.15.10.0/24

### verification options [\(learn more\)](#)

Methods available to users:

- ☐ Call to phone
- ☒ Text message to phone
- ☒ Notification through mobile app
- ☒ Verification code from mobile app or hardware token

### remember multi-factor authentication [\(learn more\)](#)

- ☒ Allow users to remember multi-factor authentication on devices they trust

Days before a device must re-authenticate (1-60):

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

NOTE: Each correct selection is worth one point.

Hot Area:

## Answer Area

Statements	Yes	No
When User1 signs in to Device1 from the Seattle office on June 10, the user will be prompted for MFA.	<input type="radio"/>	<input type="radio"/>
When User2 signs in to Device2 from the Boston office on June 5, the user will be prompted for MFA.	<input type="radio"/>	<input type="radio"/>
When User1 signs in to a new device from the Seattle office on June 7, the user will be prompted for MFA.	<input type="radio"/>	<input type="radio"/>

Answer:

### Answer Area

Statements	Yes	No
When User1 signs in to Device1 from the Seattle office on June 10, the user will be prompted for MFA.	<input type="radio"/>	<input checked="" type="radio"/>
When User2 signs in to Device2 from the Boston office on June 5, the user will be prompted for MFA.	<input type="radio"/>	<input checked="" type="radio"/>
When User1 signs in to a new device from the Seattle office on June 7, the user will be prompted for MFA.	<input checked="" type="radio"/>	<input type="radio"/>

#### Explanation:

Box1: No. because user1 had already signed in from device1 and had selected the 14 day period hence, won't be asked for MFA.

Box2: No because Boston IP range is trusted.

Box3: Yes because new device and Seattle IP is not trusted.

### Question: 77

CertyIQ

You have an Azure subscription.

You configure the subscription to use a different Azure Active Directory (Azure AD) tenant.

What are two possible effects of the change? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. Role assignments at the subscription level are lost.
- B. Virtual machine managed identities are lost.
- C. Virtual machine disk snapshots are lost.
- D. Existing Azure resources are deleted.

Answer: AB

**Explanation:**

When you change to a different Azure AD tenant your user identities are changed to. This basically mean the role assignment assigned to those identities are no longer valid.

When you enable a system-assigned managed identity an identity is created in Azure AD that is tied to the lifecycle of that service instance. So if you change to different Azure AD such an identity is no longer valid.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-how-subscriptions-associated-directory>

**Question: 78****CertyIQ**

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

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

You have an Azure subscription 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.

Reference:

<https://docs.microsoft.com/en-us/rest/api/storageservices/Establishing-a-Stored-Access-Policy>

**Question: 79****CertyIQ**

You have an Azure subscription that contains virtual machines.

You enable just in time (JIT) VM access to all the virtual machines.

You need to connect to a virtual machine by using Remote Desktop.

What should you do first?

A. From Azure Directory (Azure AD) Privileged Identity Management (PIM), activate the Security administrator user role.

B. From Azure Active Directory (Azure AD) Privileged Identity Management (PIM), activate the Owner role for the virtual machine.

- C. From the Azure portal, select the virtual machine, select Connect, and then select Request access.
- D. From the Azure portal, select the virtual machine and add the Network Watcher Agent virtual machine extension.

**Answer: C**

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-machines/windows/connect-logon>

**Question: 80**

**CertyIQ**

HOTSPOT -

Your network contains an on-premises Active Directory domain that syncs to an Azure Active Directory (Azure AD) tenant. The tenant contains the users shown in the following table.

Name	Source
User1	Azure AD
User2	Azure AD
User3	On-premises Active Directory

The tenant contains the groups shown in the following table.

Name	Members
Group1	User1, User2, User3
Group2	User2

You configure a multi-factor authentication (MFA) registration policy that has the following settings:

- Assignments:
  - Include: Group1
  - Exclude: Group2
- Controls: Require Azure MFA registration
- Enforce Policy: On

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

NOTE: Each correct selection is worth one point.

Hot Area:

**Answer Area**

Statements	Yes	No
User1 will be prompted to configure MFA registration during the user's next Azure AD authentication.	<input type="radio"/>	<input type="radio"/>
User2 must configure MFA during the user's next Azure AD authentication.	<input type="radio"/>	<input type="radio"/>
User3 will be prompted to configure MFA registration during the user's next Azure AD authentication.	<input type="radio"/>	<input type="radio"/>



Answer:

### Answer Area

Statements	Yes	No
User1 will be prompted to configure MFA registration during the user's next Azure AD authentication.	<input checked="" type="radio"/>	<input type="radio"/>
User2 must configure MFA during the user's next Azure AD authentication.	<input type="radio"/>	<input checked="" type="radio"/>
User3 will be prompted to configure MFA registration during the user's next Azure AD authentication.	<input checked="" type="radio"/>	<input type="radio"/>

### Question: 81

CertyIQ

SIMULATION -

The developers at your company plan to publish an app named App12345678 to Azure.

You need to ensure that the app is registered to Azure Active Directory (Azure AD). The registration must use the sign-on URLs of <https://app.contoso.com>.

To complete this task, sign in to the Azure portal and modify the Azure resources.

Answer:

See the explanation below.

#### Explanation:

Step 1: Register the Application

1. Sign in to your Azure Account through the Azure portal.



2. Select Azure Active Directory.

3. Select App registrations.

4. Select New registration.

5. Name the application App12345678. Select a supported account type, which determines who can use the application. Under Redirect URI, select Web for the type of application you want to create. Enter the URI: <https://app.contoso.com> , where the access token is sent to.

## Register an application

 If you are building an application for external users that will be distributed by Microsoft, you must register as a first party application to meet all security, privacy, and compliance policies. [Read our decision guide](#) 

### \* Name

The user-facing display name for this application (this can be changed later).

example-app 

### Supported account types

Who can use this application or access this API?

- ☒ Accounts in this organizational directory only (Microsoft)
- ☐ Accounts in any organizational directory
- ☐ Accounts in any organizational directory and personal Microsoft accounts (e.g. Skype, Xbox, Outlook.com)

[Help me choose...](#)

### Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web 

https://contoso.org/exampleapp 

[By proceeding, you agree to the Microsoft Platform Policies](#) 

**Register**

6. Click Register

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/develop/howto-create-service-principal-portal>

## Question: 82

CertyIQ

You have an Azure Active Directory (Azure AD) tenant named contoso.onmicrosoft.com.

The User administrator role is assigned to a user named Admin1.

An external partner has a Microsoft account that uses the [email protected] sign in.

Admin1 attempts to invite the external partner to sign in to the Azure AD tenant and receives the following error message: 'Unable to invite user [email protected] Generic authorization exception.'

You need to ensure that Admin1 can invite the external partner to sign in to the Azure AD tenant.

What should you do?

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



- B. From the Organizational relationships blade, add an identity provider.
- C. From the Custom domain names blade, add a custom domain.
- D. From the Users blade, modify the External collaboration settings.

**Answer: D**

**Explanation:**

You need to allow guest invitations in the External collaboration settings.

**Question: 83**

CertyIQ

You have an Azure Active Directory (Azure AD) tenant.  
You have the deleted objects shown in the following table.

Name	Type	Deleted on
Group1	Security group	April 5, 2020
Group2	Office 365 group	April 5, 2020
User1	User	March 25, 2020
User2	User	April 30, 2020

On May 4, 2020, you attempt to restore the deleted objects by using the Azure Active Directory admin center.  
Which two objects can you restore? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. Group1
- B. Group2
- C. User2
- D. User1

**Answer: BC**

**Explanation:**

Deleted users and deleted Office 365 groups are available for restore for 30 days.  
You cannot restore a deleted security group.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/groups-restore-deleted>

**Question: 84**

CertyIQ

HOTSPOT -

You have an Azure subscription named Subscription1 that contains the resources shown in the following table.

Name	Type	In resource group
8372f433-2dcd-4361-b5ef-5b188fed87d0	Subscription ID	Not applicable
RG1	Resource group	Not applicable
VM1	Virtual machine	RG1
VNET1	Virtual network	RG1
storage1	Storage account	RG1
User1	User account	Not applicable

You create an Azure role by using the following JSON file.

```
{
  "properties":{
    "roleName": "Role1",
    "description": "",
    "assignableScopes": [
      "/subscriptions/8372f433-2dcd-4361-b5ef-5b188fed87d0",
      "/subscriptions/8372f433-2dcd-4361-b5ef-5b188fed87d0/resourceGroups/RG1"
    ],
    "permissions": [
      {
        "actions": [
          "Microsoft.Compute/*"
        ],
        "notActions": [],
        "dataActions": [],
        "notDataActions": []
      }
    ]
  }
}
```

You assign Role1 to User1 for RG1.

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

NOTE: Each correct selection is worth one point.

Hot Area:

### Answer Area

Statements	Yes	No
User1 can create a new virtual machine in RG1.	<input type="radio"/>	<input type="radio"/>
User1 can modify the properties of storage1.	<input type="radio"/>	<input type="radio"/>
User1 can attach the network interface of VM1 to VNET1.	<input type="radio"/>	<input type="radio"/>

Answer:

### Answer Area

Statements	Yes	No
User1 can create a new virtual machine in RG1.	<input type="radio"/>	<input checked="" type="radio"/>
User1 can modify the properties of storage1.	<input type="radio"/>	<input checked="" type="radio"/>
User1 can attach the network interface of VM1 to VNET1.	<input type="radio"/>	<input checked="" type="radio"/>

Explanation:

NO

NO

NO

Reference:

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

**Question: 85**

You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains a user named User1. You plan to publish several apps in the tenant. You need to ensure that User1 can grant admin consent for the published apps. Which two possible user roles can you assign to User1 to achieve this goal? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. Security administrator
- B. Cloud application administrator
- C. Application administrator
- D. User administrator
- E. Application developer

**Answer: BC****Explanation:**

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/grant-admin-consent>**Question: 86**

You have an Azure subscription that is associated with an Azure Active Directory (Azure AD) tenant. When a developer attempts to register an app named App1 in the tenant, the developer receives the error message shown in the following exhibit.

## You do not have access



Access denied

You do not have access

You don't have permission to register applications in the sk200510outlook (Default Directory) directory. To request access, contact your administrator.

### Summary



Session ID  
f8e55e67d10141b4bf0c7ac5115b3be7

Resource ID  
Not available

Extension  
Microsoft\_AAD\_RegisteredApps

Content  
CreateApplicationBlade

Error code  
403

You need to ensure that the developer can register App1 in the tenant.  
What should you do for the tenant?

- A. Modify the Directory properties.
- B. Set Enable Security defaults to Yes.
- C. Configure the Consent and permissions settings for enterprise applications.
- D. Modify the User settings.

**Answer: D**

#### Explanation:

Microsoft itself uses the default configuration with users able to register applications and consent to applications on their own behalf.

To prevent users from registering their own applications:

In the Azure portal, go to the User settings section under Azure Active Directory

Change Users can register applications to No.

Reference:

### Question: 87

CertyIQ

You have an Azure subscription that contains an Azure Active Directory (Azure AD) tenant and a user named User1. The App registrations settings for the tenant are configured as shown in the following exhibit.

## App registrations

Users can register applications ⓘ

Yes

No

You plan to deploy an app named App1.

You need to ensure that User1 can register App1 in Azure AD. The solution must use the principle of least privilege. Which role should you assign to User1?

- A. App Configuration Data Owner for the subscription
- B. Managed Application Contributor for the subscription
- C. Cloud application administrator in Azure AD
- D. Application developer in Azure AD

**Answer: D**

**Explanation:**

Assign the Application Developer role to grant the ability to create application registrations when the Users can register applications setting is set to No. This role also grants permission to consent on one's own behalf when the Users can consent to apps accessing company data on their behalf setting is set to No.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/roles/delegate-by-task>

### Question: 88

CertyIQ

You have the Azure virtual machines shown in the following table.

Name	Location	Connected to
VM1	West US 2	VNET1/Subnet1
VM2	West US 2	VNET1/Subnet1
VM3	West US 2	VNET1/Subnet2
VM4	East US	VNET2/Subnet3
VM5	West US 2	VNET5/Subnet5

Each virtual machine has a single network interface.

You add the network interface of VM1 to an application security group named ASG1.

You need to identify the network interfaces of which virtual machines you can add to ASG1.

What should you identify?

- A. VM2 only
- B. VM2 and VM3 only

- C. VM2, VM3, VM4, and VM5
- D. VM2, VM3, and VM5 only

**Answer: B**

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-network/application-security-groups>

### Question: 89

CertyIQ

SIMULATION -

You need to create a new Azure Active Directory (Azure AD) directory named 12345678.onmicrosoft.com. The new directory must contain a user named user12345678 who is configured to sign in by using Azure Multi-Factor Authentication (MFA).

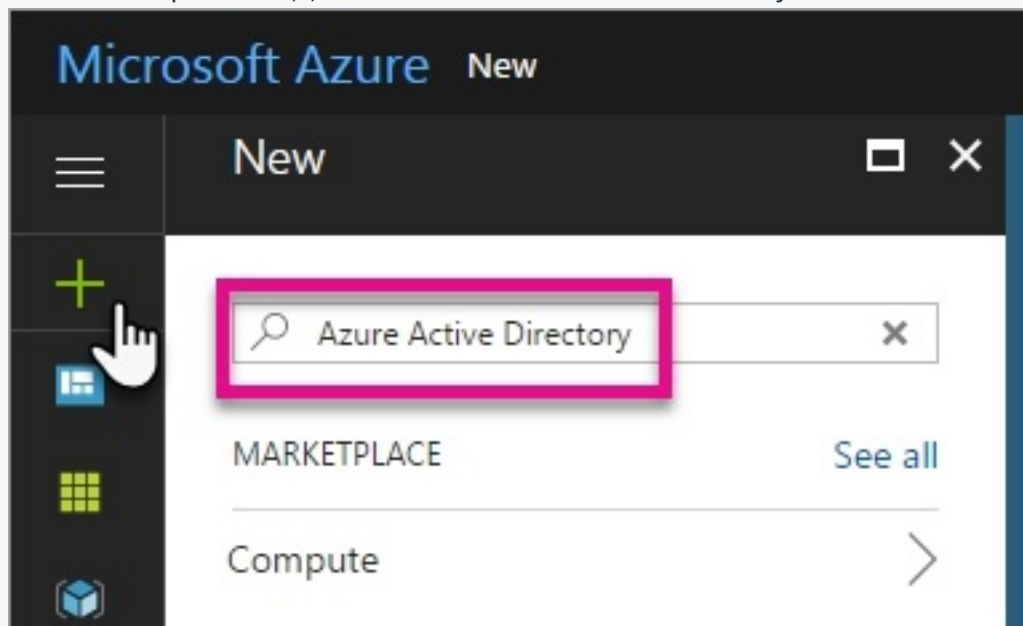
**Answer:**

See the explanation below.

**Explanation:**

To create a new Azure AD tenant:

1. Browse to the Azure portal and sign in with an account that has an Azure subscription.
2. Select the plus icon (+) and search for Azure Active Directory.



3. Select Azure Active Directory in the search results.



4. Select Create.

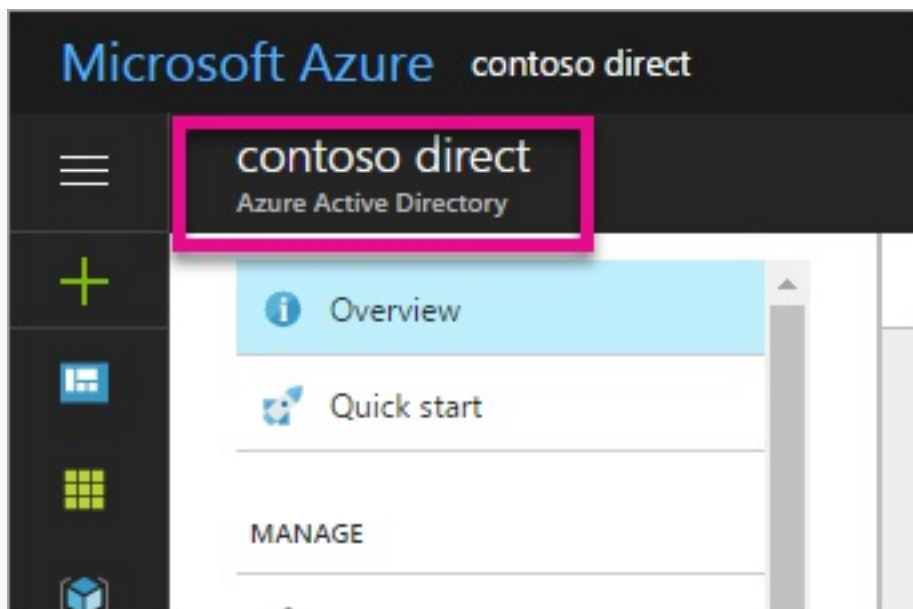
5. Provide an Organization name (12345678) and an Initial domain name (12345678). Then select Create. This will create the directory named 12345678.onmicrosoft.com.

A screenshot of the 'Create directory' form in the Azure portal. The form has a dark header with the title 'Create directory' and window control buttons. The form contains several fields: 'Organization name' with the value 'Contoso Direct' and a green checkmark; 'Initial domain name' with the value 'contosodirect' and a green checkmark; and a dropdown for 'Country or region' with the value 'United States'. Below these fields, the domain name 'contosodirect.onmicrosoft.com' is displayed. At the bottom, there is an information box with a blue 'i' icon and the text 'Directory creation will take about one minute.'

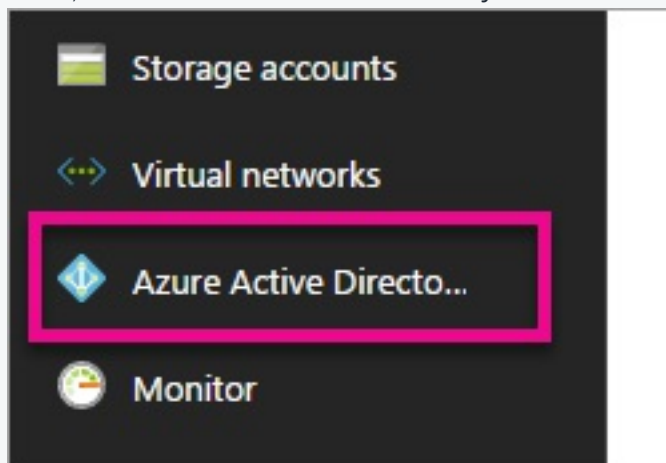
6. After directory creation is complete, select the information box to manage your new directory.  
To create the user:

1. In the Azure portal, make sure you are on the Azure Active Directory fly out.

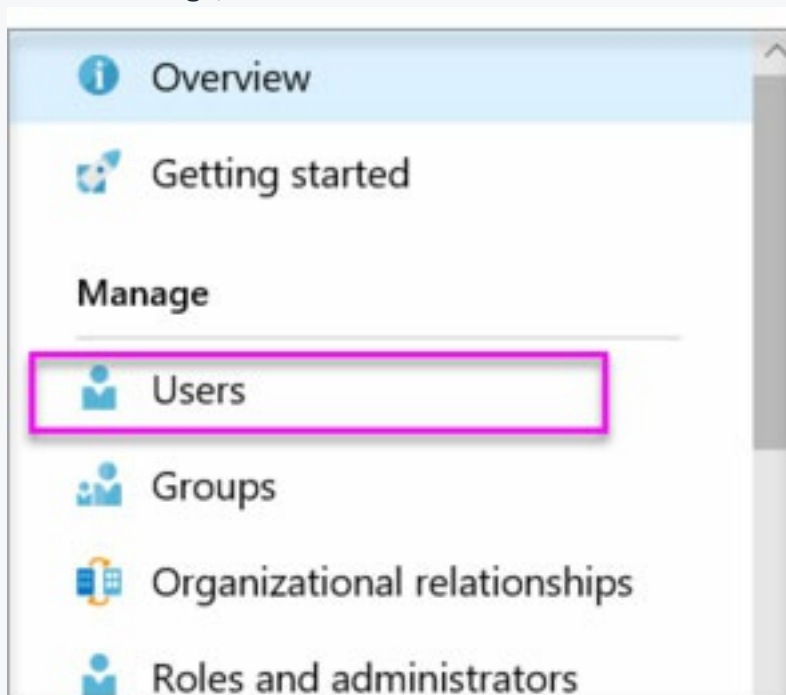




If not, select the Azure Active Directory icon from the left services navigation.



2. Under Manage, select Users.

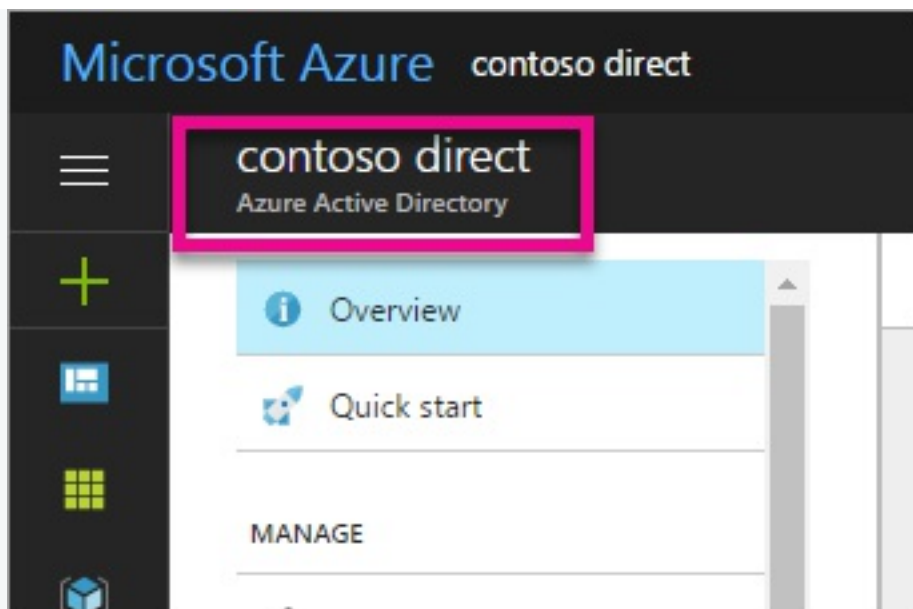


3. Select All users and then select + New user.

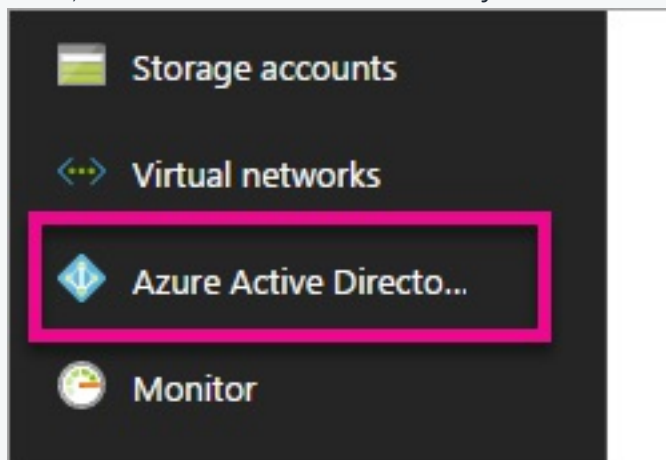
4. Provide a Name and User name (user12345678) for the user. When you're done, select Create.

To enable MFA:

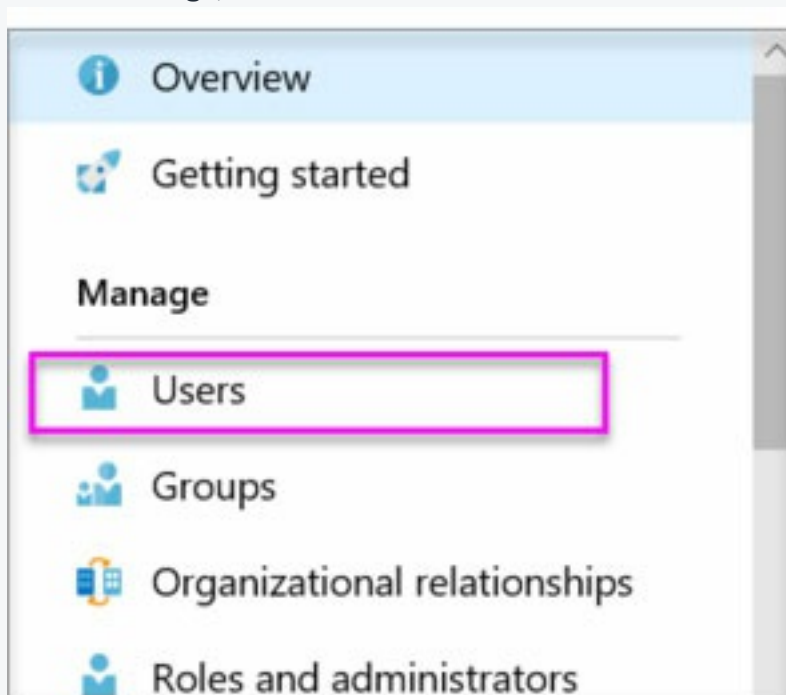
1. In the Azure portal, make sure you are on the Azure Active Directory fly out.



If not, select the Azure Active Directory icon from the left services navigation.



2. Under Manage, select Users.



3. Click on the Multi-Factor Authentication link.

4. Tick the checkbox next to the user's name and click the Enable link.

Reference:

<https://docs.microsoft.com/en-us/power-bi/developer/create-an-azure-active-directory-tenant>

**Question: 90**

You have an Azure subscription named Subscription1 that contains an Azure Active Directory (Azure AD) tenant named contoso.com and a resource group named RG1.

You create a custom role named Role1 for contoso.com. Where you can use Role1 for permission delegation?

- A. contoso.com only
- B. contoso.com and RG1 only
- C. contoso.com and Subscription1 only
- D. contoso.com, RG1, and Subscription1

**Answer: A**

**Explanation:**

contoso.com only

Azure AD role permissions can't be used in Azure custom roles and vice versa.

<https://docs.microsoft.com/en-us/azure/active-directory/roles/custom-overview>

**Question: 91**

You have an Azure subscription.

You enable Azure Active Directory (Azure AD) Privileged Identity Management (PIM).

Your company's security policy for administrator accounts has the following conditions:

- The accounts must use multi-factor authentication (MFA).
- The accounts must use 20-character complex passwords.
- The passwords must be changed every 180 days.
- The accounts must be managed by using PIM.

You receive multiple alerts about administrators who have not changed their password during the last 90 days.

You need to minimize the number of generated alerts.

Which PIM alert should you modify?

- A. Roles are being assigned outside of Privileged Identity Management
- B. Roles don't require multi-factor authentication for activation
- C. Administrators aren't using their privileged roles
- D. Potential stale accounts in a privileged role

**Answer: D**

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-configure-security-alerts?tabs=new>

**Question: 92**

Your network contains an on-premises Active Directory domain named adatum.com that syncs to Azure Active Directory (Azure AD). Azure AD Connect is installed on a domain member server named Server1.

You need to ensure that a domain administrator for the adatum.com domain can modify the synchronization options. The solution must use the principle of least privilege.

Which Azure AD role should you assign to the domain administrator?

- A. Security administrator
- B. Global administrator
- C. User administrator

**Answer: B**

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/reference-connect-accounts-permissions>

### Question: 93

CertyIQ

You have an Azure subscription that contains the users shown in the following table.

Name	Subscription role	Azure Active Directory (Azure AD) user role	Multi-factor authentication (MFA) status
User1	Owner	Authentication administrator	Enabled
User2	None	Global administrator	Enforced
User3	None	Global administrator	Disabled

Which users can enable Azure AD Privileged Identity Management (PIM)?

- A. User2 and User3 only
- B. User1 and User2 only
- C. User2 only
- D. User1 only

**Answer: A**

**Explanation:**

For Azure AD roles in PIM, only a user who is in the Privileged Role Administrator or Global Administrator role can manage assignments for other administrators.

Global Administrators, Security Administrators, Global Readers, and Security Readers can also view assignments to Azure AD roles in PIM.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-deployment-plan>

### Question: 94

CertyIQ

You have an Azure subscription.

You plan to create a custom role-based access control (RBAC) role that will provide permission to read the Azure Storage account.

Which property of the RBAC role definition should you configure?

- A. NotActions []
- B. DataActions []
- C. AssignableScopes []

#### D. Actions []

**Answer: D**

**Explanation:**

To 'Read a storage account', ie. list the blobs in the storage account, you need an 'Action' permission.  
To read the data in a storage account, ie. open a blob, you need a 'DataAction' permission.

Reference:

<https://docs.microsoft.com/en-us/azure/role-based-access-control/role-definitions>

#### Question: 95

CertyIQ

You have an Azure subscription linked to an Azure Active Directory Premium Plan 1 tenant.  
You plan to implement Azure Active Directory (Azure AD) Identity Protection.  
You need to ensure that you can configure a user risk policy and a sign-in risk policy.  
What should you do first?

- A. Purchase Azure Active Directory Premium Plan 2 licenses for all users.
- B. Register all users for Azure Multi-Factor Authentication (MFA).
- C. Enable security defaults for Azure AD.
- D. Enable Azure Defender in Azure Security Center.

**Answer: A**

**Explanation:**

To configure a user risk policy and a sign-in risk policy, you need to set the MFA.

And to use MFA, you need to Azure AD tenant with at least an Azure AD Premium P2.

Reference:

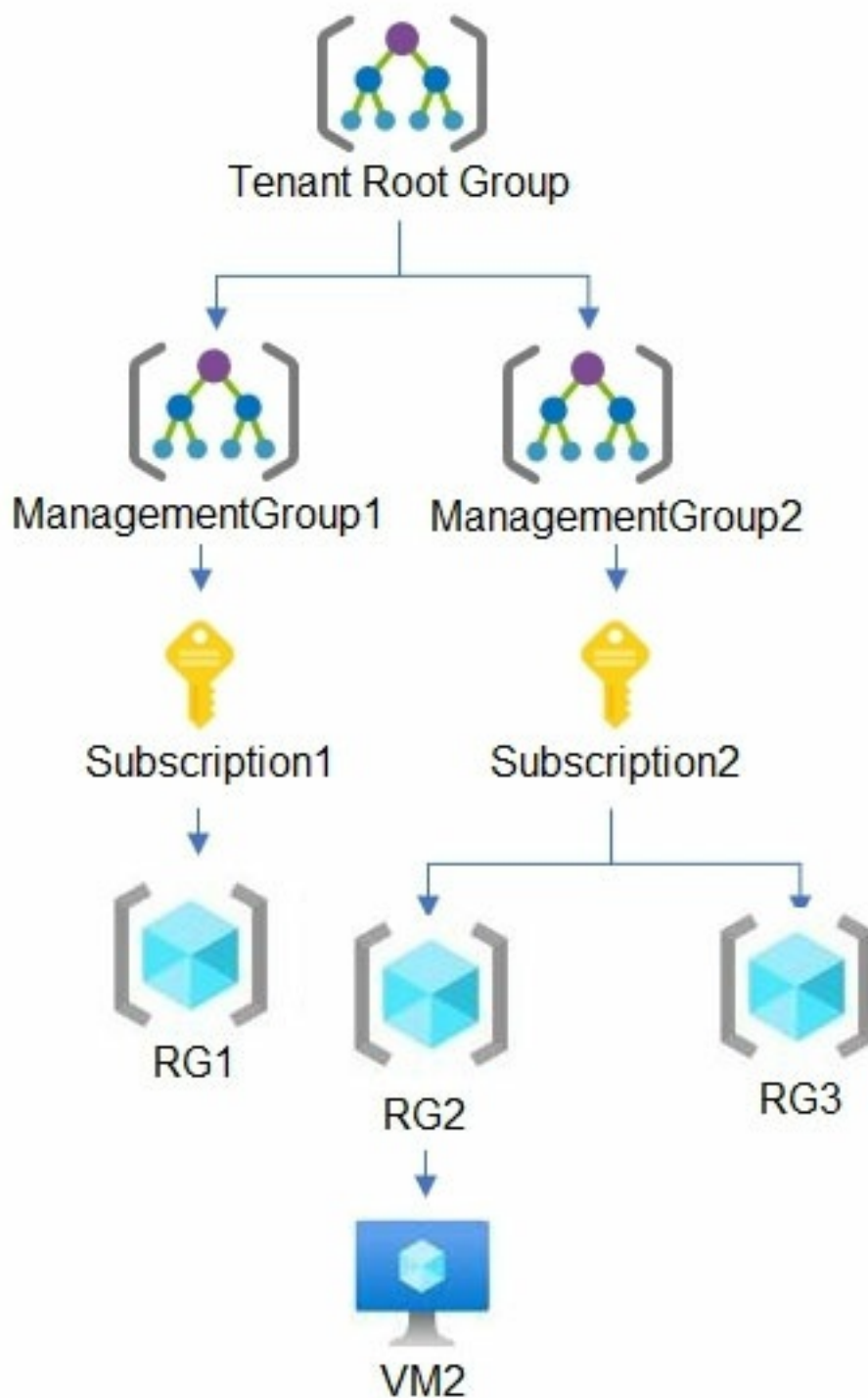
<https://docs.microsoft.com/en-us/azure/active-directory/authentication/tutorial-risk-based-sspr-mfa>

#### Question: 96

CertyIQ

HOTSPOT -

You have the hierarchy of Azure resources shown in the following exhibit.



RG1, RG2, and RG3 are resource groups.

RG2 contains a virtual machine named VM2.

You assign role-based access control (RBAC) roles to the users shown in the following table.

Name	Role	Added to resource
User1	Contributor	Tenant Root Group
User2	Virtual Machine Contributor	Subscription2
User3	Virtual Machine Administrator Login	RG2

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

NOTE: Each correct selection is worth one point.

Hot Area:



## Answer Area

Statements	Yes	No
User1 can deploy virtual machines to RG1.	<input type="radio"/>	<input type="radio"/>
User2 can delete VM2.	<input type="radio"/>	<input type="radio"/>
User3 can reset the password of the built-in Administrator account of VM2.	<input type="radio"/>	<input type="radio"/>

Answer:

### Answer Area

Statements	Yes	No
User1 can deploy virtual machines to RG1.	<input checked="" type="radio"/>	<input type="radio"/>
User2 can delete VM2.	<input checked="" type="radio"/>	<input type="radio"/>
User3 can reset the password of the built-in Administrator account of VM2.	<input type="radio"/>	<input checked="" type="radio"/>

Explanation:

1) Yes

Source : <https://docs.microsoft.com/fr-fr/azure/governance/management-groups/overview>

2) Yes

The role has this rights :

Microsoft.Compute/virtualMachines/\*

Perform all virtual machine actions including create, update, delete, start, restart, and power off virtual machines. Execute predefined scripts on virtual machines.

Source : <https://docs.microsoft.com/fr-fr/azure/role-based-access-control/built-in-roles#virtual-machine-contributor>

3) No

Virtual Machine Administrator Login -> View Virtual Machines in the portal and login as administrator

## Question: 97

CertyIQ

HOTSPOT -

You plan to implement an Azure function named Function1 that will create new storage accounts for containerized application instances.

You need to grant Function1 the minimum required privileges to create the storage accounts. The solution must minimize administrative effort.

What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

## Answer Area

Assign role to:

	▼
A group account	
A system-assigned managed identity	
A user account	
A user-assigned managed identity	

Role assignment to create:

	▼
Built-in role assignment	
Classic administrator role assignment	
Custom role-based access control (RBAC) role assignment	

Answer:

## Answer Area

Assign role to:

	▼
A group account	
A system-assigned managed identity	
A user account	
A user-assigned managed identity	

Role assignment to create:

	▼
Built-in role assignment	
Classic administrator role assignment	
Custom role-based access control (RBAC) role assignment	

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/overview> <https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/howto-assign-access-portal>

## Question: 98

CertyIQ

You have an Azure subscription that is linked to an Azure Active Directory (Azure AD) tenant. From the Azure portal, you register an enterprise application. Which additional resource will be created in Azure AD?

- A. a service principal
- B. an X.509 certificate
- C. a managed identity
- D. a user account

Answer: A

**Explanation:**

The 2 types of objects get created once the app registration is done:

Application Object

Service principal object

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-how-applications-are-added>

**Question: 99****CertyIQ**







HOTSPOT -



You have an Azure Active Directory (Azure AD) tenant that contains the resources shown in the following table.


Name	Type
User1	User
User2	User
User3	User
Group1	Security group
Group2	Security group
App1	Enterprise application

User2 is the owner of Group2.

The user and group settings for App1 are configured as shown in the following exhibit.

 Add user  Edit  Remove  Update Credentials  Columns  Got feedback?

 The application will appear on the access panel for assigned users. Set 'visible to users?' to no in properties to prevent this. 

DISPLAY NAME	OBJECT TYPE	ROLE ASSIGNED
<input type="checkbox"/>  Group1	Group	Default Access

You enable self-service application access for App1 as shown in the following exhibit.

Allow users to request access to this application? ⓘ

Yes

No

To which group should assigned users be added? ⓘ

Select group

Group2



Require approval before granting access to this application? ⓘ

Yes

No

Who is allowed to approve access to this application? ⓘ

Select approvers

1 users selected



To which role should users be assigned in this application? ⓘ

\*Select a role

Default Access



User3 is configured to approve access to App1.

After you enable self-service application access for App1, who will be configured as the Group2 owner and who will be configured as the App1 users? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

## Answer Area

Group2 owners:

	▼
User2 only	
User3 only	
User1 and User2 only	
User2 and User3 only	
User1, User2, and User3	

App1 users:

	▼
Group1 members only	
Group2 members only	
Group1 and Group2 members only	
Group1 and Group2 members and User1 only	
Group1 and Group2 members, User1, and User3 only	

Answer:

## Answer Area

Group2 owners:

	▼
User2 only	
User3 only	
User1 and User2 only	
User2 and User3 only	
User1, User2, and User3	

App1 users:

	▼
Group1 members only	
Group2 members only	
Group1 and Group2 members only	
Group1 and Group2 members and User1 only	
Group1 and Group2 members, User1, and User3 only	

### Explanation:

Group2 owners: User 3 Only

App1 users: Group 1 and Group 2 members only

## Question: 100

CertyIQ

### HOTSPOT -

You have a management group named Group1 that contains an Azure subscription named sub1. Sub1 has a subscription ID of 11111111-1234-1234-1234-1111111111.

You need to create a custom Azure role-based access control (RBAC) role that will delegate permissions to manage the tags on all the objects in Group1.

What should you include in 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

Resource provider:

	▼
Microsoft.Authorization	
Microsoft.Resources	
Microsoft.Support	

Assignable scope:

	▼
/	
/Group1	
/subscriptions/11111111-1234-1234-1234-1111111111	



Answer:

### Answer Area

Resource provider:

Microsoft.Authorization  
Microsoft.Resources  
Microsoft.Support

Assignable scope:

/  
/Group1  
/subscriptions/11111111-1234-1234-1234-1111111111

### Explanation:

Microsoft resource providers

Assignable Scope is Management Group Now which is /Group1

On the Assignable scopes tab, you specify where your custom role is available for assignment, such as management group, subscriptions, or resource groups.

Reference:

<https://docs.microsoft.com/en-us/azure/role-based-access-control/custom-roles-portal#step-5-assignable-scopes>

### Question: 101

CertyIQ

HOTSPOT -

You have an Azure subscription that contains the custom roles shown in the following table.

Name	Type
Role1	Azure Active Directory (Azure AD)
Role2	Azure subscription

In the Azure portal, you plan to create new custom roles by cloning existing roles. The new roles will be configured as shown in the following table.

Name	Type
Role3	Azure AD
Role4	Azure subscription

Which roles can you clone to create each new role? To answer, select the appropriate options in the answer area.  
NOTE: Each correct selection is worth one point.

Hot Area:



## Answer Area

Role3:

Role4:

Answer:

### Answer Area

Role3:

Role4:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/roles/custom-create> <https://docs.microsoft.com/en-us/azure/role-based-access-control/custom-roles-portal>

## Question: 102

CertyIQ

HOTSPOT -

You have an Azure subscription that contains the Azure Active Directory (Azure AD) resources shown in the following table.

Name	Description
User1	User
Group1	Security group that has a Membership type of Dynamic Device
Managed1	Managed identity
App1	Enterprise application

You create the groups shown in the following table.

Name	Description
Group5	Security group that has a Membership type of Assigned
Group6	Microsoft 365 group that has a Membership type of Assigned

Which resources can you add to Group5 and Group6? To answer, select the appropriate options in the answer area.  
NOTE: Each correct selection is worth one point.

Hot Area:

## Answer Area

Group5:

User1 only
User1 and Group1 only
User1, Group1, and Managed1 only
User1, Group1, Managed1, and App1

Group6:

User1 only
User1 and Group1 only
User1, Group1, and Managed1 only
User1, Group1, Managed1, and App1

Answer:

## Answer Area

Group5:

User1 only
User1 and Group1 only
User1, Group1, and Managed1 only
User1, Group1, Managed1, and App1


Group6:


User1 only
User1 and Group1 only
User1, Group1, and Managed1 only
User1, Group1, Managed1, and App1


HOTSPOT -  
You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains three security groups named Group1, Group2, and Group3 and the users shown in the following table.


Name	Role	Member of
User1	Application administrator	Group1
User2	Application developer	Group2
User3	Cloud application administrator	Group3


Group3 is a member of Group2.  
In contoso.com, you register an enterprise application named App1 that has the following settings:  
= Owners: User1  
= Users and groups: Group2  
You configure the properties of App1 as shown in the following exhibit.

 Save

 Discard


 Delete

 Got feedback


Enabled for users to sign-in? 


Yes


No

Name  \*


App1


Homepage URL 

Logo 





Select a file




Application ID 


75082794-3617-4347-ac6d-88cfda564072



Object ID 


4926ab6c-ef57-4c9f-a028-f6d635cde655



User assignment required? 


Yes

No

Visible to users 

Yes

No

Notes 

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

## Answer Area

Statements	Yes	No
User1 has App1 listed on his My Apps portal.	<input type="radio"/>	<input type="radio"/>
User2 has App1 listed on her My Apps portal.	<input type="radio"/>	<input type="radio"/>
User3 has App1 listed on her My Apps portal.	<input type="radio"/>	<input type="radio"/>

Answer:

## Answer Area

Statements	Yes	No
User1 has App1 listed on his My Apps portal.	<input type="radio"/>	<input checked="" type="radio"/>
User2 has App1 listed on her My Apps portal.	<input checked="" type="radio"/>	<input type="radio"/>
User3 has App1 listed on her My Apps portal.	<input type="radio"/>	<input checked="" type="radio"/>

Explanation:

1. Owners don't see app in MyApps portal unless they are also assigned the App via group or user assignment.  
- No
2. User 2 is part of Group 2 so and the app is visible so will show in MyApps portal. - Yes
3. User 3 is in Group 3 that is a member of Group 2 but nested groups aren't supported in App assignments so only direct Group 2 membership will work. - No

### Question: 104

CertyIQ

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

Name	Type	Description
RG1	Resource group	Used to store virtual machines
RG2	Resource group	Used to store virtual networks
ServerAdmins	Security group	Used to manage virtual machines

You need to ensure that ServerAdmins can perform the following tasks:

- Create virtual machines in RG1 only.
- Connect the virtual machines to the existing virtual networks in RG2 only.

The solution must use the principle of least privilege.

Which two role-based access control (RBAC) roles should you assign to ServerAdmins? Each correct answer

presents part of the solution.  
NOTE: Each correct selection is worth one point.

- A. a custom RBAC role for RG2
- B. the Network Contributor role for RG2
- C. the Contributor role for the subscription
- D. a custom RBAC role for the subscription
- E. the Network Contributor role for RG1
- F. the Virtual Machine Contributor role for RG1

**Answer: AF**

**Explanation:**

- A. a custom RBAC role for RG2 - would provide least priv over RG2
- B. the Network Contributor role for RG2 - provides too much priv over RG2
- C. the Contributor role for the subscription - Cannot be C
- D. a custom RBAC role for the subscription - to much permission
- E. the Network Contributor role for RG1 - Cannot be E
- F. the Virtual Machine Contributor role for RG1 - required to create VM's

Therefore A and F would provide least priv to perform tasks.

Reference:

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

### Question: 105

CertyIQ

HOTSPOT -

Your network contains an on-premises Active Directory domain named adatum.com that syncs to Azure Active Directory (Azure AD).

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

Name	Source	Password
User1	Azure AD	Adatum123
User2	Azure AD	N3w3rT0Gue33
User3	On-premises Active Directory	ComplexPassword33

You configure the Authentication methods "" Password Protection settings for adatum.com as shown in the following exhibit.



## Custom smart lockout

Lockout threshold ⓘ

10



Lockout duration in seconds ⓘ

60



## Custom banned passwords

Enforce custom list ⓘ

Yes

No

Custom banned password list ⓘ

Adatum



## Password protection for Windows Server Active Directory

Enable password protection on Windows Server Active Directory ⓘ

Yes

No

Mode ⓘ

Enforced

Audit

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

NOTE: Each correct selection is worth one point.

Hot Area:

### Answer Area

Statements	Yes	No
User1 will be prompted to change the password on the next sign-in.	<input type="radio"/>	<input type="radio"/>
User2 can change the password to @d@tum_C0mpleX123.	<input type="radio"/>	<input type="radio"/>
User3 can change the password to Adatum123!.	<input type="radio"/>	<input type="radio"/>

Answer:

### Answer Area

Statements	Yes	No
User1 will be prompted to change the password on the next sign-in.	<input type="radio"/>	<input checked="" type="radio"/>
User2 can change the password to @d@tum_C0mpleX123.	<input checked="" type="radio"/>	<input type="radio"/>
User3 can change the password to Adatum123!.	<input checked="" type="radio"/>	<input type="radio"/>

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-password-ban-bad-on-premise-s-deploy> <https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-password-ban-bad>



## HOTSPOT -

Your company has an Azure subscription named Subscription1. Subscription1 is associated with the Azure Active Directory tenant that includes the users shown in the following table.

Name	Role
User1	Global administrator
User2	Billing administrator
User3	Owner
User4	Account Admin

The company is sold to a new owner.

The company needs to transfer ownership of Subscription1.

Which user can transfer the ownership and which tool should the user use? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

## Answer Area

User:

▼

User1

User2

User3

User4

Tool:

▼

Azure Account Center

Azure Cloud Shell

Azure PowerShell

Azure Security Center

Answer:

## Answer Area

User: 

Tool: 

### Explanation:

1. User2-Billing Administrator
2. Azure Portal ( Azure account center)

## Question: 107

CertyIQ

You have an Azure subscription that uses Azure Active Directory (Azure AD) Privileged Identity Management (PIM). A PIM user that is assigned the User Access Administrator role reports receiving an authorization error when performing a role assignment or viewing the list of assignments. You need to resolve the issue by ensuring that the PIM service principal has the correct permissions for the subscription. The solution must use the principle of least privilege. Which role should you assign to the PIM service principle?

- A. Contributor
- B. User Access Administrator
- C. Managed Application Operator
- D. Resource Policy Contributor

### Answer: B

### Explanation:

Reference:

<https://docs.microsoft.com/bs-latn-ba/azure/active-directory/privileged-identity-management/pim-troubleshoot>

## Question: 108

CertyIQ

You have an Azure Active Directory (Azure AD) tenant that contains a user named Admin1. Admin1 is assigned the Application developer role. You purchase a cloud app named App1 and register App1 in Azure AD. Admin1 reports that the option to enable token encryption for App1 is unavailable. You need to ensure that Admin1 can enable token encryption for App1 in the Azure portal. What should you do?

- A. Upload a certificate for App1.
- B. Modify the API permissions of App1.
- C. Add App1 as an enterprise application.
- D. Assign Admin1 the Cloud application administrator role.

**Answer: A**

**Explanation:**

To enable token encryption for App1 in the Azure portal, you should upload a certificate for App1. Token encryption in Azure AD requires a public key of a certificate to encrypt the tokens. Once the certificate is uploaded, Admin1, with the Application developer role, should be able to enable token encryption for App1. So, the correct answer is A. Upload a certificate for App1.

**Question: 109**

**CertyIQ**

You plan to deploy an app that will modify the properties of Azure Active Directory (Azure AD) users by using Microsoft Graph.

You need to ensure that the app can access Azure AD.

What should you configure first?

- A. an app registration
- B. an external identity
- C. a custom role-based access control (RBAC) role
- D. an Azure AD Application Proxy

**Answer: A**

**Explanation:**

just create a service principal under App Registration

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-how-applications-are-added>

**Question: 110**

**CertyIQ**

HOTSPOT -

You have an Azure subscription named Subscription1 that contains the resources shown in the following table.

Name	Type	In resource group
cont1	Container instance	RG1
VNET1	Virtual network	RG1
App1	App Service app	RG1
VM1	Virtual machine	RG1
User1	User	<b>Not applicable</b>

You create a custom RBAC role in Subscription1 by using the following JSON file.

```
{
  "Name": "Role1",
  "IsCustom": true,
  "Description": "Role1 description",
  "Actions": [
    "*/Read",
    "Microsoft.Compute/*"
  ],
  "NotActions": [],
  "DataActions": [],
  "NotDataActions": [],
  "AssignableScopes": [
    "/subscriptions/923a419a-4358-40fb-b4a9-b8af43dd0c92/resourceGroups/RG1"
  ]
}
```

You assign Role1 to User1 on RG1.

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

NOTE: Each correct selection is worth one point.

Hot Area:

## Answer Area

Statements	Yes	No
User1 can add VM1 to VNET1.	<input type="radio"/>	<input type="radio"/>
User1 can start and stop App1.	<input type="radio"/>	<input type="radio"/>
User1 can start and stop cont1.	<input type="radio"/>	<input type="radio"/>

Answer:

## Answer Area

Statements	Yes	No
User1 can add VM1 to VNET1.	<input type="radio"/>	<input checked="" type="radio"/>
User1 can start and stop App1.	<input type="radio"/>	<input checked="" type="radio"/>
User1 can start and stop cont1.	<input type="radio"/>	<input checked="" type="radio"/>

Explanation:

Reference:

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

### Question: 111

CertyIQ

HOTSPOT -

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

Name	Type	Resource group	Location
RG1	Resource group	<b>Not applicable</b>	West US
Managed1	Managed identity	RG1	West US

The subscription is linked to an Azure Active Directory (Azure AD) tenant that contains the users shown in the following table.

Name	Usage location
User1	United States
User2	Germany

You create the groups shown in the following table.

Name	Type	Membership type
Group1	Security	Dynamic User
Group2	Microsoft 365	Dynamic User

The membership rules for Group1 and Group2 are configured as shown in the following exhibit.

Dynamic membership rules

...

×

 Save

 Discard



|

 Got feedback?

Configure Rules

Validate Rules (Preview)

You can use the rule builder or rule syntax text box to create or edit a dynamic membership rule. ⓘ [Learn more](#)

And/Or	Property	Operator	Value	
	accountEnabled	Equals	true	
Or	usageLocation	Equals	US	

+ Add expression

+ Get custom extension properties ⓘ

Rule syntax

 Edit

```
(user.accountEnabled -eq true) or (user.usageLocation - eq "US")
```

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

Hot Area:

Answer Area

Statements	Yes	No
User1 is a member of Group1 and Group2.	<input type="radio"/>	<input type="radio"/>
User2 is a member of Group2 only.	<input type="radio"/>	<input type="radio"/>
Managed1 is a member of Group1 and Group2.	<input type="radio"/>	<input type="radio"/>

Answer:



## Answer Area

### Statements

Yes No

User1 is a member of Group1 and Group2.

☒☐

User2 is a member of Group2 only.

☐☒

Managed1 is a member of Group1 and Group2.

☐☒

### Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/groups-dynamic-membership>

### Question: 112

CertyIQ

You have a Microsoft 365 tenant that uses an Azure Active Directory (Azure AD) tenant. The Azure AD tenant syncs to an on-premises Active Directory domain by using an instance of Azure AD Connect.

You create a new Azure subscription.

You discover that the synced on-premises user accounts cannot be assigned roles in the new subscription.

You need to ensure that you can assign Azure and Microsoft 365 roles to the synced Azure AD user accounts.

What should you do first?

- A. Configure the Azure AD tenant used by the new subscription to use pass-through authentication.
- B. Configure the Azure AD tenant used by the new subscription to use federated authentication.
- C. Change the Azure AD tenant used by the new subscription.
- D. Configure a second instance of Azure AD Connect.

**Answer: C**

### Explanation:

We need to assign the Subscription on the tenant

### Question: 113

CertyIQ

You have an Azure subscription that contains an app named App1. App1 has the app registration shown in the following table.

API	Permission	Type	Admin consent required	Status
Microsoft.Graph	User.Read	Delegated	No	None
Microsoft.Graph	Calendars.Read	Delegated	No	None

You need to ensure that App1 can read all user calendars and create appointments. The solution must use the principle of least privilege.

What should you do?

- A. Add a new Delegated API permission for Microsoft.Graph Calendars.ReadWrite.
- B. Add a new Application API permission for Microsoft.Graph Calendars.ReadWrite.
- C. Select Grant admin consent.

D.Add new Delegated API permission for Microsoft.Graph Calendars.ReadWrite.Shared.

**Answer: B**

**Explanation:**

Add a new Application API permission for Microsoft.Graph Calendars.ReadWrite.

### Question: 114

CertyIQ

HOTSPOT -

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

Name	Member of group	Multi-factor authentication (MFA) status
User1	Group1, Group2	Enabled
User2	Group1	Disabled

You create and enforce an Azure AD Identity Protection sign-in risk policy that has the following settings:

- Assignments: Include Group1, exclude Group2
- Conditions: Sign-in risk level: Low and above
- Access: Allow access, Require multi-factor authentication

You need to identify what occurs when the users sign in to Azure AD.

What should you identify for each user? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

#### Answer Area

When User1 signs in from an anonymous IP address,  
the user will:

Be blocked

Be prompted for MFA

Sign in by using a username and password only

When User2 signs in from an unfamiliar location,  
the user will:

Be blocked

Be prompted for MFA

Sign in by using a username and password only

**Answer:**

#### Answer Area

When User1 signs in from an anonymous IP address,  
the user will:

Be blocked

Be prompted for MFA

Sign in by using a username and password only

When User2 signs in from an unfamiliar location,  
the user will:

Be blocked

Be prompted for MFA

Sign in by using a username and password only

**Explanation:**

User1 - is excluded but user1 MFA is Enabled

Exclusion will take precedence. Ans: MFA will be prompted

User2 - is include and user meet the above threshold for sign-in risk level: low and above therefor user account will be blocked.

Note: If you target this policy to a user that hasn't registered for MFA. Their access will be blocked

Ans: Be blocked

Reference:

<http://www.rebeladmin.com/2018/09/step-step-guide-configure-risk-based-azure-conditional-access-policies/> <https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-policies> <https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks>

### Question: 115

CertyIQ

HOTSPOT -

You have an Azure subscription that contains an Azure SQL database named SQL1.

You plan to deploy a web app named App1.

You need to provide App1 with read and write access to SQL1. The solution must meet the following requirements:

- Provide App1 with access to SQL1 without storing a password.
- Use the principle of least privilege.
- Minimize administrative effort.

Which type of account should App1 use to access SQL1, and which database roles should you assign to App1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

#### Answer area

Account type:

	▼
Azure Active Directory User	
Managed identity	
Service Principal	

Roles:

	▼
db_datawriter only	
db_datareader and db_datawriter	
db_owner only	

Answer:

## Answer area

Account type:

	▼
Azure Active Directory User	
Managed identity	
Service Principal	

Roles:

	▼
db_datawriter only	
db_datareader and db_datawriter	
db_owner only	

### Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/app-service/tutorial-connect-msi-sql-database?tabs=windowsclient%2Cdotnet>

### Question: 116

CertyIQ

HOTSPOT -

You have an Azure Active Directory (Azure AD) tenant that contains two users named User1 and User2 and a registered app named App1.

You create an app-specific role named Role1.

You need to assign Role1 to User1 and enable User2 to request access to App1.

Which two settings should you modify? To answer, select the appropriate settings in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

# Answer Area



## App1 | Overview



Enterprise Application



Overview



Deployment Plan

### Manage



Properties



Owners



Roles and administrators (Preview)



Users and groups



Single sign-on



Provisioning



Application proxy



Self-service

### Security



Conditional Access



Permissions



Token encryption


### Activity

Answer:

## Answer Area

### App1 | Overview ... Enterprise Application



 Overview


 Deployment Plan


#### Manage

 Properties

 Owners

 Roles and administrators (Preview)

 Users and groups

 Single sign-on

 Provisioning

 Application proxy

 Self-service

#### Security

 Conditional Access

#### Explanation:

Box 1:users and groups.

Box 2: Self Service .

#### Question: 117

CertyIQ

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



Name	Type
storage1	Storage account
Vault1	Azure Key vault
Vault2	Azure Key vault

You plan to deploy the virtual machines shown in the following table.

Name	Role
VM1	<ul style="list-style-type: none"> <li>Storage Blob Data Reader for storage1</li> <li>Key Vault Reader for Vault1</li> </ul>
VM2	<ul style="list-style-type: none"> <li>Storage Blob Data Reader for storage1</li> <li>Key Vault Reader for Vault1</li> </ul>
VM3	<ul style="list-style-type: none"> <li>Storage Blob Data Reader for storage1</li> <li>Key Vault Reader for Vault1</li> <li>Key Vault Reader for Vault2</li> </ul>
VM4	<ul style="list-style-type: none"> <li>Storage Blob Data Reader for storage1</li> <li>Key Vault Reader for Vault1</li> <li>Key Vault Reader for Vault2</li> </ul>

You need to assign managed identities to the virtual machines. The solution must meet the following requirements:

- Assign each virtual machine the required roles.
- Use the principle of least privilege.

What is the minimum number of managed identities required?

- A. 1
- B. 2
- C. 3
- D. 4

**Answer: B**

**Explanation:**

We have two different sets of required permissions. VM1 and VM2 have the same permission requirements. VM3 and VM4 have the same permission requirements.

A user-assigned managed identity can be assigned to one or many resources. By using user-assigned managed identities, we can create just two managed identities: one with the permission requirements for VM1 and VM2 and the other with the permission requirements for VM3 and VM4.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/overview>

### Question: 118

CertyIQ

#### SIMULATION -

You need to ensure that a user named user2-12345678 can manage the properties of the virtual machines in the RG1lod12345678 resource group. The solution must use the principle of least privilege. To complete this task, sign in to the Azure portal.

#### Answer:

See the explanation below.

#### Explanation:

1. Sign in to the Azure portal.
2. Browse to Resource Groups.
3. Select the RG1lod12345678 resource group.
4. Select Access control (IAM).
5. Select Add > role assignment.
6. Select Virtual Machine Contributor (you can filter the list of available roles by typing 'virtual' in the search box) then click Next.
7. Select the +Select members option and select user2-12345678 then click the Select button.
8. Click the Review + assign button twice.

#### Reference:

<https://docs.microsoft.com/en-us/azure/role-based-access-control/role-assignments-portal?tabs=current>

### Question: 119

CertyIQ

#### SIMULATION -

You need to create a new Azure Active Directory (Azure AD) directory named 12345678.onmicrosoft.com. The new directory must contain a new user named [email protected] To complete this task, sign in to the Azure portal.

#### Answer:

See the explanation below.

#### Explanation:

The first step is to create the Azure Active Directory tenant.

1. Sign in to the Azure portal.
2. From the Azure portal menu, select Azure Active Directory.
3. On the overview page, select Manage tenants.
4. Select +Create.
5. On the Basics tab, select Azure Active Directory.
6. Select Next: Configuration to move on to the Configuration tab.
7. For Organization name, enter 12345678.
8. For the Initial domain name, enter 12345678.
9. Leave the Country/Region as the default.

The next step is to create the user.

1. From the Azure portal menu, select Azure Active Directory.
2. Select Users then select New user.
3. Enter User1 in the User name and Name fields.
4. Leave the default option of Auto-generate password.
5. Click the Create button.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-access-create-new-tenant> <https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/add-users-azure-active-directory>

## Question: 120

CertyIQ

HOTSPOT -

You have an Azure subscription that contains a resource group named RG1. RG1 contains a storage account named storage1.

You have two custom Azure roles named Role1 and Role2 that are scoped to RG1.

The permissions for Role1 are shown in the following JSON code.

```
"permissions": [
  {
    "actions": [
      "Microsoft.Storage/storageAccounts/listKeys/action",
      "Microsoft.Storage/storageAccounts/ListAccountSas/action",
      "Microsoft.Storage/storageAccounts/read"
    ],
    "notActions": [],
    "dataActions": [],
    "notDataActions": []
  }
]
```

The permissions for Role2 are shown in the following JSON code.

```
"permissions": [
  {
    "actions": [
      "Microsoft.Authorization/*/read",
      "Microsoft.Insights/alertRules/*",
      "Microsoft.Insights/diagnosticSettings/*",
      "Microsoft.Network/virtualNetworks/subnets/joinViaServiceEndpoint/action",
      "Microsoft.ResourceHealth/availabilityStatuses/read",
      "Microsoft.Resources/deployments/*",
      "Microsoft.Resources/subscriptions/resourceGroups/read",
      "Microsoft.Storage/storageAccounts/*",
      "Microsoft.Support/*"
    ],
    "notActions": [],
    "dataActions": [],
    "notDataActions": []
  }
]
```

You assign the roles to the users shown in the following table.

Name	Role
User1	Role1
User2	Role2
User3	Role1, Role2

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

NOTE: Each correct selection is worth one point.

Hot Area:

## Answer Area

Statements	Yes	No
User1 can read data in storage1.	<input type="radio"/>	<input type="radio"/>
User2 can read data in storage1.	<input type="radio"/>	<input type="radio"/>
User3 can restore storage1 from a backup in Azure Backup.	<input type="radio"/>	<input type="radio"/>

Answer:

## Answer Area

Statements	Yes	No
User1 can read data in storage1.	<input type="radio"/>	<input checked="" type="radio"/>
User2 can read data in storage1.	<input checked="" type="radio"/>	<input type="radio"/>
User3 can restore storage1 from a backup in Azure Backup.	<input type="radio"/>	<input checked="" type="radio"/>

Explanation:

No

Yes

No

You have an Azure subscription that contains a storage account named storage1 and two web apps named app1 and app2.

Both apps will write data to storage1.

You need to ensure that each app can read only the data that it has written.

What should you do?

- A. Provide each app with a system-assigned identity and configure storage1 to use Azure AD User account authentication.
- B. Provide each app with a separate Storage account key and configure the app to send the key with each request.
- C. Provide each app with a user-managed identity and configure storage1 to use Azure AD User account authentication.
- D. Provide each app with a unique Base64-encoded AES-256 encryption key and configure the app to send the key with each request.

**Answer: D**

**Explanation:**

<https://docs.microsoft.com/en-us/azure/storage/blobs/encryption-scope-overview>

"Encryption scopes enable you to manage encryption with a key that is scoped to a container or an individual blob. You can use encryption scopes to create secure boundaries between data that resides in the same storage account but belongs to different customers."

### Question: 122

CertyIQ

You have an Azure subscription that contains an Azure Files share named share1 and a user named User1. Identity-based authentication is configured for share1.

User1 attempts to access share1 from a Windows 10 device by using SMB.

Which type of token will Azure Files use to authorize the request?

- A. OAuth 2.0
- B. JSON Web Token (JWT)
- C. SAML
- D. Kerberos

**Answer: D**

**Explanation:**

Azure Files supports identity-based authentication over Server Message Block (SMB) through two types of Domain Services: on-premises Active Directory Domain

Services (AD DS) and Azure Active Directory Domain Services (Azure AD DS).

Supported scenarios and restrictions include:

Supports Kerberos authentication with AD with AES 256 encryption (recommended) and RC4-HMAC.

Note: Kerberos is an authentication protocol that is used to verify the identity of a user or host.

Reference:

<https://docs.microsoft.com/en-us/azure/storage/files/storage-files-identity-auth-active-directory-enable>

### Question: 123

CertyIQ

DRAG DROP

-

You have an Azure subscription.

You plan to create two custom roles named Role1 and Role2.

The custom roles will be used to perform the following tasks:

- Members of Role1 will manage application security groups.
- Members of Role2 will manage Azure Bastion.

You need to add permissions to the custom roles.

Which resource provider should you use for each role? To answer, drag the appropriate resource providers to the correct roles. Each resource provider may be used, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

## Answer Area

Microsoft.Compute

Microsoft.Network

Role1:

Microsoft.Security

Role2:

Microsoft.Solutions

Answer:

## Answer Area

Role1: Microsoft.Network

Role2: Microsoft.Network

Explanation:

Microsoft.Network, Microsoft.Network

<https://learn.microsoft.com/en-us/azure/templates/microsoft.network/bastionhosts>

[https://learn.microsoft.com/en-us/rest/api/virtualnetwork/application-security-groups/create-or-update?  
tabs=HTTP](https://learn.microsoft.com/en-us/rest/api/virtualnetwork/application-security-groups/create-or-update?tabs=HTTP)



**Question: 124**

You have an Azure subscription linked to an Azure Active Directory Premium Plan 1 tenant.

You plan to implement Azure Active Directory (Azure AD) Identity Protection.

You need to ensure that you can configure a user risk policy and a sign-in risk policy.

What should you do first?

- A. Purchase Azure Active Directory Premium Plan 2 licenses for all users.
- B. Register all users for Azure Multi-Factor Authentication (MFA).
- C. Enable security defaults for Azure Active Directory.
- D. Enable enhanced security features in Microsoft Defender for Cloud.

**Answer: A**

**Explanation:**

- A. Purchase Azure Active Directory Premium Plan 2 licenses for all users.

**Question: 125**

HOTSPOT

-

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

Name	Type
RG1	Resource group
VM1	Virtual machine

You perform the following tasks:

- Create a managed identity named Managed1.
- Create a Microsoft 365 group named Group1.
- Register an enterprise application named App1.
- Enable a system-assigned managed identity for VM1.

You need to identify which service principals were created and which identities can be assigned the Reader role for RG1.

What should you identify? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

## Answer Area

Service Principles:

▼

App1 only  
Managed1 and VM1 only  
Managed1, VM1, and App1 only  
Managed1, VM1, App1, and Group1

Identities:

▼

App1 only  
Managed1 and VM1 only  
Managed1, VM1, and App1 only  
Managed1, VM1, App1, and Group1

Answer:

### Answer Area

Service Principles:

▼

App1 only  
Managed1 and VM1 only  
Managed1, VM1, and App1 only  
Managed1, VM1, App1, and Group1

Identities:

▼

App1 only  
Managed1 and VM1 only  
Managed1, VM1, and App1 only  
Managed1, VM1, App1, and Group1

Explanation:

Service Principals: Managed1, VM1, and App1 only

Identities: Managed1, VM1, App1, and Group1

You have an Azure Active directory tenant that syncs with an Active Directory Domain Services (AD DS) domain.

You plan to create an Azure file share that will contain folders and files.

Which identity store can you use to assign permissions to the Azure file share and folders within the share? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

## Answer Area

Azure file share:

▼

AD DS only  
Azure AD only  
AD DS and Azure AD

Folders in the file share:

▼

AD DS only  
Azure AD only  
AD DS and Azure AD

Answer:

### Answer Area

Azure file share:

▼

AD DS only  
Azure AD only  
AD DS and Azure AD

Folders in the file share:

▼

AD DS only  
Azure AD only  
AD DS and Azure AD

**Explanation:**

box1: AD DS only

The selected Azure AD identity must be a hybrid identity and cannot be a cloud only identity. This means that the same identity is also represented in AD DS. <https://learn.microsoft.com/en-us/azure/storage/files/storage-files-identity-ad-ds-assign-permissions?tabs=azureportal>

Box 2: AD DS only

### Question: 127

CertyIQ

You have an Azure subscription.

You plan to deploy a new Conditional Access policy named CAPolicy1.

You need to use the What if tool to evaluate how CAPolicy1 will affect users. The solution must minimize the impact of CAPolicy1 on the users.

To what should you set the Enable policy setting for CAPolicy1?

- A. Off
- B. On
- C. Report only

**Answer: C**

**Explanation:**

By setting the "Enable policy" setting to "Report only" for CAPolicy1, the policy will not be enforced, but it will still generate reports on how it would have affected users if it were enforced. This will allow you to evaluate the impact of the policy on users and make any necessary adjustments before enabling it.

### Question: 128

CertyIQ

You have an Azure Active Directory (Azure AD) tenant that contains 500 users and an administrative unit named AU1.

From the Azure Active Directory admin center, you plan to add the users to AU1 by using Bulk add members.

You need to create and upload a file for the bulk add.

What should you include in the file?

- A. only the display name of each user
- B. only the user principal name (UPN) of each user
- C. only the user principal name (UPN) and display name of each user
- D. only the user principal name (UPN) and object identifier of each user
- E. only the object identifier of each user

**Answer: B**

**Explanation:**

When adding users to an administrative unit using the Bulk add members feature, the file should contain only the user principal names (UPNs) of the users. The UPN is the unique identifier for each user in Azure AD and is typically in the format of an email address (e.g. [email protected]). By including only the UPN in the file, you can ensure that the correct users are added to the administrative unit.

**Question: 129**

HOTSPOT

-

You have the role assignments shown in the following exhibit.

```
[
  {
    "RoleAssignmentId": "13ae6e22-b93a-412f-9dc5-fc82b1726bde",
    "Scope": "/subscriptions/0a1baf97-0be4-424a-92fa-873c5a45fbbc/resourceGroups/RG1",
    "DisplayName": "Admin1",
    "SignInName": "Admin1@contoso.com",
    "RoleDefinitionName": "Owner",
    "RoleDefinitionId": "/subscriptions/0a1baf97-0be4-424a-92fa-873c5a45fbbc/providers/Microsoft.Authorization/roleDefinitions/8e3af657-a8ff-443c-a75c-2fe8c4bcb635",
    "ObjectId": "8e951033-c8a5-4da0-81dd-014ed03affbf",
    "ObjectType": "User",
    "RoleAssignmentDescription": "",
    "ConditionVersion": "",
    "Condition": ""
  },
  {
    "RoleAssignmentId": "b194df76-9432-4396-4783-0fec78996708",
    "Scope": "/providers/Microsoft.Management/managementGroups/80a7e2e3-0283-40b8-9271-4c3403fdf12d",
    "DisplayName": "Admin4",
    "SignInName": "Admin4@contoso.com",
    "RoleDefinitionName": "Security Reader",
    "RoleDefinitionId": "/subscriptions/0a1baf97-0be4-424a-92fa-873c5a45fbbc/providers/Microsoft.Authorization/roleDefinitions/39bc4728-0917-49c7-9d2c-d95423bc2eb4",
    "ObjectId": "232790da-a072-4a74-854f-11ce8e48a0ca",
    "ObjectType": "User",
    "RoleAssignmentDescription": "",
    "ConditionVersion": "",
    "Condition": ""
  }
]
```

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

NOTE: Each correct selection is worth one point.

[answer choice] can delete VM1.

Only Admin1  
Only Admin1 and Admin2  
Only Admin1 and Admin3  
Only Admin1 and Admin4  
Admin1, Admin2, Admin3, and Admin4

[answer choice] can create new resource groups.

Admin1 only  
Admin2 only  
Admin3 only  
Admin1 and Admin3 only  
Admin1, Admin2, Admin3, and Admin4

**Answer:**

[answer choice] can delete VM1.

Only Admin1  
Only Admin1 and Admin2  
Only Admin1 and Admin3  
Only Admin1 and Admin4  
Admin1, Admin2, Admin3, and Admin4

[answer choice] can create new resource groups.

Admin1 only  
Admin2 only  
Admin3 only  
Admin1 and Admin3 only  
Admin1, Admin2, Admin3, and Admin4

### Question: 130

CertyIQ

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

You need to ensure that User1 can create managed identities. The solution must use the principle of least privilege.

What should you do?

- A. Create a management group and assign User1 the Hybrid Identity Administrator Azure Active Directory (Azure AD) role.
- B. Create a management group and assign User1 the Managed Identity Operator role.
- C. Create a resource group and assign User1 to the Managed Identity Contributor role.
- D. Create an organizational unit (OU) and assign User1 the User administrator Azure Active Directory (Azure AD) role.

**Answer: C**

**Explanation:**

A - Wrong - Hybrid Identity Admin cannot create managed identities. Permissions are: Can manage AD to Azure AD cloud provisioning, Azure AD Connect, Pass-through Authentication (PTA), Password hash synchronization (PHS), Seamless Single sign-on (Seamless SSO), and federation settings.



B - wrong - Managed Identity Operator cannot create managed identities. Permissions are: Read and Assign User Assigned Identity

C - correct: Managed Identity Contributor can Create, Read, Update, and Delete User Assigned Identity.

D - incorrect - can create users, but does not follow the principal of least privilege, as the permission set is comprehensive. User administrator can manage all aspects of users and groups.

<https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference>

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

### Question: 131

CertyIQ

HOTSPOT

-

You have an Azure subscription that contains a resource group named RG1. RG1 contains a virtual machine named VM1 that uses Azure Active Directory (Azure AD) authentication.

You have two custom Azure roles named Role1 and Role2 that are scoped to RG1.

The permissions for Role1 are shown in the following JSON code.

```
"permissions": [
  {
    "actions": [
      "Microsoft.Compute/virtualMachines/*"
    ],
    "notActions": [
      "Microsoft.Compute/virtualMachines/delete"
    ],
    "dataActions": [].
    "notDataActions": []
  }
]
```

The permissions for Role2 are shown in the following JSON code.

```
"permissions": [
  {
    "actions": [
      "Microsoft.Compute/virtualMachines/*"
    ],
    "notActions": [],
    "dataActions": [],
    "notDataActions": []
  }
]
```

You assign the roles to the users shown in the following table.

Name	Role
User1	Role1
User2	Role1, Role2
User3	Role1, Role2

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

NOTE: Each correct selection is worth one point.

## Answer Area

Statements	Yes	No
User1 can delete VM1.	<input type="radio"/>	<input type="radio"/>
User2 can delete VM1.	<input type="radio"/>	<input type="radio"/>
User3 can sign in to VM1 by using Azure AD credentials.	<input type="radio"/>	<input type="radio"/>

Answer:

## Answer Area

### Statements

Yes

No

User1 can delete VM1.

☐☒

User2 can delete VM1.

☒☐

User3 can sign in to VM1 by using Azure AD credentials.

☐☒

### Explanation:

Box1: User1 can delete VM1 - No

User1 only has Role1, and Roles has notActions of VM delete.

Box2: User2 can delete VM - Yes

User2 has both Role1 and Role2 assigned. Role2 gives User2 the ability to delete VM.

Box3: User3 can sign in to VM by using Azure AD credentials - No

To be able to sign in to VM by using Azure AD credentials, User3 needs to have either Virtual Machine Administrator Login or Virtual Machine User Login. Those logins have actions defined in the dataActions section. For example, Microsoft.Compute/virtualMachines/login/action provides Log in to a virtual machine as a regular user. In both Role1 and Role2, the dataActions is not defined.

Refs:

<https://learn.microsoft.com/en-us/azure/active-directory/devices/howto-vm-sign-in-azure-ad-windows>

<https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#virtual-machine-administrator-login>

### Question: 132

CertyIQ

DRAG DROP

-

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

Name	Type
VM1	Virtual machine
VM2	Virtual machine
st1	Storage account
Vault1	Azure Key Vault

You plan to perform the following actions:

- Deploy a new app named App1 that will require access to Vault1.
- Configure a shared identity for VM1 and VM2 to access st1.

You need to configure identities for each requirement. The solution must minimize administrative effort.

Which type of identity should you configure for each requirement? To answer, drag the appropriate identity types to the correct requirements. Each identity type may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

### Identity types

### Answer Area

Security group

System-assigned managed identity

User account

User-assigned managed identity

VM1 and VM2 access to st1:

App1 access to Vault1:

#### Answer:

### Identity types

### Answer Area

Security group

System-assigned managed identity

User account

User-assigned managed identity

VM1 and VM2 access to st1:

User-assigned managed identity

App1 access to Vault1:

System-assigned managed identity

#### Explanation:

Box1: VM1 and VM2 access to st1 - User-assigned managed identity

Requirement: Configure a shared identity for VM1 and VM2 to access st1

We have to create a User-assigned managed identity to be shared with VM1 and VM2

Box2: App1 access to Vault1 - System-assigned managed identity

### Question: 133

CertyIQ

You have an Azure AD tenant. The tenant contains users that are assigned Azure AD Premium P2 licenses.

You have a partner company that has a domain named fabrikam.com. The fabrikam.com domain contains a user named User1. User1 has an email address of [email protected]

You need to provide User1 with access to the resources in the tenant. The solution must meet the following requirements:

- User1 must be able to sign in by using the [email protected] credentials.

- You must be able to grant User1 access to the resources in the tenant.
- Administrative effort must be minimized.

What should you do?

- A. Create a user account for User1.
- B. To the tenant, add fabrikam.com as a custom domain.
- C. Create an invite for User1.
- D. Set Enable guest self-service sign up via user flows to Yes for the tenant.

**Answer: C**

**Explanation:**

You should create an invite for User1 to join your Azure AD tenant as a guest user. This will allow him to sign in with his existing credentials ([email protected]), and you can then grant him access to the resources in the tenant. This option also minimizes administrative effort as it is a simple process to invite a guest user.

#### Question: 134

CertyIQ

You have an Azure AD tenant that contains the identities shown in the following table.

Type	Amount
User	1,000
Microsoft 365 group	200
Mail-enabled security group	65
Security group	25

You plan to implement Azure AD Identity Protection.

What is the maximum number of user risk policies you can configure?

- A. 1
- B. 90
- C. 200
- D. 265
- E. 1000

**Answer: A**

**Explanation:**

You can only configure one user risk policy per tenant.

<https://janbakker.tech/microsoft-secure-score-series-11-turn-on-user-risk-policy/#:~:text=You%20can%20only%20configure%20one%20user%20risk%20policy%20per%20tenant.>

#### Question: 135

CertyIQ

You have an Azure subscription that contains a resource group named RG1 and the identities shown in the following table.

Name	Type	Azure AD roles can be assigned to the group
User1	User	<i>Not applicable</i>
Group1	Microsoft 365 group	Yes
Group2	Security group	No
Group3	Security group	Yes
Group4	Security group	Yes

You assign Group4 the Contributor role for RG1.

Which identities can you add to Group4 as members?

- A. User1 only
- B. User1 and Group3 only
- C. User1, Group1, and Group3 only
- D. User1, Group2, and Group3 only
- E. User1, Group1, Group2, and Group3

**Answer: A**

**Explanation:**

This exam question test about role-assignable group feature in Azure Active Directory.

Refer to Microsoft document on role-assignable group: “Group nesting is not supported. A group can't be added as a member of a role-assignable group.”

Reference

Create a role-assignable group in Azure Active Directory

<https://learn.microsoft.com/en-us/azure/active-directory/roles/groups-create-eligible>

Use Azure AD groups to manage role assignments

<https://learn.microsoft.com/en-us/azure/active-directory/roles/groups-concept>

### Question: 136

CertyIQ

HOTSPOT

-

You have an Azure subscription that contains a storage account named contoso2023.

You need to perform the following tasks:

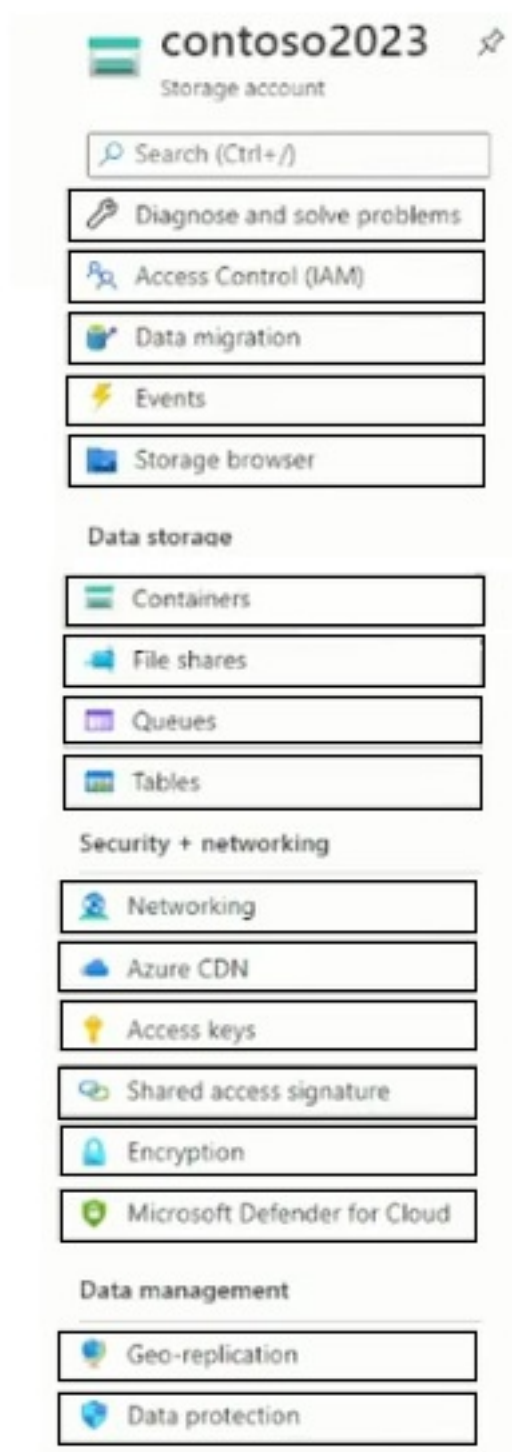
- Verify that identity-based authentication over SMB is enabled.
- Only grant users access to contoso2023 in the year 2023.

Which two settings should you use? To answer, select the appropriate settings in the answer area.

NOTE: Each correct selection is worth one point.

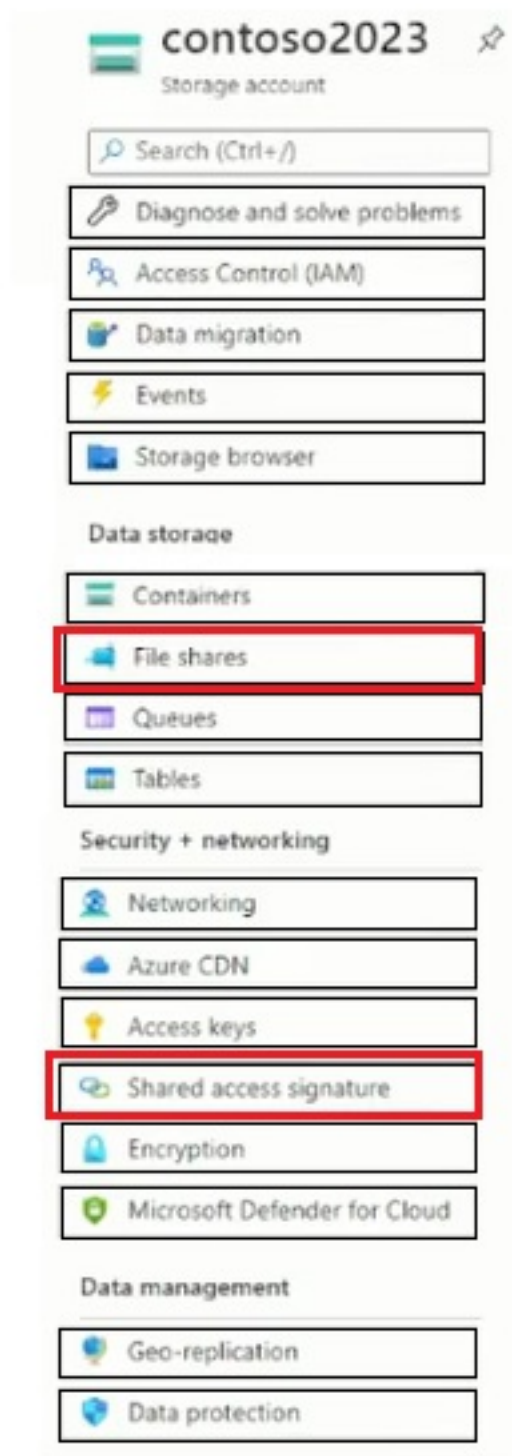


# Answer Area



Answer:

# Answer Area



## Explanation:

### 1. File Shares

Requirement: Verify that identity-based authentication over SMB is enabled

Go there to configure Identity-based authentication (Active Directory) for Azure file shares.

### 2. Share access signature

Requirement: Only grant users access to contoso2023 in the year 2023

Reference:

<https://learn.microsoft.com/en-us/azure/storage/files/storage-files-active-directory-overview>

**Question: 137****CertyIQ**

You have an Azure subscription that is linked to an Azure AD tenant and contains the resources shown in the following table.

Name	Location	Description
Group1	<i>Not applicable</i>	Dynamic device security group in Azure AD
Managed1	East US	Managed identity
VM1	West US	Virtual machine that has a system-assigned managed identity
VM2	Central US	Virtual machine
App1	<i>Not applicable</i>	Enterprise application in Azure AD

Which resources can be assigned the Contributor role for VM1?

- A.Managed1 and App1 only
- B.Group1 and Managed1 only
- C.Group1, Managed1, and VM2 only
- D.Group1, Managed1, VM1, and App1 only

**Answer: D****Explanation:**

Confirmed in my lab. I think VM1 in D should change to VM2 though.

**Question: 138****CertyIQ**

DRAG DROP

-

You have an Azure AD tenant that contains the users shown in the following table.

Name	User device
User1	Android mobile device with facial recognition
User2	Windows device with Windows Hello for Business-compatible hardware

You enable passwordless authentication for the tenant.

Which authentication method can each user use for passwordless authentication? To answer, drag the appropriate authentication methods to the correct users. Each authentication method may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Authentication methods

FIDO2 security key only

Microsoft Authenticator app only

Windows Hello for Business only

Microsoft Authenticator app and Windows Hello for Business only

Windows Hello for Business and FIDO2 security key only

Microsoft Authenticator app, Windows Hello for Business, and FIDO2 security key

Answer Area

User1:

Authentication method

User2:

Authentication method

Answer:

Answer Area

User1:

Microsoft Authenticator app only

User2:

Microsoft Authenticator app, Windows Hello for Business, and FIDO2 security key

Question: 139

DRAG DROP

You have an Azure AD tenant and an application named App1.

You need to ensure that App1 can use Microsoft Entra Verified ID to verify credentials.

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.

## Actions

## Answer Area

Configure the Verified ID service.

Register App1 in Azure AD and grant permissions.

Create an Azure key vault.

Configure an authentication methods policy.

Add an identity provider.



### Answer:

#### Answer Area

Create an Azure key vault.

Configure the Verified ID service.

Register App1 in Azure AD and grant permissions.

### Explanation:

<https://learn.microsoft.com/en-us/azure/active-directory/verifiable-credentials/verifiable-credentials-configure-tenant>

## Question: 140

CertyIQ

DRAG DROP

-

You have an Azure subscription that contains an Azure web app named App1.

You plan to configure a Conditional Access policy for App1. The solution must meet the following requirements:

- Only allow access to App1 from Windows devices.
- Only allow devices that are marked as compliant to access App1.

Which Conditional Access policy settings should you configure? To answer, drag the appropriate settings to the correct requirements. Each setting may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

## Policy settings

Cloud apps or actions

Conditions

Grant

Session

Users or workload identities

## Answer Area

Only allow access to App1 from  
Windows devices:

Policy setting

Only allow devices that are marked as  
compliant to access App1:

Policy setting

### Answer:

#### Policy settings

Cloud apps or actions

Conditions

Grant

Session

Users or workload identities

#### Answer Area

Only allow access to App1 from  
Windows devices:

Conditions

Only allow devices that are marked as  
compliant to access App1:

Grant

### Explanation:

Only allow access to App1 from Windows devices: Conditions  
Only allow devices that are marked as compliant to access App1: Grant

### Question: 141

CertyIQ

You have an Azure subscription that contains a web app named App1.

Users must be able to select between a Google identity or a Microsoft identity when authenticating to App1.

You need to add Google as an identity provider in Azure AD.

Which two pieces of information should you configure? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A.a client ID

B.a tenant name

C.the endpoint URL of an application



D.a tenant ID  
E.a client secret

**Answer: AE**

**Explanation:**

A.a client ID  
E.a client secret

### Question: 142

CertyIQ

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

You need to ensure that User1 can perform the following tasks:

- Create groups.
- Create access reviews for role-assignable groups.
- Assign Azure AD roles to groups.

The solution must use the principle of least privilege.

Which role should you assign to User1?

- A.Groups administrator
- B.Authentication administrator
- C.Identity Governance Administrator
- D.Privileged role administrator

**Answer: D**

**Explanation:**

D : Users with this role can manage role assignments in Azure Active Directory, as well as within Azure AD Privileged Identity Management. They can create and manage groups that can be assigned to Azure AD roles. In addition, this role allows management of all aspects of Privileged Identity Management and administrative units. Under Action you'll find

:microsoft.directory/accessReviews/definitions.groupsAssignableToRoles/create >>Create access reviews for membership in groups that are assignable to Azure AD roles

<https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#privileged-role-administrator>

### Question: 143

CertyIQ

SIMULATION

-

You need to ensure that a user named user2-28681041 can manage the properties of the virtual machines in the RG1lod28681041 resource group. The solution must use the principle of least privilege.

To complete this task, sign in to the Azure portal.

## Answer:

### RBAC role: Virtual Machine Contributor

Create and manage virtual machines, manage disks, install and run software, reset password of the root user of the virtual machine using VM extensions, and manage local user accounts using VM extensions. This role does not grant you management access to the virtual network or storage account the virtual machines are connected to. This role does not allow you to assign roles in Azure RBAC.

Grant a user access to Azure resources using the Azure portal

Azure role-based access control (Azure RBAC) is the way that you manage access to Azure resources.

Here you will grant a user access to create and manage virtual machines in a resource group.

### Grant access

In Azure RBAC, to grant access, you assign an Azure role.

Step 1: In the list of Resource groups, open the RG1lod28681041 resource group.

Step 2: In the navigation menu, click Access control (IAM).

Step 3: Click the Role assignments tab to see the current list of role assignments.

Home > Resource groups > example-group

example-group | Access control (IAM)

Search (Ctrl+/)

+ Add Download role assignments Edit columns Refresh Remove Got feedback?

Check access **Role assignments** Roles Roles (Classic) Deny assignments Classic administrators

Number of role assignments for this subscription 37 / 2000

Search by name or email... Type: All Role: All Scope: All scopes Group by: Role

22 items (11 Users, 4 Groups, 6 Service Principals, 1 Managed Identities)

Name	Type	Role	Scope	Condition
<b>Billing Reader</b>				
App2	App	Billing Reader	Subscription (Inherited)	None
user-assigned-identity	User Assigned Man...	Billing Reader	Subscription (Inherited)	None
Sales Admins	Group	Billing Reader	Subscription (Inherited)	None
<b>Contributor</b>				
azure-user	User	Contributor	Subscription (Inherited)	None

Step 4: Click Add > Add role assignment.

Step 5: On the Role tab, select the Virtual Machine Contributor role.

Home >

Add role assignment

Role Members Review + assign

A role definition is a collection of permissions. You can use the built-in roles or you can create your own custom roles. [Learn more](#)

Search by role name or description Type: All Category: All

Name	Description	Type	Category	Details
Owner	Grants full access to manage all resources, including the ability to a...	BuiltInRole	General	<a href="#">View</a>
Contributor	Grants full access to manage all resources, but does not allow you ...	BuiltInRole	General	<a href="#">View</a>
Reader	View all resources, but does not allow you to make any changes.	BuiltInRole	General	<a href="#">View</a>
AcrDelete	acr delete	BuiltInRole	Containers	<a href="#">View</a>
AcrImageSigner	acr image signer	BuiltInRole	Containers	<a href="#">View</a>
AcrPull	acr pull	BuiltInRole	Containers	<a href="#">View</a>
AcrPush	acr push	BuiltInRole	Containers	<a href="#">View</a>
AcrQuarantineReader	acr quarantine data reader	BuiltInRole	Containers	<a href="#">View</a>
AcrQuarantineWriter	acr quarantine data writer	BuiltInRole	Containers	<a href="#">View</a>

Review + assign

Previous

Next

Step 6: On the Members tab, select yourself or another user.

Step 7: On the Review + assign tab, review the role assignment settings.

Step 8: Click Review + assign to assign the role.

After a few moments, the user is assigned the Virtual Machine Contributor role at the RG1lod28681041 resource group scope.

+ Add Download role assignments Edit columns Refresh Remove Got feedback?

Check access **Role assignments** Roles Roles (Classic) Deny assignments Classic administrators


Number of role assignments for this subscription ⓘ

38 2000

Search by name or em... Type: All Role: Virtual Machine Contributor Scope: All scopes Group by: Role

Showing a filtered set of results. Total number of role assignments: 23

1 items (1 Users)

<input type="checkbox"/>	Name	Type	Role	Scope	Condition
<input type="checkbox"/>	Virtual Machine Contributor				
<input type="checkbox"/>	 AL Alain	User	Virtual Machine Contributor ⓘ	This resource	None

Reference:

<https://learn.microsoft.com/en-us/azure/role-based-access-control/quickstart-assign-role-user-portal>

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

## Question: 144

CertyIQ

### SIMULATION

You need to create a new Azure AD directory named 28681041.onmicrosoft.com. The new directory must contain a new user named [email protected].

To complete this task, sign in to the Azure portal.

### Answer:

Create Azure AD directory

To create a new tenant

Azure Active Directory - Overview page - Create a tenant

Step 1: Sign in to your organization's Azure portal.

Step 2: From the Azure portal menu, select Azure Active Directory.

Step 3: On the overview page, select Manage tenants

Step 4: Select Create.

Microsoft Azure Search resources, services, and docs (G+/)

Home > Fourth Coffee >

Switch tenant ...

+ Create Refresh Columns Switch Delete Leave tenant Make default tenant More information Got feedback?

Current tenant: Fourth Coffee

Search tenants Add filters

Showing 1 of 1 results

<input type="checkbox"/>	Organization name	Domain name	Tenant type	Organization ID	Favorite
<input type="checkbox"/>	Fourth Coffee (Default)	fourthcoffee.club	Azure Active Directory	340d0dd4-7adc-4196-b880-8b6f865aa6...	★

Step 5: On the Basics tab, select the type of tenant you want to create, either Azure Active Directory or Azure Active Directory (B2C).

Step 6: Select Next: Configuration to move on to the Configuration tab.

Step 7: On the Configuration tab, enter the following information:

Type your desired Organization name (for example Contoso Organization) into the Organization name box.

Type your desired Initial domain name (We use 28681041) into the Initial domain name box.

Select your desired Country/Region or leave the United States option in the Country or region box.

Step 8: Select Next: Review + Create. Review the information you entered and if the information is correct, select create.

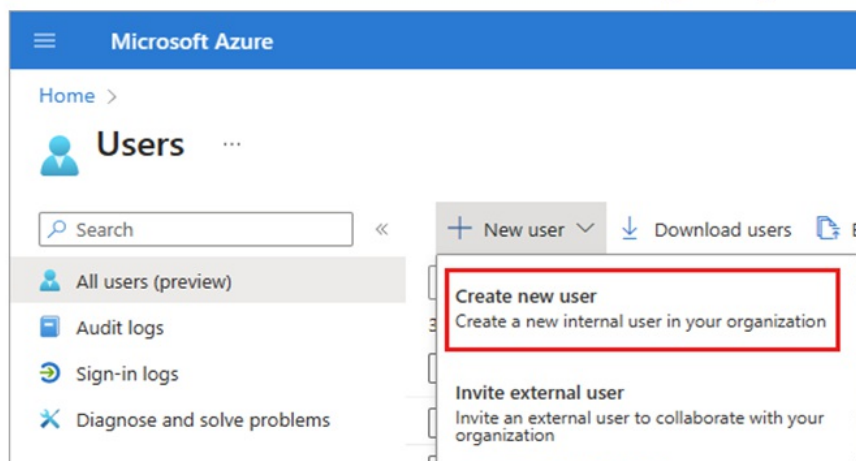
Step 9: Your new tenant is created with the domain 28681041.onmicrosoft.com.

Add new users or delete existing users from your Azure Active Directory (Azure AD) tenant.

Add a new user

You can create a new user for your organization or invite an external user from the same starting point.

1. Sign in to the Azure portal in the User Administrator role.
2. Navigate to Azure Active Directory > Users.
3. Select either Create new user or Invite external user from the menu. You can change this setting on the next screen.



4. On the New User page, provide the new user's information:

Identity: user1@28681041.onmicrosoft.com

\*Details omitted\*

5. Copy the autogenerated password provided in the Password box. You'll need to give this password to the user to sign in for the first time.

6. Select Create.

The user is created and added to your Azure AD organization.

Reference:

<https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-access-create-new-tenant>

<https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/add-users-azure-active-directory>

### Explanation:

In QUESTION[EMAILPROTECTED]=@28681041.onmicrosoft.com.

## Question: 145

CertyIQ

HOTSPOT

-

You have an Azure subscription that contains a user named Admin1 and an Azure key vault named Vault1.

You plan to implement Microsoft Entra Verified ID.

You need to create an access policy to ensure that Admin1 has permissions to Vault1 that support the implementation of the Verified ID service. The solution must use the principle of least privilege.

Which three key permissions should you select? To answer, select the appropriate permissions in the answer area.

NOTE: Each correct selection is worth one point.

## Answer Area

### Key permissions

#### Key Management Operations

☐ Select all

☐ Get

☐ List

☐ Update

☐ Create

☐ Import

☐ Delete



☐ Recover

☐ Backup

☐ Restore

---

### Cryptographic Operations

☐ Select all

---

☐ Decrypt

☐ Encrypt

☐ Unwrap Key

☐ Wrap Key

☐ Verify

☐ Sign

---

### Privileged Key Operations

☐ Select all

---

☐ Purge

☐ Release

---

### Rotation Policy Operations

☐ Select all

---

☐ Rotate

☐ Get Rotation Policy

☐ Set Rotation Policy

Answer:

**Answer Area**



## Key permissions

### Key Management Operations

☐ Select all

---

☐ Get

☐ List

☐ Update

☐ Create

☐ Import

☐ Delete

☐ Recover

☐ Backup

☐ Restore

---

### Cryptographic Operations

☐ Select all

---

☐ Decrypt

☐ Encrypt

☐ Unwrap Key

☐ Wrap Key

☐ Verify

☐ Sign

---

### Privileged Key Operations

☐ Select all

---

☐ Purge

☐ Release

---

### Rotation Policy Operations

☐ Select all

---

☐ Rotate

- ☐ Rotate
- ☐ Get Rotation Policy
- ☐ Set Rotation Policy

**Explanation:**



<https://learn.microsoft.com/en-us/azure/active-directory/verifiable-credentials/verifiable-credentials-configure-tenant>

**Question: 146**

CertyIQ

You have an Azure AD tenant that contains three users named User1, User2, and User3.

You configure Azure AD Password Protection as shown in the following exhibit.

 Save
  Discard

---

**Custom smart lockout**

Lockout threshold ⓘ

Lockout duration in seconds ⓘ

**Custom banned passwords**

Enforce custom list ⓘ Yes No

Custom banned password list ⓘ

Contoso ✓  
 Product  
 Fabrikam

**Password protection for Windows Server Active Directory**

Enable password protection on Windows Server Active Directory ⓘ Yes No

Mode ⓘ Enforced Audit

The users perform the following tasks:

- User1 attempts to reset her password to C0nt0s0.
- User2 attempts to reset her password to [email protected].
- User3 attempts to reset her password to Pr0duct123.

Which password reset attempts fail?

- A.User1 only
- B.User2 only
- C.User3 only
- D.User1 and User 3 only
- E.User1, User2, and User3

**Answer: E**

**Explanation:**

Confirmed in my lab, you'll get " Unfortunately, you can't use that password because it contains words or characters that have been blocked by your administrator. Please try again with a different password." when you select either of those password.

**Question: 147**

**CertyIQ**

You have an Azure subscription that uses Azure AD Privileged Identity Management (PIM).

A user named User1 is eligible for the Billing administrator role.

You need to ensure that the role can only be used for a maximum of two hours.

What should you do?

- A.Create a new access review.
- B.Edit the role assignment settings.
- C.Update the end date of the user assignment.
- D.Edit the role activation settings.

**Answer: D**

**Explanation:**

Role Activation settings<https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-change-default-settings#role-settings>

D. - Similar as xcapell <https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-change-default-settingshttps://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-change-default-settings>

**Question: 148**

**CertyIQ**

HOTSPOT

-

You have an Azure subscription that contains a user named User1 and a storage account named storage1. The storage1 account contains the resources shown in the following table.

Name	Type
container1	Container
folder1	File share
table1	Table

User1 is assigned the following roles for storage1:

- Storage Blob Data Reader
- Storage Table Data Contributor
- Storage File Data SMB Share Reader

In storage1, you create a shared access signature (SAS) named SAS1 as shown in the following exhibit.

Allowed services ⓘ
☐ Blob
☒ File
☐ Queue
☐ Table

Allowed resource types ⓘ
☒ Service
☒ Container
☒ Object

Allowed permissions ⓘ
☒ Read
☒ Write
☒ Delete
☒ List
☐ Add
☒ Create
☐ Update
☐ Process
☐ Immutable storage

Blob versioning permissions ⓘ
☐ Enables deletion of versions

Allowed blob index permissions ⓘ
☐ Read/Write
☐ Filter

Start and expiry date/time ⓘ

Start
01/01/2022
12:00:00 AM

End
01/01/2023
12:00:00 AM

(UTC+01:00) Belgrade, Bratislava, Budapest, Ljubljana, Prague

Allowed IP addresses ⓘ

For example, 168.1.5.65 or 168.1.5.65-168.1.5.70

Allowed protocols ⓘ
☒ HTTPS only
☐ HTTPS and HTTP

Preferred routing tier ⓘ
☒ Basic (default)
☐ Microsoft network routing
☐ Internet routing

Some routing options are disabled because the endpoints are not published.

Signing key ⓘ

key1

Generate SAS and connection string

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

## Answer Area

Statements	Yes	No
On October 1, 2022, if User1 accesses folder1 by using SAS1, he can delete the files in folder1.	<input type="radio"/>	<input type="radio"/>
On October 1, 2022, if User1 maps folder1 as a network drive by using his Azure AD credentials, he can delete the files in folder1.	<input type="radio"/>	<input type="radio"/>
On October 1, 2022, User1 can delete the rows in table1 by using SAS1.	<input type="radio"/>	<input type="radio"/>

Answer:

## Answer Area

Statements	Yes	No
On October 1, 2022, if User1 accesses folder1 by using SAS1, he can delete the files in folder1.	<input checked="" type="radio"/>	<input type="radio"/>
On October 1, 2022, if User1 maps folder1 as a network drive by using his Azure AD credentials, he can delete the files in folder1.	<input type="radio"/>	<input checked="" type="radio"/>
On October 1, 2022, User1 can delete the rows in table1 by using SAS1.	<input type="radio"/>	<input checked="" type="radio"/>

## Question: 149

CertyIQ

You have an Azure subscription that contains a user named User1 and a storage account that hosts a blob container named blob1.

You need to grant User1 access to blob1. The solution must ensure that the access expires after six days.

What should you use?

- A.a shared access signature (SAS)
- B.role-based access control (RBAC)
- C.a shared access policy
- D.a managed identity

Answer: A

Explanation:

answer is correct - SAS can specific expired date

## Question: 150

CertyIQ

You have an Azure subscription linked to an Azure AD tenant named contoso.com. Contoso.com contains a user named User1 and an Azure web app named App1.

You plan to enable User1 to perform the following tasks:

- Configure contoso.com to use Microsoft Entra Verified ID.
- Register App1 in contoso.com.

You need to identify which roles to assign to User1. The solution must use the principle of least privilege.

Which two roles should you identify? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A.Authentication Policy Administrator
- B.Authentication Administrator
- C.Cloud App Security Administrator
- D.Application Administrator
- E.User Administrator

**Answer: AD**

**Explanation:**

AD.

<https://learn.microsoft.com/en-us/azure/active-directory/verifiable-credentials/verifiable-credentials-configure-tenant>Ensure that you have the global administrator or the authentication policy administrator permission for the directory you want to configure. If you're not the global administrator, you need the application administrator permission to complete the app registration including granting admin consent.

### Question: 151

CertyIQ

You have an Azure AD tenant.

You plan to implement an authentication solution to meet the following requirements:

- Require number matching.
- Display the geographical location when signing in.

Which authentication method should you include in the solution?

- A.Microsoft Authenticator
- B.FIDO2 security key
- C.SMS
- D.Temporary Access Pass

**Answer: A**

**Explanation:**

A. Microsoft Authenticator

<https://learn.microsoft.com/en-us/azure/active-directory/authentication/how-to-mfa-additional-context>

### Question: 152

CertyIQ



Your network contains an on-premises Active Directory Domain Services (AD DS) domain that syncs with an Azure AD tenant.

You plan to implement single sign-on (SSO) for Azure AD resources.

You need to configure an Intranet Zone setting for all users by using a Group Policy Object (GPO).

Which setting should you configure?

- A.Logon options
- B.Allow updates to status bar via script
- C.Allow active scripting
- D.Access data sources across domains

**Answer: B**

**Explanation:**

Correct answer is B:Allow updates to status bar via script.

### Question: 153

CertyIQ

HOTSPOT

-

You have an Azure AD tenant that contains the groups shown in the following table.

Name	Type	Contains members
Group1	Security	Yes
Group2	Microsoft 365	No
Group3	Microsoft 365	Yes

You assign licenses to the groups as shown in the following table.

Group	License
Group1	Azure Active Directory Premium P2
Group2	Office 365 E5
Group3	Azure Active Directory Premium P2

On May1, you delete Group1, Group2, and Group3.

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

NOTE: Each correct selection is worth one point.

## Answer Area

Statements	Yes	No
On May 3, you can restore Group1.	<input type="radio"/>	<input type="radio"/>
On May 15, you can restore Group2.	<input type="radio"/>	<input type="radio"/>
On June 3, you can restore Group3.	<input type="radio"/>	<input type="radio"/>

Answer:

### Answer Area

Statements	Yes	No
On May 3, you can restore Group1.	<input type="radio"/>	<input checked="" type="radio"/>
On May 15, you can restore Group2.	<input checked="" type="radio"/>	<input type="radio"/>
On June 3, you can restore Group3.	<input type="radio"/>	<input checked="" type="radio"/>

Explanation:

No

Yes

No

### Question: 154

CertyIQ

You have an Azure AD tenant.

You need to ensure that users cannot create passwords containing a variation of the word contoso.

What should you configure?

- A.Microsoft Entra Verified ID
- B.Microsoft Entra Identity Governance
- C.Azure AD Privileged Identity Management (PIM)
- D.Azure AD Password Protection
- E.Azure AD Identity Protection

Answer: D

Explanation:

D is correct Azure AD Password Protection enables you to: Define custom password policies. Prevent the use of common words or patterns. Protect against various types of common attacks on passwords.

Question: 155

CertyIQ

HOTSPOT

-

You have a Microsoft Entra tenant that contains the users shown in the following table.

Name	Member of	Role
Admin1	Group1	Global Administrator
Admin2	Group1	Privileged Authentication Administrator
User1	None	None

You configure the Temporary Access Pass settings as shown in the following exhibit.

## Temporary Access Pass settings ... ×

Temporary Access Pass, or TAP, is a time-limited or limited-use passcode that can be used by users for bootstrapping new accounts, account recovery, or when other auth methods are unavailable.

[Learn more.](#)

TAP is issuable only by administrators, and is seen by the system as strong authentication. It is not usable for Self Service Password Reset.

**Enable and Target**    Configure

Enable ☒

**Include**    Exclude

Target ☐ All users ☒ Select groups

[Add groups](#)

Name	Type	Registration
Group1	Group	Optional <span>▼</span>

You add the Temporary Access Pass authentication method to Admin2.

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

NOTE: Each correct selection is worth one point.

Answer Area		
Statements	Yes	No
Admin1 can view the Temporary Access Pass of Admin2.	<input type="radio"/>	<input type="radio"/>
Admin2 can add the Temporary Access Pass authentication method to User1.	<input type="radio"/>	<input type="radio"/>
Admin2 can add the Temporary Access Pass authentication method to Admin1.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area		
Statements	Yes	No
Admin1 can view the Temporary Access Pass of Admin2.	<input checked="" type="radio"/>	<input type="radio"/>
Admin2 can add the Temporary Access Pass authentication method to User1.	<input type="radio"/>	<input checked="" type="radio"/>
Admin2 can add the Temporary Access Pass authentication method to Admin1.	<input checked="" type="radio"/>	<input type="radio"/>

Explanation:

Reference:

<https://learn.microsoft.com/en-us/entra/identity/authentication/howto-authentication-temporary-access-pass>

Question: 156

CertyIQ

HOTSPOT

-

Your network contains an on-premises Active Directory domain named adatum.com that syncs to a Microsoft Entra tenant.

The Microsoft Entra tenant contains the users shown in the following table.

Name	On-premises sync enabled	Password
User1	No	Adatum123
User2	No	N3w3rT0Gue33
User3	Yes	ComplexPassword33

You configure the Microsoft Entra Password Protection settings for adatum.com as shown in the following exhibit.

### Custom smart lockout

Lockout threshold ⓘ

10

Lockout duration in seconds ⓘ

60

### Custom banned passwords

Enforce custom list ⓘ

Yes

No

Custom banned password list ⓘ

Adatum

### Password protection for Windows Server Active Directory

Enable password protection on Windows Server Active Directory ⓘ

Yes

No

Mode ⓘ

Enforced

Audit

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

NOTE: Each correct selection is worth one point.

### Answer Area

Statements	Yes	No
User1 will be prompted to change the password on the next sign-in.	<input type="radio"/>	<input type="radio"/>
User2 can change the password to @d@tum_C0mpleX123.	<input type="radio"/>	<input type="radio"/>
User3 can change the password to Adatum123!.	<input type="radio"/>	<input type="radio"/>

Answer:

### Answer Area

Statements	Yes	No
User1 will be prompted to change the password on the next sign-in.	<input type="radio"/>	<input checked="" type="radio"/>
User2 can change the password to @d@tum_C0mpleX123.	<input type="radio"/>	<input checked="" type="radio"/>
User3 can change the password to Adatum123!.	<input checked="" type="radio"/>	<input type="radio"/>

Explanation:

No

No

Yes

**Question: 157**

**CertyIQ**

HOTSPOT

-

You have a Microsoft Entra tenant that contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Group2
User3	Group1, Group2

From Microsoft Entra Privileged Identity Management (PIM), you configure the settings for the Security Administrator role as shown in the following exhibit.



# Role setting details - Security Administrator

Privileged Identity Management | Azure AD roles

 Edit

## Activation

Setting	State
Activation maximum duration (hours)	5 hour(s)
On activation, require	None
Require justification on activation	No
Require ticket information on activation	No
Require approval to activate	No
Approvers	None

## Assignment

Setting	State
Allow permanent eligible assignment	Yes
Expire eligible assignments after	-
Allow permanent active assignment	Yes
Expire active assignments after	-
Require Azure Multi-Factor Authentication on active assignment	No
Require justification on active assignment	Yes

From PIM, you assign the Security Administrator role to the following groups:

- Group1: Active assignment type, permanently assigned
- Group2: Eligible assignment type, permanently eligible

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

NOTE: Each correct selection is worth one point.

### Answer Area

Statements	Yes	No
User1 has five hours to activate the Security Administrator role.	<input type="radio"/>	<input type="radio"/>
If User2 activates the Security Administrator role, the user will be assigned the role immediately.	<input type="radio"/>	<input type="radio"/>
User3 can activate the Security Administrator role.	<input type="radio"/>	<input type="radio"/>

Answer:

### Answer Area

Statements	Yes	No
User1 has five hours to activate the Security Administrator role.	<input type="radio"/>	<input checked="" type="radio"/>
If User2 activates the Security Administrator role, the user will be assigned the role immediately.	<input checked="" type="radio"/>	<input type="radio"/>
User3 can activate the Security Administrator role.	<input type="radio"/>	<input checked="" type="radio"/>

### Question: 158

CertyIQ

DRAG DROP

-

You have an Azure subscription that contains an Azure web app named App1.

You plan to configure a Conditional Access policy for App1. The solution must meet the following requirements:

- Only allow access to App1 from Windows devices.
- Only allow devices that are marked as compliant to access App1.

Which Conditional Access policy settings should you configure? To answer, drag the appropriate settings to the correct requirements. Each setting may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

## Policy settings

Target resources

Conditions

Grant

Session

Users or workload identities

## Answer Area

Only allow access to App1 from  
Windows devices:

Policy setting

Only allow devices that are marked as  
compliant to access App1:

Policy setting

### Answer:

#### Policy settings

Target resources

Conditions

Grant

Session

Users or workload identities

#### Answer Area

Only allow access to App1 from  
Windows devices:

Conditions

Only allow devices that are marked as  
compliant to access App1:

Grant

### Explanation:

Conditions.

Grant.

## Question: 159

CertyIQ

HOTSPOT

-

Your network contains an on-premises Active Directory domain that syncs to a Microsoft Entra tenant. The tenant contains the users shown in the following table.

Name	On-premises sync enabled
User1	No
User2	No
User3	Yes

The tenant contains the groups shown in the following table.

Name	Members
Group1	User1, User2, User3
Group2	User2

You configure a multi-factor authentication (MFA) registration policy that has the following settings:

- Assignments:
  - oInclude: Group1
  - oExclude: Group2
- Controls: Require Azure MFA registration
- Enforce Policy: On

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

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
User1 will be prompted to configure MFA registration during the user's next Microsoft Entra authentication.	<input type="radio"/>	<input type="radio"/>
User2 must configure MFA during the user's next Microsoft Entra authentication.	<input type="radio"/>	<input type="radio"/>
User3 will be prompted to configure MFA registration during the user's next Microsoft Entra authentication.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
User1 will be prompted to configure MFA registration during the user's next Microsoft Entra authentication.	<input checked="" type="radio"/>	<input type="radio"/>
User2 must configure MFA during the user's next Microsoft Entra authentication.	<input type="radio"/>	<input checked="" type="radio"/>
User3 will be prompted to configure MFA registration during the user's next Microsoft Entra authentication.	<input checked="" type="radio"/>	<input type="radio"/>

Explanation:

Yes

No

Yes

Question: 160

You have a Microsoft Entra tenant named contoso.com.

You plan to collaborate with a partner organization that has a Microsoft Entra tenant named fabrikam.com.

Fabrikam.com uses the following identity providers:

- Google Cloud Platform (GCP)
- Microsoft accounts
- Microsoft Entra ID

You need to configure the Cross-tenant access settings for B2B collaboration.

Which identity providers support cross-tenant access?

- A.Microsoft Entra ID only
- B.GCP and Microsoft Entra ID only
- C.Microsoft accounts and Microsoft Entra ID only
- D.GCP, Microsoft accounts, and Microsoft Entra ID

**Answer: D**

**Explanation:**

GCP, Microsoft accounts, and Microsoft Entra ID.

### Question: 161

CertyIQ

You have a Microsoft Entra tenant named contoso.com.

You have a partner company that has a Microsoft Entra tenant named fabrikam.com.

You need to ensure that when a user in fabrikam.com attempts to access the resources in contoso.com, the user only receives a single Microsoft Entra Multi-Factor Authentication (MFA) prompt. The solution must minimize administrative effort.

What should you do?

- A.From the Azure portal of contoso.com, configure the inbound access default settings.
- B.From the Azure portal of contoso.com, configure the External collaboration settings.
- C.From the Azure portal of contoso.com, configure the outbound access default settings.
- D.From the Azure portal of fabrikam.com, configure the outbound access default settings.

**Answer: A**

**Explanation:**

From the Azure portal of contoso.com, configure the inbound access default settings.

### Question: 162

CertyIQ

HOTSPOT

-

You have a Microsoft Entra tenant that contains the groups shown in the following table.

Name	Type
Group1	Security
Group2	Mail-enabled Security
Group3	Microsoft 365

From the Azure portal, you configure a group expiration policy that has a lifetime of 180 days.

Which groups will be deleted after 180 days of inactivity, and what is the maximum amount of time you have to restore a deleted group? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

### Answer Area

Groups that will be deleted:

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

Maximum amount of time to restore a deleted group:

1 day  
15 days  
30 days  
180 days

Answer:

### Answer Area

Groups that will be deleted:

Group1 only  
Group2 only  
**Group3 only**  
Group1 and Group2 only  
Group2 and Group3 only  
Group1, Group2, and Group3

Maximum amount of time to restore a deleted group:

1 day  
15 days  
**30 days**  
180 days



**Question: 163****CertyIQ**

You have a Microsoft Entra tenant that uses Microsoft Entra Permissions Management and contains the accounts shown in the following table:

Name	Role
Admin1	Global Administrator
Admin2	Privileged Role Administrator
Admin3	Privileged Authentication Administrator
Admin4	Exchange Administrator

Which accounts will be listed as assigned to highly privileged roles on the Azure AD insights tab in the Entra Permissions Management portal?

- A.Admin1 only
- B.Admin2 and Admin3 only
- C.Admin2 and Admin4 only
- D.Admin1, Admin2, and Admin3 only
- E.Admin2, Admin3, and Admin4 only
- F.Admin1, Admin2, Admin3, and Admin4

**Answer: C****Explanation:**

Admin2 and Admin4 only.

**Question: 164****CertyIQ**

HOTSPOT

-

You have a Microsoft Entra tenant that contains the user shown in the following table.

Name	Member of
User1	Group1
User2	Group1, Group2
User3	Group2

You configure a Conditional Access policy that has the following settings:

- Name:CAPolicy1
- Assignments
  - oUsers or workload identities: Group1
  - oTarget resources: All cloud apps
- Access controls
  - oGrant access: Require multifactor authentication

From Microsoft Authenticator settings for the tenant, the Enable and Target settings are configured as shown in the Enable and Target exhibit. (Click the Enable and Target tab.)

## Enable and Target

## Configure

Enable



Include

Exclude

Target



All users



Select groups

[Add groups](#)

Name

Type

Registration

Authentication mode

Group1

Group

Optional



Passwordless



From Microsoft Authenticator settings for the tenant, the Configure settings are configured as shown in the Configure exhibit. (Click the Configure tab.)

## Enable and Target

## Configure

Note: Users must be included as part of the Microsoft Authenticator targeted groups under the 'Enable and Target' tab.

### GENERAL

Allow use of Microsoft Authenticator OTP

Yes

No

### Require number matching for push notifications

Note: If the feature status is set to Microsoft-managed, it will be enabled by Microsoft at an appropriate time after the preview.

Status

Enabled



Target

Include

Exclude



All users



Select group

[Add selected group](#)

Include target

Group2



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

NOTE: Each correct selection is worth one point.

## Answer Area

Statements	Yes	No
User1 is required to use number matching during sign-in.	<input type="radio"/>	<input type="radio"/>
User2 is required to use number matching during sign-in.	<input type="radio"/>	<input type="radio"/>
User3 is required to use number matching during sign-in.	<input type="radio"/>	<input type="radio"/>

Answer:

### Answer Area

Statements	Yes	No
User1 is required to use number matching during sign-in.	<input type="radio"/>	<input checked="" type="radio"/>
User2 is required to use number matching during sign-in.	<input checked="" type="radio"/>	<input type="radio"/>
User3 is required to use number matching during sign-in.	<input type="radio"/>	<input checked="" type="radio"/>

Explanation:

No

Yes

No

#### Question: 165

CertyIQ

You have a Microsoft Entra tenant that contains three users named User1, User2, and User3.

You configure Microsoft Entra Password Protection as shown in the following exhibit.

### Custom smart lockout

Lockout threshold ⓘ

10

Lockout duration in seconds ⓘ

60

### Custom banned passwords

Enforce custom list ⓘ

Yes

No

Custom banned password list ⓘ

Contoso  
Product  
Fabrikam



### Password protection for Windows Server Active Directory

Enable password protection on Windows Server Active Directory ⓘ

Yes

No

Mode ⓘ

Enforced

Audit

The users perform the following tasks:

- User1 attempts to reset her password to C0nt0s0.
- User2 attempts to reset her password to F@brikamHQ.
- User3 attempts to reset her password to Pr0duct123.

Which password reset attempts fail?

- A.User1 only
- B.User2 only
- C.User3 only
- D.User1 and User 3 only
- E.User1, User2, and User3

**Answer: E**

**Explanation:**

User1, User2, and User3.

### Question: 166

CertyIQ

You have an Azure subscription that contains a user named User1 and an Azure Container Registry named ContReg1.

You enable content trust for ContReg1.

You need to ensure that User1 can create trusted images in ContReg1. The solution must use the principle of least

privilege.

Which two roles should you assign to User1? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. AcrQuarantineReader
- B. Contributor
- C. AcrPush
- D. AcrImageSigner
- E. AcrQuarantineWriter

**Answer: CD**

**Explanation:**

AcrPush

AcrImageSigner

Reference:

<https://docs.microsoft.com/en-us/azure/container-registry/container-registry-content-trust>

<https://docs.microsoft.com/en-us/azure/container-registry/container-registry-roles>

### Question: 167

CertyIQ

You have an Azure Container Registry named ContReg1 that contains a container image named image1.

You enable content trust for ContReg1.

After content trust is enabled, you push two images to ContReg1 as shown in the following table.

Name	Details
image2	Image was pushed with client content trust enabled.
image3	Image was pushed with client content trust disabled.

Which images are trusted images?

- A. image1 and image2 only
- B. image2 only
- C. image1, image2, and image3

**Answer: B**

**Explanation:**

Azure Container Registry implements Docker's content trust model, enabling pushing and pulling of signed images.

To push a trusted image tag to your container registry, enable content trust and push the image with docker push.

To work with trusted images, both image publishers and consumers need to enable content trust for their Docker clients. As a publisher, you can sign the images you push to a content trust-enabled registry.

Reference:

<https://docs.microsoft.com/en-us/azure/container-registry/container-registry-content-trust>

## Question: 168

### SIMULATION -

You need to configure Azure to allow RDP connections from the Internet to a virtual machine named VM1. The solution must minimize the attack surface of VM1.

To complete this task, sign in to the Azure portal.

#### Answer:

See the explanation below.

#### Explanation:

To enable the RDP port in an NSG, follow these steps:

1. Sign in to the Azure portal.
2. In Virtual Machines, select VM1
3. In Settings, select Networking.
4. In Inbound port rules, check whether the port for RDP is set correctly. The following is an example of the configuration:

Priority: 300 -

Name: Port\_3389 -

Port(Destination): 3389 -

Protocol: TCP -

Source: Any -

Destinations: Any -

Action: Allow -

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-machines/troubleshooting/troubleshoot-rdp-nsg-problem>

## Question: 169

### SIMULATION -

You need to add the network interface of a virtual machine named VM1 to an application security group named ASG1.

To complete this task, sign in to the Azure portal.

#### Answer:

See the explanation below.

#### Explanation:

1. In the Search resources, services, and docs box at the top of the portal, begin typing the name of a virtual machine, VM1 that has a network interface that you want to add to, or remove from, an application security group.
2. When the name of your VM appears in the search results, select it.
3. Under SETTINGS, select Networking. Select Configure the application security groups, select the application security groups that you want to add the network interface to, or unselect the application security groups that you want to remove the network interface from, and then select Save.



Reference:

<https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-network-interface>

## Question: 170

CertyIQ

SIMULATION -

You need to perform a full malware scan every Sunday at 02:00 on a virtual machine named VM1 by using Microsoft Antimalware for Virtual Machines.

To complete this task, sign in to the Azure portal.

### Answer:

See the explanation below.

### Explanation:

Deploy the Microsoft Antimalware Extension using the Azure Portal for single VM deployment

1. In Azure Portal, go to the Azure VM1's blade, navigate to the Extensions section and press Add.

Dashboard > Virtual machines > devrgvm > devrg > devrgvm - Extensions

**devrgvm - Extensions**  
Virtual machine

Search (Ctrl+/)

Overview  
Activity log  
Access control (IAM)  
Tags  
Diagnose and solve problems  
Settings  
Networking  
Disks  
Size  
Security  
Extensions

+ Add

Search to filter items...

NAME	TYPE
CustomScriptExtension	Microsoft.Compute.CustomScriptEx
DependencyAgentWindows	Microsoft.Azure.Monitoring.Depend
enablevmaccess	Microsoft.Compute.VMAccessAgen
IaaS.Diagnostics	Microsoft.Azure.Diagnostics.IaaS
MicrosoftMonitoringAgent	Microsoft.EnterpriseCloud.Monitori
SiteRecovery-Windows	Microsoft.Azure.RecoveryServices.S

2. Select the Microsoft Antimalware extension and press Create.

3. Fill the Install extension form as desired and press OK.

Scheduled: Enable -

Scan type: Full -

Scan day: Sunday -

## Install extension



Excluded files and locations ⓘ

Excluded file extensions ⓘ

Excluded processes ⓘ

Real-time protection ⓘ

Enable

Disable

Run a scheduled scan ⓘ

Enable

Disable

Scan type ⓘ

Quick

Full

Scan day ⓘ

Saturday



Scan time ⓘ

120

Reference:

<https://www.e-apostolidis.gr/microsoft/azure/azure-vm-antimalware-extension-management/>

### Question: 171

CertyIQ

SIMULATION -

You need to prevent administrative users from accidentally deleting a virtual network named VNET1. The administrative users must be allowed to modify the settings of VNET1.

To complete this task, sign in to the Azure portal.

**Answer:**

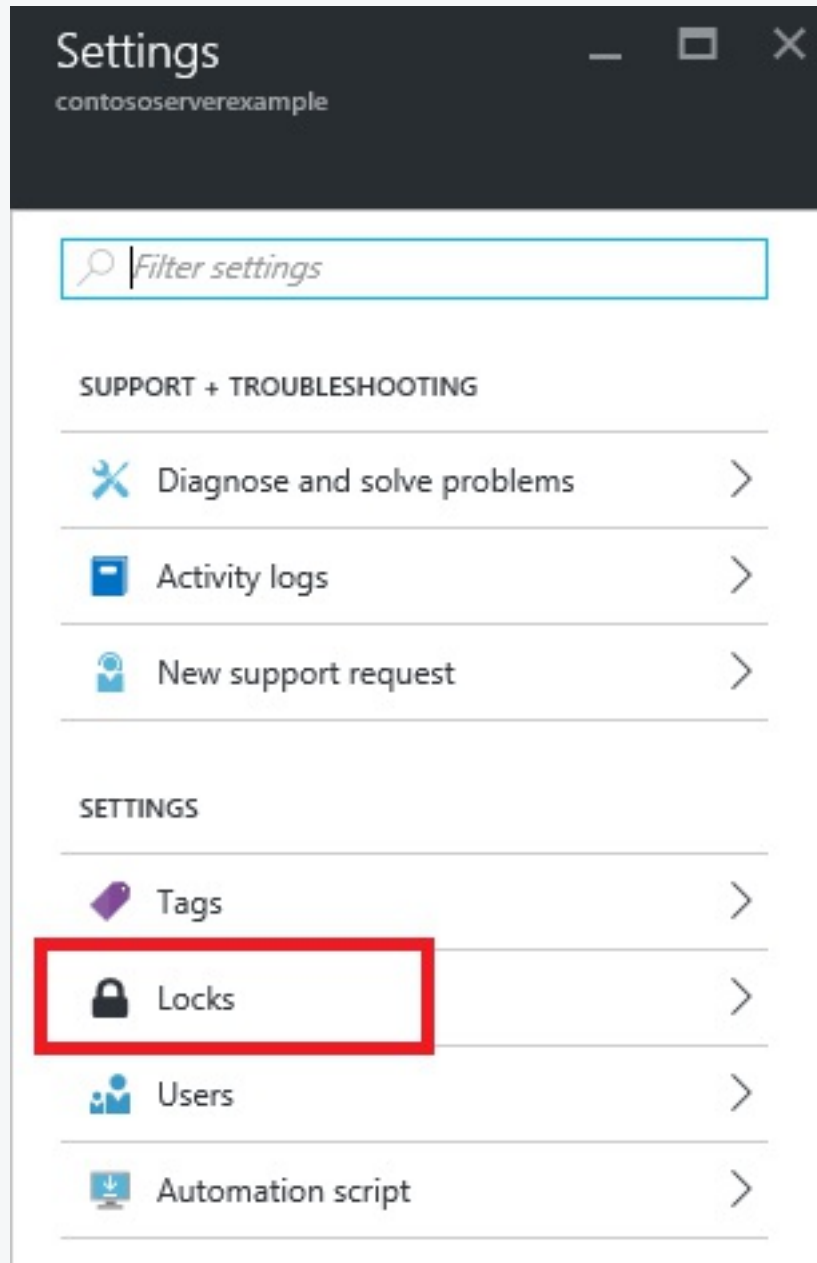
See the explanation below.

**Explanation:**

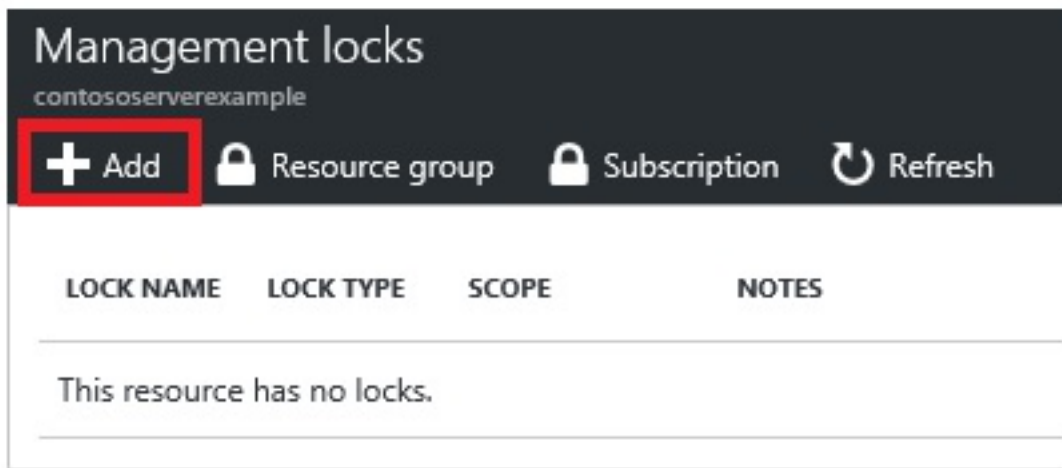
Locking prevents other users in your organization from accidentally deleting or modifying critical resources, such as Azure subscription, resource group, or resource.

Note: In Azure, the term resource refers to an entity managed by Azure. For example, virtual machines, virtual networks, and storage accounts are all referred to as Azure resources.

1. In the Settings blade for virtual network VNET, select Locks.



2. To add a lock, select Add.



3. For Lock type select Delete lock, and click OK

Reference:

<https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-lock-resources>

## Question: 172

CertyIQ

SIMULATION -

You need to grant the required permissions to a user named User2-1234578 to manage the virtual networks in the RG1lod1234578 resource group. The solution must use the principle of least privilege.

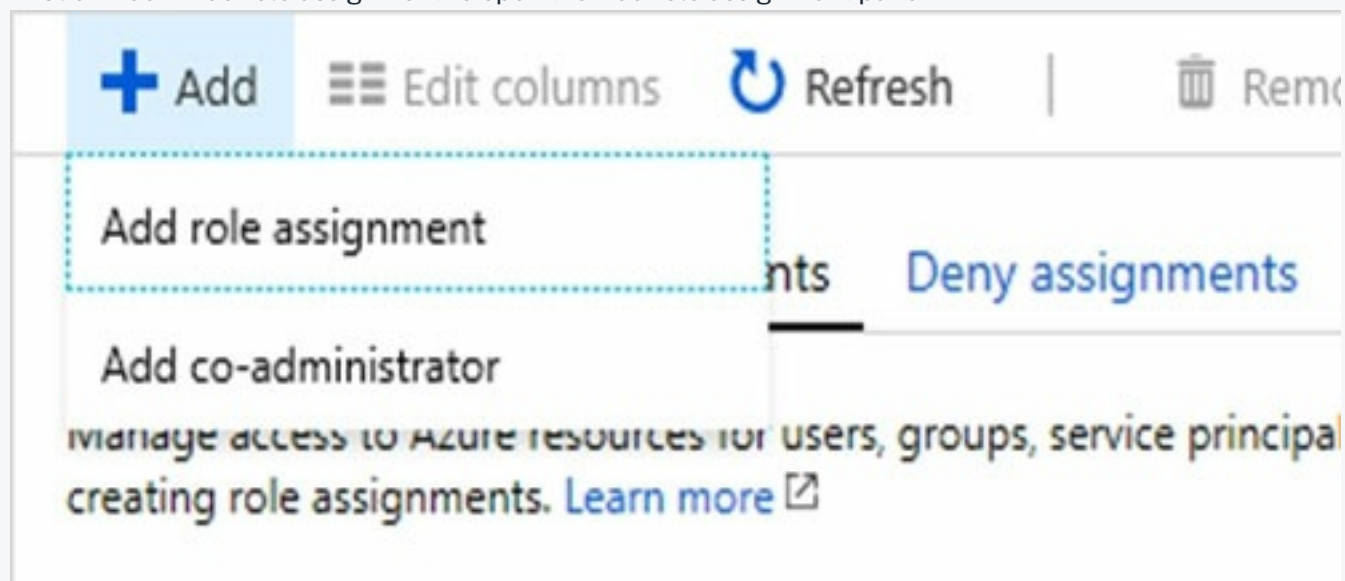
To complete this task, sign in to the Azure portal.

### Answer:

See the explanation below.

### Explanation:

1. In Azure portal, locate and select the RG1lod1234578 resource group.
2. Click Access control (IAM).
3. Click the Role assignments tab to view all the role assignments at this scope.
4. Click Add > Add role assignment to open the Add role assignment pane.



5. In the Role drop-down list, select the role Virtual Machine Contributor.

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

6. In the Select list, select user User2-1234578

7. Click Save to assign the role.

Reference:

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

**Question: 173**

CertyIQ

**SIMULATION -**

You need to ensure that only devices connected to a 131.107.0.0/16 subnet can access data in the rg1lod1234578 Azure Storage account.

To complete this task, sign in to the Azure portal.

**Answer:**

See the explanation below.

**Explanation:**

**Step 1:**

1. In Azure portal go to the storage account you want to secure. Here: rg1lod1234578
2. Click on the settings menu called Firewalls and virtual networks.
3. To deny access by default, choose to allow access from Selected networks. To allow traffic from all networks, choose to allow access from All networks.
4. Click Save to apply your changes.

**Step 2:**

1. Go to the storage account you want to secure. Here: rg1lod1234578
2. Click on the settings menu called Firewalls and virtual networks.
3. Check that you've selected to allow access from Selected networks.
4. To grant access to a virtual network with a new network rule, under Virtual networks, click Add existing virtual network, select Virtual networks and Subnets options. Enter the 131.107.0.0/16 subnet and then click Add.

Note: When network rules are configured, only applications requesting data over the specified set of networks can access a storage account. You can limit access to your storage account to requests originating from specified IP addresses, IP ranges or from a list of subnets in an Azure Virtual Network (VNet).

Reference:

<https://docs.microsoft.com/en-us/azure/storage/common/storage-network-security>

**Question: 174**

CertyIQ

**HOTSPOT -**

You create resources in an Azure subscription as shown in the following table.

Name	Type	Region
RG1	Resource group	West Europe
VNET1	Azure virtual network	West Europe
Contoso1901	Azure Storage account	West Europe

VNET1 contains two subnets named Subnet1 and Subnet2. Subnet1 has a network ID of 10.0.0.0/24. Subnet2 has a network ID of 10.1.1.0/24.

Contoso1901 is configured as shown in the exhibit. (Click the Exhibit tab.)

```

PS C:\> (Get-AzStorageAccount -ResourceGroupName RG1 -Name contoso1901).NetworkRuleSet

ByPass           : Logging, Metrics
DefaultAction    : Deny
IpRules          : [193.77.0.0/16,...]
VirtualNetworkRules : [/subscriptions/a90c8c8f-d8bc-4112-abfb-
                    dac4906573dd/resourceGroups/RG1/providers/Microsoft.Network/
                    virtualNetworks/VNET1/subnets/Subnet1,...]

PS C:\> (Get-AzStorageAccount -ResourceGroupName RG1 -Name contoso1901).NetworkRuleSet.
                                             IpRules
Action  IPAddressOrRange
-----  -
Allow   193.77.0.0/16

PS C:\> (Get-AzStorageAccount -ResourceGroupName RG1 -Name contoso1901).NetworkRuleSet.
                                             VirtualNetworkRules
Action  VirtualNetworkResourceId
-----  -
Allow   /subscriptions/a90c8c8f-d8bc-4112-abfb-dac4906573dd/resourceGroups/
        RG1/providers/Microsoft.Network/virtualNetworks/VNET1/subnets/Subnet1
State
-----
Succeeded

```

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

NOTE: Each correct selection is worth one point.

Hot Area:

### Answer area

Statements	Yes	No
An Azure virtual machine on Subnet1 can access data in Contoso1901.	<input type="radio"/>	<input type="radio"/>
An Azure virtual machine on Subnet2 can access data in Contoso1901.	<input type="radio"/>	<input type="radio"/>
A computer on the Internet that has an IP address of 193.77.10.2 can access data in Contoso1901.	<input type="radio"/>	<input type="radio"/>

Answer:

### Answer area

Statements	Yes	No
An Azure virtual machine on Subnet1 can access data in Contoso1901.	<input checked="" type="radio"/>	<input type="radio"/>
An Azure virtual machine on Subnet2 can access data in Contoso1901.	<input type="radio"/>	<input checked="" type="radio"/>
A computer on the Internet that has an IP address of 193.77.10.2 can access data in Contoso1901.	<input checked="" type="radio"/>	<input type="radio"/>

### Explanation:

Box 1: Yes -

Access from Subnet1 is allowed.

Box 2: No -

No access from Subnet2 is allowed.



Box 3: Yes -  
Access from IP address 193.77.10.2 is allowed.

### Question: 175

CertyIQ

You have an Azure subscription that contains the virtual machines shown in the following table.

Name	Location	Virtual network name
VM1	East US	VNET1
VM2	West US	VNET2
VM3	East US	VNET1
VM4	West US	VNET3

All the virtual networks are peered.  
You deploy Azure Bastion to VNET2.  
Which virtual machines can be protected by the bastion host?

- A. VM1, VM2, VM3, and VM4
- B. VM1, VM2, and VM3 only
- C. VM2 and VM4 only
- D. VM2 only

**Answer: A**

#### Explanation:

Azure Bastion and VNet peering can be used together. When VNet peering is configured, you don't have to deploy Azure Bastion in each peered VNet. This means if you have an Azure Bastion host configured in one virtual network (VNet), it can be used to connect to VMs deployed in a peered VNet without deploying an additional bastion host.

Reference:

<https://docs.microsoft.com/en-us/azure/bastion/vnet-peering>

### Question: 176

CertyIQ

You have Azure Resource Manager templates that you use to deploy Azure virtual machines. You need to disable unused Windows features automatically as instances of the virtual machines are provisioned. What should you use?

- A. device configuration policies in Microsoft Intune
- B. Azure Automation State Configuration
- C. security policies in Azure Security Center
- D. device compliance policies in Microsoft Intune

**Answer: B**

#### Explanation:

You can use Azure Automation State Configuration to manage Azure VMs (both Classic and Resource Manager), on-premises VMs, Linux machines, AWS VMs, and on-premises physical machines.

Note: Azure Automation State Configuration provides a DSC pull server similar to the Windows Feature DSC-

Service so that target nodes automatically receive configurations, conform to the desired state, and report back on their compliance. The built-in pull server in Azure Automation eliminates the need to set up and maintain your own pull server. Azure Automation can target virtual or physical Windows or Linux machines, in the cloud or on-premises.

Reference:

<https://docs.microsoft.com/en-us/azure/automation/automation-dsc-getting-started>

### Question: 177

CertyIQ

You have an Azure subscription named Sub1. Sub1 contains a virtual network named VNet1 that contains one subnet named Subnet1.

Subnet1 contains an Azure virtual machine named VM1 that runs Ubuntu Server 18.04.

You create a service endpoint for Microsoft.Storage in Subnet1.

You need to ensure that when you deploy Docker containers to VM1, the containers can access Azure Storage resources by using the service endpoint.

What should you do on VM1 before you deploy the container?

- 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.

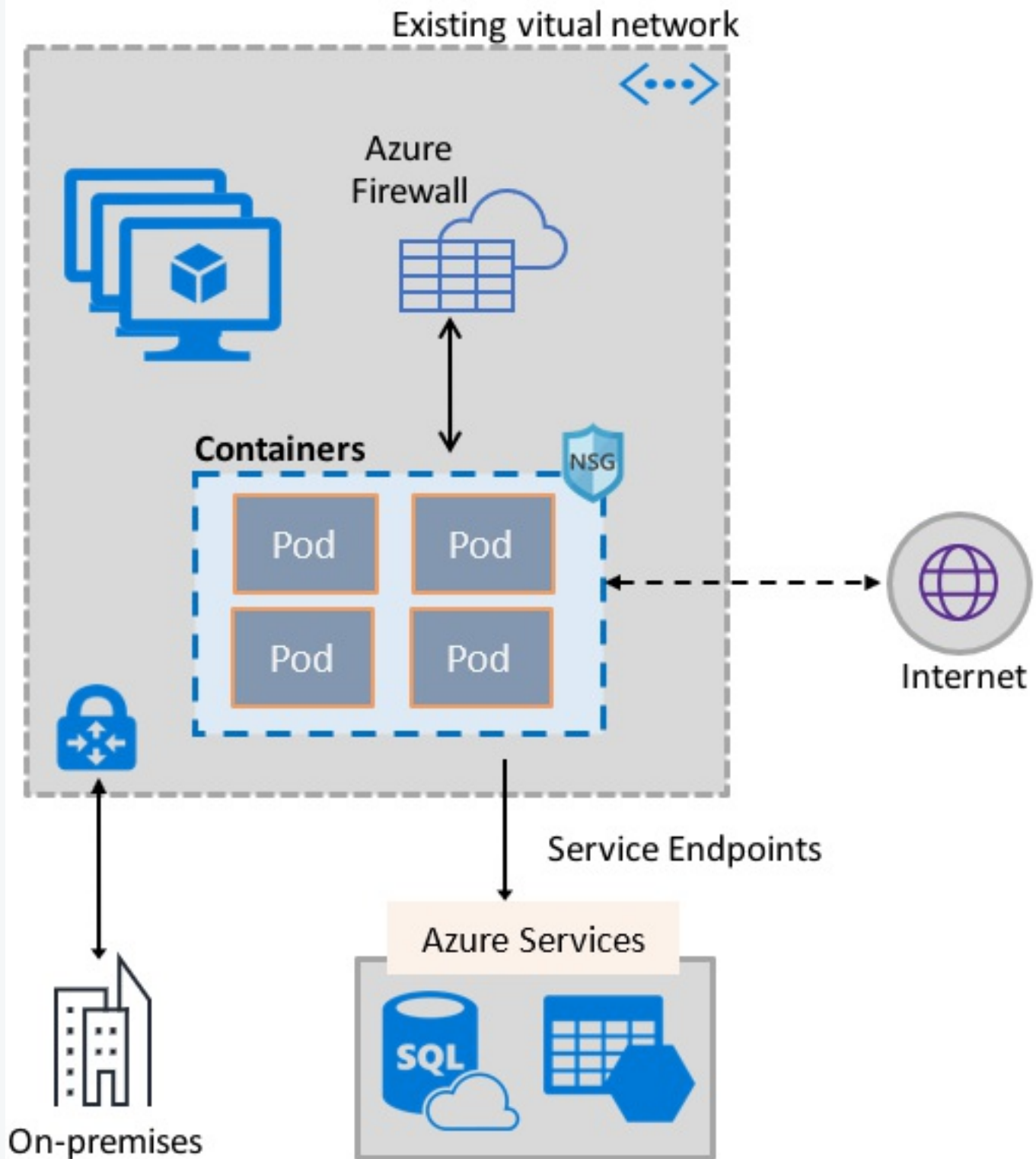
**Answer: C**

#### 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:



Reference:

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

### Question: 178

CertyIQ

You have Azure Resource Manager templates that you use to deploy Azure virtual machines. You need to disable unused Windows features automatically as instances of the virtual machines are provisioned. What should you use?

- A. device configuration policies in Microsoft Intune
- B. an Azure Desired State Configuration (DSC) virtual machine extension
- C. application security groups
- D. device compliance policies in Microsoft Intune

**Answer: B**

**Explanation:**

The primary use case for the Azure Desired State Configuration (DSC) extension is to bootstrap a VM to the Azure Automation State Configuration (DSC) service.

The service provides benefits that include ongoing management of the VM configuration and integration with other operational tools, such as Azure Monitoring.

Using the extension to register VM's to the service provides a flexible solution that even works across Azure subscriptions.

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-machines/extensions/dsc-overview>

**Question: 179**

CertyIQ

DRAG DROP -

You have an Azure subscription that contains the virtual networks shown in the following table.

Name	Region	Description
HubVNet	East US	HubVNet is a virtual network connected to the on-premises network by using a site-to-site VPN that has BGP route propagation enabled. HubVNet contains subnets named HubVNetSubnet0, AzureFirewallSubnet and GatewaySubnet. Virtual network gateway is connected to GatewaySubnet.
SpokeVNet	East US	SpokeVNet is a virtual network connected to HubVNet by using VNet peering. SpokeVNet contains a subnet named SpokeVNetSubnet0.

The Azure virtual machines on SpokeVNetSubnet0 can communicate with the computers on the on-premises network.

You plan to deploy an Azure firewall to HubVNet.

You create the following two routing tables:

⇒ RT1: Includes a user-defined route that points to the private IP address of the Azure firewall as a next hop address

⇒ RT2: Disables BGP route propagation and defines the private IP address of the Azure firewall as the default gateway

You need to ensure that traffic between SpokeVNetSubnet0 and the on-premises network flows through the Azure firewall.

To which subnet should you associate each route table? To answer, drag the appropriate subnets to the correct route tables. Each subnet may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:

## Answer Area

### Subnets

AzureFirewallSubnet

GatewaySubnet

SpokeVNetSubnet0

RT1:

RT2:

Answer:

## Answer Area

### Subnets

AzureFirewallSubnet

GatewaySubnet

SpokeVNetSubnet0

RT1:

GatewaySubnet

RT2:

SpokeVNetSubnet0

### Explanation:

RT1 - Configure a UDR on the hub gateway subnet that points to the firewall IP address as the next hop to the spoke networks.

RT2 - To route the spoke subnet traffic through the hub firewall, you can use a User Defined route (UDR) that points to the firewall with the Virtual network gateway route propagation option disabled

<https://docs.microsoft.com/en-us/azure/firewall/tutorial-hybrid-portal#prerequisites>

Reference:

<https://docs.microsoft.com/en-us/azure/firewall/tutorial-hybrid-portal#create-the-routes>

### Question: 180

CertyIQ

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
            ": {
          }
        }
      }
    }
  }
}
```

Answer:



## 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
            ": {
          }
        }
      }
    }
  }
}
```

### 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

Reference:

<https://docs.microsoft.com/en-us/azure/governance/policy/concepts/effects>

## Question: 181

CertyIQ

You are configuring an Azure Kubernetes Service (AKS) cluster that will connect to an Azure Container Registry. You need to use the auto-generated service principal to authenticate to the Azure Container Registry. What should you create?

- A. an Azure Active Directory (Azure AD) group
- B. an Azure Active Directory (Azure AD) role assignment
- C. an Azure Active Directory (Azure AD) user
- D. a secret in Azure Key Vault

**Answer: B**

**Explanation:**

When you create an AKS cluster, Azure also creates a service principal to support cluster operability with other Azure resources. You can use this auto-generated service principal for authentication with an ACR registry. To do so, you need to create an Azure AD role assignment that grants the cluster's service principal access to the container registry.

Reference:

<https://docs.microsoft.com/bs-latn-ba/azure/container-registry/container-registry-auth-aks>

**Question: 182**

**CertyIQ**

You have an Azure subscription that contains the Azure virtual machines shown in the following table.

Name	Operating system
VM1	Windows 10
VM2	Windows Server 2016
VM3	Windows Server 2019
VM4	Ubuntu Server 18.04 LTS

You create an MDM Security Baseline profile named Profile1.  
You need to identify to which virtual machines Profile1 can be applied.  
Which virtual machines should you identify?

- A. VM1 only
- B. VM1, VM2, and VM3 only
- C. VM1 and VM3 only
- D. VM1, VM2, VM3, and VM4

**Answer: A**

**Explanation:**

intunes enrollment works with windows 10 version 1809 or later

Reference:

<https://docs.microsoft.com/en-us/mem/intune/protect/security-baselines>

**Question: 183**

**CertyIQ**

SIMULATION -

You need to ensure that connections from the Internet to VNET1\subnet0 are allowed only over TCP port 7777. The solution must use only currently deployed resources.  
To complete this task, sign in to the Azure portal.

**Answer:**

See the explanation below.

**Explanation:**

You need to configure the Network Security Group that is associated with subnet0.

1. In the Azure portal, type Virtual Networks in the search box, select Virtual Networks from the search results then select VNET1. Alternatively, browse to Virtual Networks in the left navigation pane.
2. In the properties of VNET1, click on Subnets. This will display the subnets in VNET1 and the Network Security Group associated to each subnet. Note the name of the Network Security Group associated to Subnet0.
3. Type Network Security Groups into the search box and select the Network Security Group associated with Subnet0.
4. In the properties of the Network Security Group, click on Inbound Security Rules.
5. Click the Add button to add a new rule.
6. In the Source field, select Service Tag.
7. In the Source Service Tag field, select Internet.
8. Leave the Source port ranges and Destination field as the default values (\* and All).
9. In the Destination port ranges field, enter 7777.
10. Change the Protocol to TCP.
11. Leave the Action option as Allow.
12. Change the Priority to 100.
13. Change the Name from the default Port\_8080 to something more descriptive such as Allow\_TCP\_7777\_from\_Internet. The name cannot contain spaces.
14. Click the Add button to save the new rule.

**Question: 184****CertyIQ****SIMULATION -**

You need to prevent administrators from performing accidental changes to the Homepage app service plan. To complete this task, sign in to the Azure portal.

**Answer:**

See the explanation below.

**Explanation:**

You need to configure a 'lock' for the app service plan. A read-only lock ensures that no one can make changes to the app service plan without first deleting the lock.

1. In the Azure portal, type App Service Plans in the search box, select App Service Plans from the search results then select Homepage. Alternatively, browse to App Service Plans in the left navigation pane.
2. In the properties of the app service plan, click on Locks.
3. Click the Add button to add a new lock.
4. Enter a name in the Lock name field. It doesn't matter what name you provide for the exam.
5. For the Lock type, select Read-only.
6. Click OK to save the changes.

**Question: 185****CertyIQ****SIMULATION -**

You need to ensure that a user named Danny1234578 can sign in to any SQL database on a Microsoft SQL server named web1234578 by using SQL Server Management Studio (SSMS) and Azure Active Directory (Azure AD) credentials. To complete this task, sign in to the Azure portal.

**Answer:**

See the explanation below.

**Explanation:**

You need to provision an Azure AD Admin for the SQL Server.

1. In the Azure portal, type SQL Server in the search box, select SQL Server from the search results then select the server named web1234578. Alternatively, browse to SQL Server in the left navigation pane.
2. In the SQL Server properties page, click on Active Directory Admin.
3. Click the Set Admin button.
4. In the Add Admin window, search for and select Danny1234578.
5. Click the Select button to add Danny1234578.
6. Click the Save button to save the changes.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-sql/database/authentication-aad-configure?tabs=azure-power-shell>

**Question: 186**

CertyIQ

SIMULATION -

You need to configure a Microsoft SQL server named Web1234578 only to accept connections from the Subnet0 subnet on the VNET01 virtual network.

To complete this task, sign in to the Azure portal.

**Answer:**

See the explanation below.

**Explanation:**

You need to allow access to Azure services and configure a virtual network rule for the SQL Server.

1. In the Azure portal, type SQL Server in the search box, select SQL Server from the search results then select the server named web1234578. Alternatively, browse to SQL Server in the left navigation pane.
2. In the properties of the SQL Server, click Firewalls and virtual networks.
3. In the Virtual networks section, click on Add existing. This will open the Create/Update virtual network rule window.
4. Give the rule a name such as Allow\_VNET01-Subnet0 (it doesn't matter what name you enter for the exam).
5. In the Virtual network box, select VNET01.
6. In the Subnet name box, select Subnet0.
7. Click the OK button to save the rule.
8. Back in the Firewall / Virtual Networks window, set the Allow access to Azure services option to On.

**Question: 187**

CertyIQ

You have Azure Resource Manager templates that you use to deploy Azure virtual machines.

You need to disable unused Windows features automatically as instances of the virtual machines are provisioned. What should you use?

- A.device configuration policies in Microsoft Intune
- B.an Azure Desired State Configuration (DSC) virtual machine extension
- C.security policies in Azure Security Center
- D.Azure Logic Apps

**Answer: B**

**Explanation:**

The primary use case for the Azure Desired State Configuration (DSC) extension is to bootstrap a VM to the Azure Automation State Configuration (DSC) service.

The service provides benefits that include ongoing management of the VM configuration and integration with other operational tools, such as Azure Monitoring.

Using the extension to register VM's to the service provides a flexible solution that even works across Azure subscriptions.

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-machines/extensions/dsc-overview>

**Question: 188****CertyIQ**

HOTSPOT -

You have an Azure subscription that contains the virtual machines shown in the following table.

Name	Resource group	Status
VM1	RG1	Stopped (Deallocated)
VM2	RG2	Stopped (Deallocated)

You create the Azure policies shown in the following table.

Policy definition	Resource type	Scope
Not allowed resource types	virtualMachines	RG1
Allowed resource types	virtualMachines	RG2

You create the resource locks shown in the following table.

Name	Type	Created on
Lock1	Read-only	VM1
Lock2	Read-only	RG2

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

NOTE: Each correct selection is worth one point.

Hot Area:

## Answer Area

Statements	Yes	No
You can start VM1.	<input type="radio"/>	<input type="radio"/>
You can start VM2.	<input type="radio"/>	<input type="radio"/>
You can create a virtual machine in RG2.	<input type="radio"/>	<input type="radio"/>

Answer:

## Answer Area

Statements	Yes	No
You can start VM1.	<input type="radio"/>	<input checked="" type="radio"/>
You can start VM2.	<input type="radio"/>	<input checked="" type="radio"/>
You can create a virtual machine in RG2.	<input type="radio"/>	<input checked="" type="radio"/>

**Explanation:**

You cannot start VM1 because of read only lock on VM1

You cannot start VM2 because of read only lock on RG2

You cannot create a new VM in RG2 because of read only lock on RG2

### Question: 189

CertyIQ

HOTSPOT -

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



Name	Subscription role	Azure AD user role
User1	Owner	<i>None</i>
User2	Contributor	<i>None</i>
User3	Security Admin	<i>None</i>
User4	<i>None</i>	Service administrator

You create a resource group named RG1.

Which users can modify the permissions for RG1 and which users can create virtual networks in RG1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

### Answer Area

Users who can modify the permissions for RG1:

▼

☐ User1 only
 ☐ User1 and User2 only
 ☐ User1 and User3 only
 ☐ User1, User2 and User3 only
 ☐ User1, User2, User3, and User4

Users who can create virtual networks in RG1:

▼

☐ User1 only
 ☐ User1 and User2 only
 ☐ User1 and User3 only
 ☐ User1, User2 and User3 only
 ☐ User1, User2, User3, and User4

Answer:

### Answer Area

Users who can modify the permissions for RG1:

▼

☒ User1 only
 ☐ User1 and User2 only
 ☐ User1 and User3 only
 ☐ User1, User2 and User3 only
 ☐ User1, User2, User3, and User4

Users who can create virtual networks in RG1:

▼

☐ User1 only
 ☒ User1 and User2 only
 ☐ User1 and User3 only
 ☐ User1, User2 and User3 only
 ☐ User1, User2, User3, and User4

Explanation:

Box 1: Only an owner can change permissions on resources.

Box 2: A Contributor can create/modify/delete anything in the subscription but cannot change permissions.

### Question: 190

CertyIQ

#### SIMULATION -

You need to configure network connectivity between a virtual network named VNET1 and a virtual network named VNET2. The solution must ensure that virtual machines connected to VNET1 can communicate with virtual machines connected to VNET2.

To complete this task, sign in to the Azure portal and modify the Azure resources.

#### Answer:

See the explanation below.

#### Explanation:

You need to configure VNet Peering between the two networks. The questions states, The solution must ensure that virtual machines connected to VNET1 can communicate with virtual machines connected to VNET2. It doesn't say the VMs on VNET2 should be able to communicate with VMs on VNET1. Therefore, we need to configure the peering to allow just the one-way communication.

1. In the Azure portal, type Virtual Networks in the search box, select Virtual Networks from the search results then select VNET1. Alternatively, browse to Virtual Networks in the left navigation pane.
  2. In the properties of VNET1, click on Peerings.
  3. In the Peerings blade, click Add to add a new peering.
  4. In the Name of the peering from VNET1 to remote virtual network box, enter a name such as VNET1-VNET2 (this is the name that the peering will be displayed as in VNET1)
  5. In the Virtual Network box, select VNET2.
  6. In the Name of the peering from remote virtual network to VNET1 box, enter a name such as VNET2-VNET1 (this is the name that the peering will be displayed as in VNET2).
- There is an option Allow virtual network access from VNET to remote virtual network. This should be left as Enabled.
7. For the option Allow virtual network access from remote network to VNET1, click the slider button to Disabled.
  8. Click the OK button to save the changes.

#### Reference:

<https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-manage-peering>

### Question: 191

CertyIQ

#### SIMULATION -

You need to deploy an Azure firewall to a virtual network named VNET3.

To complete this task, sign in to the Azure portal and modify the Azure resources.

This task might take several minutes to complete. You can perform other tasks while the task completes.

#### Answer:

See the explanation below.

#### Explanation:

To add an Azure firewall to a VNET, the VNET must first be configured with a subnet named AzureFirewallSubnet (if it doesn't already exist).

Configure VNET3.

1. In the Azure portal, type Virtual Networks in the search box, select Virtual Networks from the search results then select VNET3. Alternatively, browse to Virtual Networks in the left navigation pane.
  2. In the Overview section, note the Location (region) and Resource Group of the virtual network. We'll need these when we add the firewall.
  3. Click on Subnets.
  4. Click on + Subnet to add a new subnet.
  5. Enter AzureFirewallSubnet in the Name box. The subnet must be named AzureFirewallSubnet.
  6. Enter an appropriate IP range for the subnet in the Address range box.
  7. Click the OK button to create the subnet.
- Add the Azure Firewall.
1. In the settings of VNET3 click on Firewall.
  2. Click the Click here to add a new firewall link.
  3. The Resource group will default to the VNET3 resource group. Leave this default.
  4. Enter a name for the firewall in the Name box.
  5. In the Region box, select the same region as VNET3.
  6. In the Public IP address box, select an available public IP address if one exists, or click Add new to add a new public IP address.
  7. Click the Review + create button.
  8. Review the settings and click the Create button to create the firewall.

Reference:

<https://docs.microsoft.com/en-us/azure/firewall/tutorial-firewall-deploy-portal>

## Question: 192

CertyIQ

### SIMULATION -

You need to configure a virtual network named VNET2 to meet the following requirements:

- ⇒ Administrators must be prevented from deleting VNET2 accidentally.
- ⇒ Administrators must be able to add subnets to VNET2 regularly.

To complete this task, sign in to the Azure portal and modify the Azure resources.

### Answer:

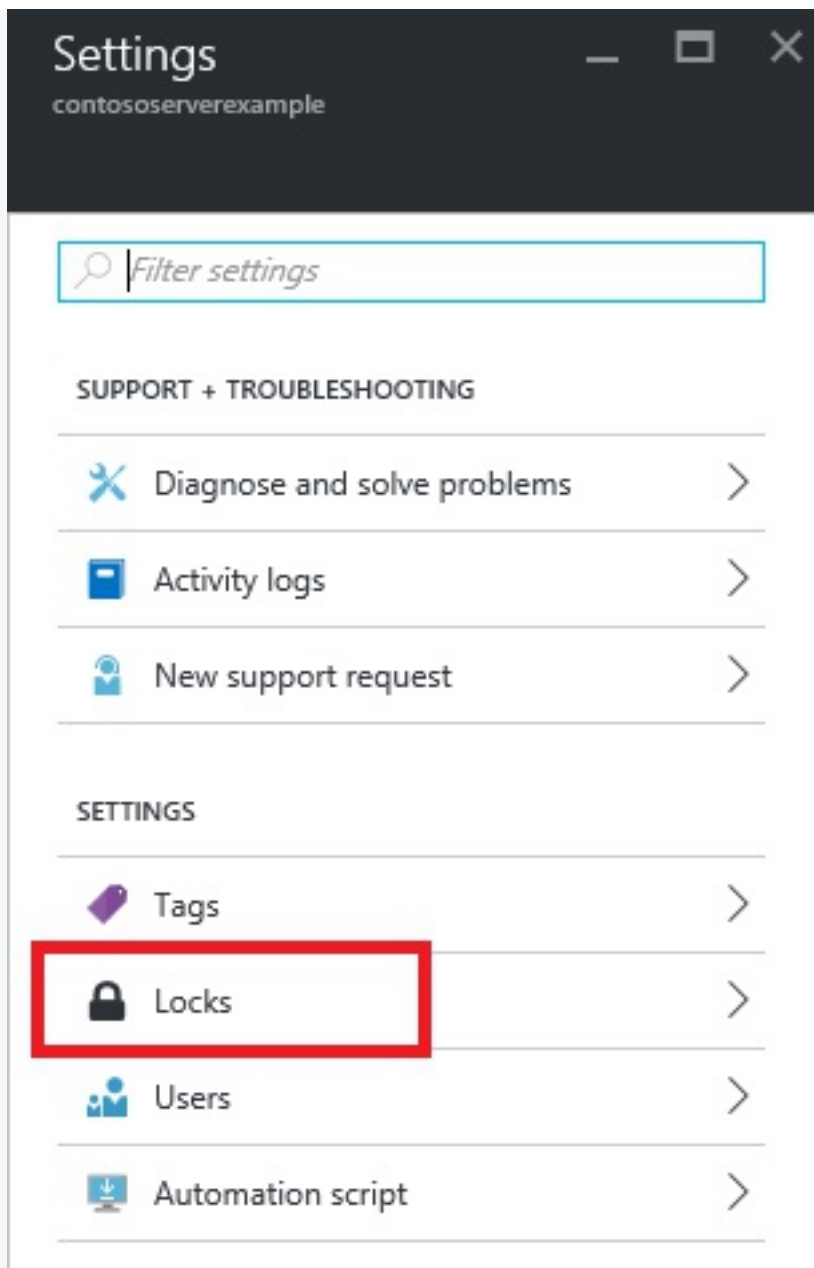
See the explanation below.

### Explanation:

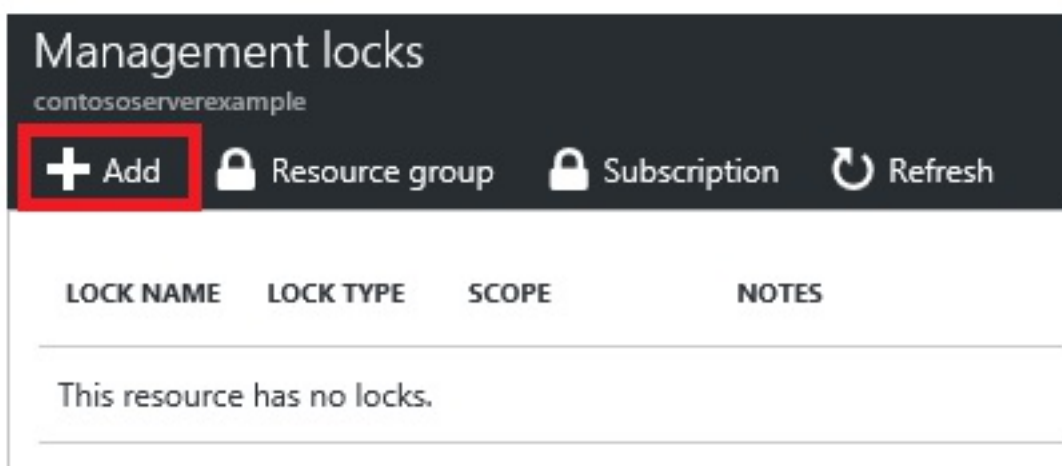
Locking prevents other users in your organization from accidentally deleting or modifying critical resources, such as Azure subscription, resource group, or resource.

Note: In Azure, the term resource refers to an entity managed by Azure. For example, virtual machines, virtual networks, and storage accounts are all referred to as Azure resources.

1. In the Azure portal, type Virtual Networks in the search box, select Virtual Networks from the search results then select VNET2. Alternatively, browse to Virtual Networks in the left navigation pane.
2. In the Settings blade for virtual network VNET2, select Locks.



3. To add a lock, select Add.



4. For Lock type select Delete lock, and click OK

Reference:

<https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-lock-resources>

You have an Azure virtual machine named VM1.

From Microsoft Defender for Cloud, you get the following high-severity recommendation: 'Install endpoint protection solutions on virtual machine'.

You need to resolve the issue causing the high-severity recommendation.

What should you do?

- A. Add the Microsoft Antimalware extension to VM1.
- B. Install Microsoft System Center Security Management Pack for Endpoint Protection on VM1.
- C. Add the Network Watcher Agent for Windows extension to VM1.
- D. Onboard VM1 to Microsoft Defender for Endpoint.

**Answer: A**

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/security-center-endpoint-protection>

### Question: 194

CertyIQ

HOTSPOT -

You have a file named File1.yaml that contains the following contents.

```
apiVersion: 2018-10-01
location: eastus
name: containergroup1
properties:
  containers:
  - name: container1
    properties:
      environmentVariables:
      - name: 'Variable1'
        value: 'Value1'
      - name: 'Variable2'
        secureValue: 'Value2'
      image: nginx
      ports: []
      resources:
        requests:
          cpu: 1.0
          memoryInGB: 1.5
      osType: Linux
      restartPolicy: Always
    tags: null
  type: Microsoft.ContainerInstance/containerGroups
```

You create an Azure container instance named container1 by using File1.yaml.

You need to identify where you can access the values of Variable1 and Variable2.

What should you identify? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



## Answer Area

Variable1:

	▼
Cannot be accessed	
Can be accessed from the Azure portal only	
Can be accessed from inside container1 only	
Can be accessed from inside container1 and the Azure portal	

Variable2:

	▼
Cannot be accessed	
Can be accessed from the Azure portal only	
Can be accessed from inside container1 only	
Can be accessed from inside container1 and the Azure portal	

Answer:

## Answer Area

Variable1:

	▼
Cannot be accessed	
Can be accessed from the Azure portal only	
Can be accessed from inside container1 only	
Can be accessed from inside container1 and the Azure portal	

Variable2:

	▼
Cannot be accessed	
Can be accessed from the Azure portal only	
Can be accessed from inside container1 only	
Can be accessed from inside container1 and the Azure portal	

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/container-instances/container-instances-environment-variables>

### Question: 195

CertyIQ

You have an Azure subscription that contains a virtual network. The virtual network contains the subnets shown in the following table.



Name	Has a network security group (NSG) associated to the virtual subnet
Subnet1	Yes
Subnet2	No

The subscription contains the virtual machines shown in the following table.

Name	Has an NSG associated to the network adaptor of the virtual machine	Connected to
VM1	No	Subnet1
VM2	No	Subnet2
VM3	No	Subnet1
VM4	Yes	Subnet2

You enable just in time (JIT) VM access for all the virtual machines.

You need to identify which virtual machines are protected by JIT.

Which virtual machines should you identify?

- A. VM4 only
- B. VM1 and VM3 only
- C. VM1, VM3 and VM4 only
- D. VM1, VM2, VM3, and VM4

**Answer: C**

**Explanation:**

An NSG needs to be enabled, either at the VM level or the subnet level.

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/security-center-just-in-time>

## Question: 196

CertyIQ

HOTSPOT -

You have an Azure subscription that contains the virtual machines shown in the following table.

Name	Connected to	Private IP address	Public IP address
VM1	VNET1/Subnet1	10.1.1.4	13.80.73.87
VM2	VNET2/Subnet2	10.2.1.4	213.199.133.190
VM3	VNET2/Subnet2	10.2.1.5	None

Subnet1 and Subnet2 have a Microsoft.Storage service endpoint configured.

You have an Azure Storage account named storageacc1 that is configured as shown in the following exhibit.

Save Discard Refresh

Allow access from

All networks Selected networks

Configure network security for your storage accounts. [Learn more.](#)

## Virtual networks

Secure your storage account with virtual networks. [+ Add existing virtual network](#)

[+ Add new virtual network](#)

VIRTUAL NETWORK	SUBNET	ADDRESS RANGE	ENDPOINT STATUS	RESOURCE GROUP	SUBSCRIPTION
-----------------	--------	---------------	-----------------	----------------	--------------

No network selected.

## Firewall

Add IP ranges to allow access from the internet on your on-premises networks. [Learn more.](#)

### Address Range

13.80.73.87



IP address or CIDR

## Exceptions

- ☒ Allow trusted Microsoft services to access this storage account ⓘ
- ☐ Allow read access to storage logging from any network
- ☐ Allow read access to storage metrics from any network

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

## Answer Area

Statements	Yes	No
From VM1, you can upload a blob to storageacc1.	<input type="radio"/>	<input type="radio"/>
From VM2, you can upload a blob to storageacc1.	<input type="radio"/>	<input type="radio"/>
From VM3 , you can upload a blob to storageacc1.	<input type="radio"/>	<input type="radio"/>

Answer:

## Answer Area

Statements	Yes	No
From VM1, you can upload a blob to storageacc1.	<input checked="" type="radio"/>	<input type="radio"/>
From VM2, you can upload a blob to storageacc1.	<input type="radio"/>	<input checked="" type="radio"/>
From VM3 , you can upload a blob to storageacc1.	<input type="radio"/>	<input checked="" type="radio"/>

### Explanation:

Box 1: Yes -

The public IP of VM1 is allowed through the firewall.

Box 2: No -

The allowed virtual network list is empty so VM2 cannot access storageacc1 directly. The public IP address of VM2 is not in the allowed IP list so VM2 cannot access storageacc1 over the Internet.

Box 3: No -

The allowed virtual network list is empty so VM3 cannot access storageacc1 directly. VM3 does not have a public IP address so it cannot access storageacc1 over the Internet.

Reference:

<https://docs.microsoft.com/en-gb/azure/storage/common/storage-network-security>

### Question: 197

CertyIQ

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	

Answer:

# 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	

## Explanation:

An update deployment can apply to Windows VMs or Linux VMs but not both. The VMs can be in different regions, different subscriptions and different resource groups.

Update1: VM1 and VM2 only -  
VM3: Windows Server 2016.

Update2: VM4 and VM5 only -  
VM6: CentOS 7.5.

For Linux, the machine must have access to an update repository. The update repository can be private or public.

Reference:

<https://docs.microsoft.com/en-us/azure/automation/update-management/overview>

## Question: 198

CertyIQ

HOTSPOT -

You have an Azure subscription named Sub1.

You create a virtual network that contains one subnet. On the subnet, you provision the virtual machines shown in the following table.



Name	Network interface	Application security group assignment	IP address
VM1	NIC1	AppGroup12	10.0.0.10
VM2	NIC2	AppGroup12	10.0.0.11
VM3	NIC3	AppGroup3	10.0.0.100
VM4	NIC4	AppGroup4	10.0.0.200

Currently, you have not provisioned any network security groups (NSGs).  
You need to implement network security to meet the following requirements:

- Allow traffic to VM4 from VM3 only.
- Allow traffic from the Internet to VM1 and VM2 only.
- Minimize the number of NSGs and network security rules.

How many NSGs and network security rules should you create? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

# Answer Area

NSGs:

▼

1

2

3

4

Network security rules:

▼

1

2

3

4

Answer:



# Answer Area

NSGs: 

	▼
1	
2	
3	
4	

Network security rules: 

	▼
1	
2	
3	
4	

## Explanation:

) You can only assign 1 NSG to a subnet, and there is only one subnet in the description. So Box 1 is 1

2) Number of rules in NSG can be any, they are processed in sequence.

Rule 1: You can have AppGroup3 as the source and AppGroup4 as destination in one rule then allow traffic.

Rule 2: You can have Service Tag "Internet" as a source and AppGroup12 as the destination. then allow traffic.

Rule 3: YOu can have source as the subnet range and destination as subnet range then deny all traffic, so only above rules will be allowing traffic.

Box 2 is 3.

You still have 3 default rules that allow traffic from VNET, LoadBalancer and deny all other inbound traffic.

References:

<https://docs.microsoft.com/en-us/azure/virtual-network/security-overview>

## Question: 199

CertyIQ

HOTSPOT -

You have an Azure key vault.

You need to delegate administrative access to the key vault to meet the following requirements:

- Provide a user named User1 with the ability to set advanced access policies for the key vault.
- Provide a user named User2 with the ability to add and delete certificates in the key vault.
- Use the principle of least privilege.

What should you use to assign access to each user? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

## Answer Area

User1:

	▼
A key vault access policy	
Azure Policy	
Managed identities for Azure resources	
RBAC	

User2:

	▼
A key vault access policy	
Azure Policy	
Managed identities for Azure resources	
RBAC	

Answer:

## Answer Area

User1:

	▼
A key vault access policy	
Azure Policy	
Managed identities for Azure resources	
RBAC	

User2:

	▼
A key vault access policy	
Azure Policy	
Managed identities for Azure resources	
RBAC	

**Explanation:**

User1: RBAC -

RBAC is used as the Key Vault access control mechanism for the management plane. It would allow a user with the proper identity to:

- set Key Vault access policies
- create, read, update, and delete key vaults

⇒ set Key Vault tags

Note: Role-based access control (RBAC) is a system that provides fine-grained access management of Azure resources. Using RBAC, you can segregate duties within your team and grant only the amount of access to users that they need to perform their jobs.

User2: A key vault access policy

A key vault access policy is the access control mechanism to get access to the key vault data plane. Key Vault access policies grant permissions separately to keys, secrets, and certificates.

Reference:

<https://docs.microsoft.com/en-us/azure/key-vault/key-vault-secure-your-key-vault>

### Question: 200

CertyIQ

You have Azure Resource Manager templates that you use to deploy Azure virtual machines. You need to disable unused Windows features automatically as instances of the virtual machines are provisioned. What should you use?

- A. device compliance policies in Microsoft Intune
- B. Azure Automation State Configuration
- C. application security groups
- D. Azure Advisor

**Answer: B**

#### Explanation:

You can use Azure Automation State Configuration to manage Azure VMs (both Classic and Resource Manager), on-premises VMs, Linux machines, AWS VMs, and on-premises physical machines. Note: Azure Automation State Configuration provides a DSC pull server similar to the Windows Feature DSC Service so that target nodes automatically receive configurations, conform to the desired state, and report back on their compliance. The built-in pull server in Azure Automation eliminates the need to set up and maintain your own pull server. Azure Automation can target virtual or physical Windows or Linux machines, in the cloud or on-premises.

### Question: 201

CertyIQ

You have an Azure Container Registry named Registry1. From Azure Security Center, you enable Azure Container Registry vulnerability scanning of the images in Registry1.

You perform the following actions:

- ⇒ Push a Windows image named Image1 to Registry1.
- ⇒ Push a Linux image named Image2 to Registry1.
- ⇒ Push a Windows image named Image3 to Registry1.
- ⇒ Modify Image1 and push the new image as Image4 to Registry1.
- Modify Image2 and push the new image as Image5 to Registry1.

Which two images will be scanned for vulnerabilities? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. Image4
- B. Image2
- C. Image1
- D. Image3
- E. Image5

**Answer: BE**

**Explanation:**

Only Linux images are scanned. Windows images are not scanned.

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/azure-container-registry-integration>

**Question: 202**

**CertyIQ**

HOTSPOT -

You have two Azure virtual machines in the East US 2 region as shown in the following table.

Name	Operating system	Type	Tier
VM1	Windows Server 2008 R2	A3	Basic
VM2	Ubuntu 16.04-DAILY-LTS	L4s	Standard

You deploy and configure an Azure Key vault.

You need to ensure that you can enable Azure Disk Encryption on VM1 and VM2.

What should you modify on each virtual machine? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

## Answer Area

VM1:

	▼
The operating system version	
The tier	
The type	

VM2:

	▼
The operating system version	
The tier	
The type	

**Answer:**

# Answer Area

VM1:

	▼
The operating system version	
The tier	
The type	

VM2:

	▼
The operating system version	
The tier	
The type	

## Explanation:

VM1: The Tier -

The Tier needs to be upgraded to standard.

Disk Encryption for Windows and Linux IaaS VMs is in General Availability in all Azure public regions and Azure Government regions for Standard VMs and VMs with Azure Premium Storage.

VM2: The type -

Need to change the VMtype to any of A, D, DS, G, GS, F, and so on, series IaaS VMs.

Not the operating system version: Ubuntu 16.04 is supported.

Reference:

<https://docs.microsoft.com/en-us/azure/security/azure-security-disk-encryption-overview> [https://docs.microsoft.com/en-us/azure/security/azure-security-disk-encryption-faq#bkmk\\_LinuxOSSupport](https://docs.microsoft.com/en-us/azure/security/azure-security-disk-encryption-faq#bkmk_LinuxOSSupport)

## Question: 203

CertyIQ

You have the Azure virtual machines shown in the following table.

Name	Operating system	Region	Resource group
VM1	Windows Server 2012	East US	RG1
VM2	Windows Server 2012 R2	West Europe	RG1
VM3	Windows Server 2016	West Europe	RG2
VM4	Red Hat Enterprise Linux 7.4	East US	RG2

You create an Azure Log Analytics workspace named Analytics1 in RG1 in the East US region. Which virtual machines can be enrolled in Analytics1?

- A. VM1 only
- B. VM1, VM2, and VM3 only
- C. VM1, VM2, VM3, and VM4
- D. VM1 and VM4 only

**Answer: C**

**Explanation:**

You can monitor Azure VMs in any region. The VMs themselves aren't limited to the regions supported by the Log Analytics workspace.

<https://docs.microsoft.com/en-us/azure/azure-monitor/vm/vminsights-configure-workspace?tabs=CLI>

#### Question: 204

CertyIQ

You are testing an Azure Kubernetes Service (AKS) cluster. The cluster is configured as shown in the exhibit. (Click the Exhibit tab.)



## Basics

Subscription	Azure Pass - Sponsorship
Resource group	RG1
Region	(US) East US
Kubernetes cluster name	AKScluster
Kubernetes version	1.12.8
DNS name prefix	AKScluster
Node count	3
Node size	Standard_DS2_v2

## Scale

Virtual nodes	Disabled
VM scale sets (preview)	Disabled

## Authentication

Enable RBAC	No
-------------	----

## Networking

HTTP application routing	No
Network configuration	Basic

## Monitoring

Enable container monitoring	No
-----------------------------	----

## Tags

(none)

You plan to deploy the cluster to production. You disable HTTP application routing. You need to implement application routing that will provide reverse proxy and TLS termination for AKS services by using a single IP address. What should you do?

- A.Create an AKS Ingress controller.
- B.Install the container network interface (CNI) plug-in.
- C.Create an Azure Standard Load Balancer.
- D.Create an Azure Basic Load Balancer.

**Answer: A**

**Explanation:**

An ingress controller is a piece of software that provides reverse proxy, configurable traffic routing, and TLS termination for Kubernetes services.

Reference:

<https://docs.microsoft.com/en-us/azure/aks/ingress-tls>

**Question: 205**

**CertyIQ**

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

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

You have an Azure subscription. The subscription contains 50 virtual machines that run Windows Server 2012 R2 or Windows Server 2016.

You need to deploy Microsoft Antimalware to the virtual machines.

Solution: You add an extension to each virtual machine.

Does this meet the goal?

A. Yes

B. No

**Answer: A**

**Explanation:**

You can use Visual Studio to enable and configure the Microsoft Antimalware service. This entails selecting Microsoft Antimalware extension from the dropdown list under Installed Extensions and click Add to configure with default antimalware configuration.

Reference:

<https://docs.microsoft.com/en-us/azure/security/fundamentals/antimalware>

**Question: 206**

**CertyIQ**

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

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

You have an Azure subscription. The subscription contains 50 virtual machines that run Windows Server 2012 R2 or Windows Server 2016.

You need to deploy Microsoft Antimalware to the virtual machines.

Solution: You connect to each virtual machine and add a Windows feature.

Does this meet the goal?

A. Yes

B. No

**Answer: B**

**Explanation:**

Microsoft Antimalware is deployed as an extension and not a feature.

Reference:

<https://docs.microsoft.com/en-us/azure/security/fundamentals/antimalware>

### Question: 207

CertyIQ

You have an Azure Active Directory (Azure AD) tenant named Contoso.com and an Azure Kubernetes Service (AKS) cluster AKS1.

You discover that AKS1 cannot be accessed by using accounts from Contoso.com.

You need to ensure AKS1 can be accessed by using accounts from Contoso.com. The solution must minimize administrative effort.

What should you do first?

- A. From Azure, recreate AKS1.
- B. From AKS1, upgrade the version of Kubernetes.
- C. From Azure AD, implement Azure AD Premium P2
- D. From Azure AD, configure the User settings.

**Answer: A**

**Explanation:**

From Azure, recreate AKS1.

Reference:

<https://docs.microsoft.com/en-us/azure/aks/azure-ad-integration-cli>

### Question: 208

CertyIQ

You have an Azure subscription that contains an Azure Container Registry named Registry1. Microsoft Defender for Cloud is enabled in the subscription.

You upload several container images to Registry1.

You discover that vulnerability security scans were not performed.

You need to ensure that the container images are scanned for vulnerabilities when they are uploaded to Registry1.

What should you do?

- A. From the Azure portal, modify the Pricing tier settings.
- B. From Azure CLI, lock the container images.
- C. Upload the container images by using AzCopy.
- D. Push the container images to Registry1 by using Docker.

**Answer: A**

**Explanation:**

Defender for Cloud offers basic, and many enhanced security features that can help protect your organization against threats and attacks.

When you enable the enhanced security features (paid), Defender for Cloud can provide unified security management and threat protection across your hybrid cloud workloads, including: Container security features

Container security features - Benefit from vulnerability management and real-time threat protection on your containerized environments. Charges are based on the number of unique container images pushed to your

connected registry. After an image has been scanned once, you won't be charged for it again unless it's modified and pushed once more.

Basic and enhanced security features

Reference:

<https://charbelnemnom.com/scan-container-images-in-azure-container-registry-with-azure-security-center/>

<https://learn.microsoft.com/en-us/azure/defender-for-cloud/enhanced-security-features-overview>

### Question: 209

CertyIQ

From Azure Security Center, you create a custom alert rule.  
You need to configure which users will receive an email message when the alert is triggered.  
What should you do?

- A. From Azure Monitor, create an action group.
- B. From Security Center, modify the Security policy settings of the Azure subscription.
- C. From Azure Active Directory (Azure AD), modify the members of the Security Reader role group.
- D. From Security Center, modify the alert rule.

**Answer: A**

**Explanation:**

A: Correct - assumes ASC is configured to stream logs to Azure monitor.

B: Incorrect - (badly worded) - "security policy defines the desired configuration of your workloads and helps ensure you're complying with the security requirements of your company or regulators" - nothing to do with alerts

C: Incorrect - Security Reader role group membership does not imply receiving email notifications

D: Incorrect - Security Center alert rules don't specify recipients.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-monitor/platform/action-groups>

### Question: 210

CertyIQ

You are configuring and securing a network environment.  
You deploy an Azure virtual machine named VM1 that is configured to analyze network traffic.  
You need to ensure that all network traffic is routed through VM1.  
What should you configure?

- A. a system route
- B. a network security group (NSG)
- C. a user-defined route

**Answer: C**

**Explanation:**

Although the use of system routes facilitates traffic automatically for your deployment, there are cases in which you want to control the routing of packets through a virtual appliance. You can do so by creating user defined routes that specify the next hop for packets flowing to a specific subnet to go to your virtual appliance instead, and enabling IP forwarding for the VM running as the virtual appliance.

Note: User Defined Routes -

For most environments you will only need the system routes already defined by Azure. However, you may need to create a route table and add one or more routes in specific cases, such as:

- ⇒ Force tunneling to the Internet via your on-premises network.
- ⇒ Use of virtual appliances in your Azure environment.
- ⇒ In the scenarios above, you will have to create a route table and add user defined routes to it.

Reference:

<https://github.com/uglide/azure-content/blob/master/articles/virtual-network/virtual-networks-udr-overview.md>

### Question: 211

CertyIQ

HOTSPOT -

You have a network security group (NSG) bound to an Azure subnet.

You run Get-AzNetworkSecurityRuleConfig and receive the output shown in the following exhibit.

Name	:	DenyStorageAccess
Description	:	
Protocol	:	*
SourcePortRange	:	{*}
DestinationPortRange	:	{*}
SourceAddressPrefix	:	{*}
DestinationAddressPrefix	:	{Storage}
SourceApplicationSecurityGroups	:	[]
DestinationApplicationSecurityGroups	:	[]
Access	:	Deny
Priority	:	105
Direction	:	Outbound

Name	:	StorageEA2Allow
ProvisioningState	:	Succeeded
Description	:	
Protocol	:	*
SourcePortRange	:	{*}
DestinationPortRange	:	{443}
SourceAddressPrefix	:	{*}
DestinationAddressPrefix	:	{Storage.EastUS2}
SourceApplicationSecurityGroups	:	[]
DestinationApplicationSecurityGroups	:	[]
Access	:	Allow
Priority	:	104
Direction	:	Outbound

Name	:	Contoso_FTP
Description	:	
Protocol	:	TCP
SourcePortRange	:	{*}
DestinationPortRange	:	{21}
SourceAddressPrefix	:	{1.2.3.4/32}
DestinationAddressPrefix	:	{10.0.0.5/32}
SourceApplicationSecurityGroups	:	[]
DestinationApplicationSecurityGroups	:	[]
Access	:	Allow
Priority	:	504
Direction	:	Inbound

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

NOTE: Each correct selection is worth one point.

Hot Area:



## Answer Area

Traffic destined for an Azure Storage account is [answer choice].

	▼
able to connect to East US	
able to connect to East US 2	
able to connect to West Europe	
prevented from connecting to all regions	

FTP connections from 1.2.3.4 to 10.0.0.10/32 are [answer choice].

	▼
allowed	
dropped	
forwarded	

Answer:

### Answer Area

Traffic destined for an Azure Storage account is [answer choice].

	▼
able to connect to East US	
able to connect to East US 2	
able to connect to West Europe	
prevented from connecting to all regions	

FTP connections from 1.2.3.4 to 10.0.0.10/32 are [answer choice].

	▼
allowed	
dropped	
forwarded	

### Explanation:

Box 1: able to connect to East US 2

The StorageEA2Allow has DestinationAddressPrefix Storage/EastUS2

Box 2: DROPPED

because the cidr notation is a /32 which means only one IP, which is different from the IP in the rule. so the packet would be dropped.

## Question: 212

CertyIQ

You have an Azure subscription that contains the virtual networks shown in the following table.

Name	Region	Subnet
VNET1	West US	Subnet11 and Subnet12
VNET2	West US 2	Subnet21
VNET3	East US	Subnet31

The subscription contains the virtual machines shown in the following table.

Name	Network interface	Connected to
VM1	NIC1	Subnet11
VM2	NIC2	Subnet11
VM3	NIC3	Subnet12
VM4	NIC4	Subnet21
VM5	NIC5	Subnet31

On NIC1, you configure an application security group named ASG1.  
On which other network interfaces can you configure ASG1?

- A. NIC2 only
- B. NIC2, NIC3, NIC4, and NIC5
- C. NIC2 and NIC3 only
- D. NIC2, NIC3, and NIC4 only

**Answer: C**

**Explanation:**

Only network interfaces in VNET1, which consists of Subnet11 and Subnet12, can be configured in ASG1, as all network interfaces assigned to an application security group have to exist in the same virtual network that the first network interface assigned to the application security group is in.

Reference:

<https://azure.microsoft.com/es-es/blog/applicationsecuritygroups/>

### Question: 213

CertyIQ

You have 15 Azure virtual machines in a resource group named RG1.  
All the virtual machines run identical applications.  
You need to prevent unauthorized applications and malware from running on the virtual machines.  
What should you do?

- A. Apply an Azure policy to RG1.
- B. From Azure Security Center, configure adaptive application controls.
- C. Configure Azure Active Directory (Azure AD) Identity Protection.
- D. Apply a resource lock to RG1.

**Answer: B**

**Explanation:**

Adaptive application control is an intelligent, automated end-to-end application whitelisting solution from

Azure Security Center. It helps you control which applications can run on your Azure and non-Azure VMs (Windows and Linux), which, among other benefits, helps harden your VMs against malware. Security Center uses machine learning to analyze the applications running on your VMs and helps you apply the specific whitelisting rules using this intelligence.

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/security-center-adaptive-application>

### Question: 214

CertyIQ

You have a web app hosted on an on-premises server that is accessed by using a URL of <https://www.contoso.com>. You plan to migrate the web app to Azure. You will continue to use <https://www.contoso.com>. You need to enable HTTPS for the Azure web app. What should you do first?

- A. Export the public key from the on-premises server and save the key as a P7b file.
- B. Export the private key from the on-premises server and save the key as a PFX file that is encrypted by using TripleDES.
- C. Export the public key from the on-premises server and save the key as a CER file.
- D. Export the private key from the on-premises server and save the key as a PFX file that is encrypted by using AES256.

**Answer: B**

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/azure/app-service/configure-ssl-certificate#private-certificate-requirements>

### Question: 215

CertyIQ

You plan to deploy Azure container instances. You have a containerized application that is comprised of two containers: an application container and a validation container. The application container is monitored by the validation container. The validation container performs security checks by making requests to the application container and waiting for responses after every transaction. You need to ensure that the application container and the validation container are scheduled to be deployed together. The containers must communicate to each other only on ports that are not externally exposed. What should you include in the deployment?

- A. application security groups
- B. network security groups (NSGs)
- C. management groups
- D. container groups

**Answer: D**

**Explanation:**

Azure Container Instances supports the deployment of multiple containers onto a single host using a container group. A container group is useful when building an application sidecar for logging, monitoring, or any other configuration where a service needs a second attached process.

Reference:

### Question: 216

CertyIQ

DRAG DROP -

You are configuring network connectivity for two Azure virtual networks named VNET1 and VNET2.

You need to implement VPN gateways for the virtual networks to meet the following requirements:

- VNET1 must have six site-to-site connections that use BGP.
- VNET2 must have 12 site-to-site connections that use BGP.
- Costs must be minimized.

Which VPN gateway SKU should you use for each virtual network? To answer, drag the appropriate SKUs to the correct networks. Each SKU may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:

#### Answer Area

SKUs	
Basic	VpnGw1
VpnGw2	VpnGw3

VNET1:

VNET2:

Answer:

#### Answer Area

SKUs	
Basic	VpnGw1
VpnGw2	VpnGw3

VNET1:

VNET2:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpngateways#gwsku>

### Question: 217

CertyIQ

You are securing access to the resources in an Azure subscription.

A new company policy states that all the Azure virtual machines in the subscription must use managed disks.

You need to prevent users from creating virtual machines that use unmanaged disks.

What should you use?

- A. Azure Monitor
- B. Azure Policy
- C. Azure Security Center
- D. Azure Service Health

Answer: B

HOTSPOT -

You have an Azure subscription that contains a storage account named storage1 and several virtual machines. The storage account and virtual machines are in the same Azure region. The network configurations of the virtual machines are shown in the following table.

Name	Public IP address	Connected to
VM1	52.232.128.194	VNET1/Subnet1
VM2	52.233.129.82	VNET2/Subnet2
VM3	52.233.130.11	VNET3/Subnet3

The virtual network subnets have service endpoints defined as shown in the following table.

Name	Service endpoint
VNET1/Subnet1	Microsoft.Storage
VNET2/Subnet2	None
VNET3/Subnet3	Microsoft.KeyVault

You configure the following Firewall and virtual networks settings for storage1:

- Allow access from: Selected networks
  - Virtual networks: VNET3\Subnet3
- Firewall " " Address range: 52.233.129.0/24

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

Hot Area:

Answer Area

Statements	Yes	No
VM1 can connect to storage1.	<input type="radio"/>	<input type="radio"/>
VM2 can connect to storage1.	<input type="radio"/>	<input type="radio"/>
VM3 can connect to storage1.	<input type="radio"/>	<input type="radio"/>

Answer:

## Answer Area

Statements	Yes	No
VM1 can connect to storage1.	<input type="radio"/>	<input checked="" type="radio"/>
VM2 can connect to storage1.	<input checked="" type="radio"/>	<input type="radio"/>
VM3 can connect to storage1.	<input checked="" type="radio"/>	<input type="radio"/>

### Explanation:

Box 1: No -

VNet1 has a service endpoint configure for Azure Storage. However, the Azure storage does not allow access from VNet1 or the public IP address of VM1.

Box 2: Yes -

VNet2 does not have a service endpoint configured. However, the Azure storage allows access from the public IP address of VM2.

Box 3: yes

VM3 can connect to the storage - at the moment you register the subnet to the storage selected network, you have also to enable a service end point to the storage.

### Question: 219

CertyIQ

You plan to create an Azure Kubernetes Service (AKS) cluster in an Azure subscription. The manifest of the registered server application is shown in the following exhibit.



The editor below allows you to update this application by directly modifying its JSON representation. For more details, see: [Understanding the Azure Active Directory application manifest](#).

```
1 {
2   "id": "d6b00db3-7ef4-4f3c-b1e7-8346f0a59546",
3   "acceptMappedClaims": null,
4   "accessTokenAcceptedVersion": null,
5   "addIns": [],
6   "allowPublicClient": null,
7   "appId": "88137405-6a75-4c20-903a-f7b18ff7d496",
8   "appRoles": [],
9   "oauth2AllowUrlPathMatching": false,
10  "createdDateTime": "2019-07-15T21:09:20Z",
11  "groupMembershipClaims": null,
12  "identifierUris": [],
13  "informationalUrls": {
14    "termsOfService": null,
15    "support": null,
16    "privacy": null,
17    "marketing": null
18  },
19  "keyCredentials": [],
20  "knownClientApplications": [],
21  "logoUrl": null,
22  "logoutUrl": null,
23  "name": "AKSAzureADServer",
24  "oauth2AllowIdTokenImplicitFlow": false,
25  "oauth2AllowImplicitFlow": false,
26  "oauth2Permissions": [],
27  "oauth2RequirePostResponse": false,
28  "optionalClaims": null,
29  "orgRestrictions": [],
30  "parentalControlSettings": {
```

You need to ensure that the AKS cluster and Azure Active Directory (Azure AD) are integrated. Which property should you modify in the manifest?

- A. accessTokenAcceptedVersion
- B. keyCredentials
- C. groupMembershipClaims
- D. acceptMappedClaims

**Answer: C**

**Explanation:**

Select Manifest, and then edit the groupMembershipClaims: value as "All". When you're finished with the updates, select Save.

Reference:

<https://docs.microsoft.com/en-us/azure/aks/azure-ad-integration-cli>

<https://www.codeproject.com/Articles/3211864/Operation-and-Maintenance-of-AKS-Applications>

HOTSPOT -  
You have the Azure virtual networks shown in the following table.

Name	Location	Subnet	Peered network
VNET1	East US	Subnet1	VNET2
VNET2	West US	Subnet2, Subnet3	VNET1
VNET4	East US	Subnet4	None

You have the Azure virtual machines shown in the following table.

Name	Application security group	Network security group (NSG)	Connected to	Public IP address
VM1	ASG1	NSG1	Subnet1	No
VM2	ASG2	NSG1	Subnet2	No
VM3	ASG2	NSG1	Subnet3	Yes
VM4	ASG4	NSG1	Subnet4	Yes

The firewalls on all the virtual machines allow ping traffic.  
NSG1 is configured as shown in the following exhibit.

Inbound security rules -

Priority	Name	Port	Protocol	Source	Destination	Action
110	Allow_RDP	3389	Any	Any	Any	Allow
130	Rule1	Any	Any	ASG1	Any	Allow
140	Rule2	Any	Any	ASG2	Any	Allow
150	Rule3	Any	Any	ASG4	Any	Allow
160	Rule4	Any	Any	Any	Any	Deny
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalan...	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

Outbound security rules -

Priority	Name	Port	Protocol	Source	Destination	Action
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowInternetOutBou...	Any	Any	Any	Internet	Allow
65500	DenyAllOutBound	Any	Any	Any	Any	Deny

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

Answer Area

Statements	Yes	No
VM1 can ping VM3 successfully.	<input type="radio"/>	<input type="radio"/>
VM2 can ping VM4 successfully.	<input type="radio"/>	<input type="radio"/>
VM3 can be accessed by using Remote Desktop from the internet.	<input type="radio"/>	<input type="radio"/>

Answer:

## Answer Area

Statements	Yes	No
VM1 can ping VM3 successfully.	<input checked="" type="radio"/>	<input type="radio"/>
VM2 can ping VM4 successfully.	<input type="radio"/>	<input checked="" type="radio"/>
VM3 can be accessed by using Remote Desktop from the internet.	<input checked="" type="radio"/>	<input type="radio"/>

### Explanation:

Box 1: Yes -

VM1 and VM3 are on peered VNets. The firewall rules with a source of ASG1 and ASG2 allow 'any' traffic on 'any' protocol so pings are allowed between VM1 and VM3.

Box 2: No -

VM2 and VM4 are on separate VNets and the VNets are not peered. Therefore, the pings would have to go over the Internet. VM4 does have a public IP and the firewall allows pings. However, for VM2 to be able to ping VM4, VM2 would also need a public IP address. In Azure, pings don't go out through the default gateway as they would in a physical network. For an Azure VM to ping external IPs, the VM must have a public IP address assigned to it.

Box 3: Yes -

VM3 has a public IP address and the firewall allows traffic on port 3389.

## Question: 221

CertyIQ

You have multiple development teams that will create apps in Azure.

You plan to create a standard development environment that will be deployed for each team.

You need to recommend a solution that will enforce resource locks across the development environments and ensure that the locks are applied in a consistent manner.

What should you include in the recommendation?

- A. an Azure policy
- B. an Azure Resource Manager template
- C. a management group
- D. an Azure blueprint

**Answer: D**

### Explanation:

Azure Blueprint

Reference: "

How blueprint locks work"

<https://docs.microsoft.com/en-us/azure/governance/blueprints/concepts/resource-locking>

<https://docs.microsoft.com/en-us/azure/governance/blueprints/concepts/resource-locking>

**Question: 222****CertyIQ**

You have an Azure Kubernetes Service (AKS) cluster that will connect to an Azure Container Registry. You need to use the automatically generated service principal for the AKS cluster to authenticate to the Azure Container Registry. What should you create?

- A. a secret in Azure Key Vault
- B. a role assignment
- C. an Azure Active Directory (Azure AD) user
- D. an Azure Active Directory (Azure AD) group

**Answer: B****Explanation:**

Reference:

<https://docs.microsoft.com/en-us/azure/aks/kubernetes-service-principal>**Question: 223****CertyIQ**

You have an Azure subscription that contains two virtual machines named VM1 and VM2 that run Windows Server 2019.

You are implementing Update Management in Azure Automation.

You plan to create a new update deployment named Update1.

You need to ensure that Update1 meets the following requirements:

- ⊞ Automatically applies updates to VM1 and VM2.
- ⊞ Automatically adds any new Windows Server 2019 virtual machines to Update1.

What should you include in Update1?

- A. a security group that has a Membership type of Assigned
- B. a security group that has a Membership type of Dynamic Device
- C. a dynamic group query
- D. a Kusto query language query

**Answer: C****Explanation:**

Update Management allows you to target a dynamic group of Azure or non-Azure VMs for update deployments. A dynamic group is defined by a query that Azure Automation evaluates at deployment time.

Reference:

<https://docs.microsoft.com/en-us/azure/automation/update-management/configure-groups>**Question: 224****CertyIQ**

You have the Azure virtual machines shown in the following table.

Name	Operating system	State
VM1	Windows Server 2012	Running
VM2	Windows Server 2012 R2	Running
VM3	Windows Server 2016	Stopped
VM4	Ubuntu Server 18.04 LTS	Running

For which virtual machines can you enable Update Management?

- A. VM2 and VM3 only
- B. VM2, VM3, and VM4 only
- C. VM1, VM2, and VM4 only
- D. VM1, VM2, VM3, and VM4
- E. VM1, VM2, and VM3 only

**Answer: C**

**Explanation:**

VM1, VM2, and VM4 only

Because the VM3 is stopped. If the VM3 is on, it will be VM1, VM2, VM3 and VM4

References:

<https://docs.microsoft.com/en-us/azure/automation/automation-update-management?toc=%2Fazure%2Fautomation%2Ftoc.json>

## Question: 225

CertyIQ

DRAG DROP -

You have an Azure subscription named Sub1.

You have an Azure Active Directory (Azure AD) group named Group1 that contains all the members of your IT team. You need to ensure that the members of Group1 can stop, start, and restart the Azure virtual machines in Sub1. The solution must use the principle of least privilege.

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**

**Answer Area**

Create a JSON file.

Run the Update-AzManagementGroup cmdlet.

Create an XML file.

Run the New-AzRoleDefinition cmdlet.

Run the New-AzRoleAssignment cmdlet.

**Answer:**



**Actions**

Run the Update-AzManagementGroup cmdlet.

Create an XML file.

**Answer Area**

Create a JSON file.

Run the New-AzRoleDefinition cmdlet.

Run the New-AzRoleAssignment cmdlet.

**Explanation:**

Create a json file that contains role definition (<https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-how-applications-are-added#what-are-service-principals-and-where-do-they-come-from>).

- Create a new role definition by running New-AzRoleDefinition -InputFile "C:\CustomRoles\customrole1.json" (<https://docs.microsoft.com/en-us/azure/role-based-access-control/custom-roles-powershell#create-a-custom-role-with-json-template>)

- Assigning a new role definition to the Group1 in subscription scope by running New-AzRoleAssignment <https://docs.microsoft.com/en-us/azure/role-based-access-control/role-assignments-powershell#step-4-assign-role>

**References:**

<https://www.petri.com/cloud-security-create-custom-rbac-role-microsoft-azure>

**Question: 226****CertyIQ****DRAG DROP -**

You have an Azure subscription that contains the following resources:

A virtual network named VNET1 that contains two subnets named Subnet1 and Subnet2.

■ A virtual machine named VM1 that has only a private IP address and connects to Subnet1.

⇒ You need to ensure that Remote Desktop connections can be established to VM1 from the internet.

You need to ensure that Remote Desktop connections can be established to VM1 from the internet. 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**

Configure a network security group (NSG).

Create a network rule collection.

Create a NAT rule collection.

Create a new subnet.

Deploy Azure Application Gateway.

Deploy Azure Firewall.

**Answer Area****Answer:**



**Actions****Answer Area****Question: 227****CertyIQ****HOTSPOT -**

You have an Azure subscription that is linked to an Azure Active Directory (Azure AD). The tenant contains the users shown in the following table.

Name	Role	Member of
User1	Security administrator	Group1
User2	Network Contributor	Group2
User3	Key Vault Contributor	Group1, Group2

You have an Azure key vault named Vault1 that has Purge protection set to Disable. Vault1 contains the access policies shown in the following table.

Name	Key permission	Secret permission	Certificate permission
Group1	Purge	Purge	Purge
Group2	Select all	Select all	Select all

You create role assignments for Vault1 as shown in the following table.

Name	Role
User1	None
User2	Key Vault Reader
User3	User Access Administrator

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

NOTE: Each correct selection is worth one point.

Hot Area:

Statements	Yes	No
User1 can set Purge protection to Enable for Vault1.	<input type="radio"/>	<input type="radio"/>
User2 can configure firewalls and virtual networks for Vault1.	<input type="radio"/>	<input type="radio"/>
User3 can add access policies to Vault1.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
User1 can set Purge protection to Enable for Vault1.	<input type="radio"/>	<input checked="" type="radio"/>
User2 can configure firewalls and virtual networks for Vault1.	<input type="radio"/>	<input checked="" type="radio"/>
User3 can add access policies to Vault1.	<input checked="" type="radio"/>	<input type="radio"/>

Explanation:

Box 1: No -

Resource Policy Contributor or Security Administrator is required.

User1 is Security Administrator only with the no specific permission granted to Vault1.

The Security Admin can view and update permissions for Security Center. Same permissions as the Security Reader role and can also update the security policy and dismiss alerts and recommendations.

However:

Last but not least, you need to have the appropriate permissions to assign the **Contributor** role for the **Managed Identity** (Application ID) created during the assignment of the policy either on a management group or a subscription, so the policy with “**DeployIfNotExists**” can remediate and modify your Key Vault settings. Azure Policy creates a managed identity for each assignment but must have details about what roles to grant the managed identity.

Box 2:no

Network Contributor or Key Vault Reader cannot change the key vault firewall

<https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-role>

Box 3: Yes -

User3 is a Key Vault Contributor and a User Access Administrator for Vault.

The Key Vault Contributor role allows you to manage key vaults, but does not allow you to assign roles in Azure RBAC, and does not allow you to access secrets, keys, or certificates.

## Question: 228

CertyIQ

HOTSPOT

-

You have an Azure subscription that contains the virtual machines shown in the following table.

Name	Azure region	Connected to	Associated network security group (NSG)
VM1	West US	VNET1/Subnet1	None
VM2	West US	VNET1/Subnet2	NSG2
VM3	Central US	VNET2/Subnet1	NSG3
VM4	West US	VNET3/Subnet1	NSG4

VNET1, VNET2, and VNET3 are peered with each other.

You perform the following actions:

- Create two application security groups named ASG1 and ASG2 in the West US region.
- Add the network interface of VM1 to ASG1.

The network interfaces of which virtual machines can you add to ASG1 and ASG2? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

## Answer Area

ASG1:  ▼

VM2 only

VM2 and VM4 only

VM2, VM3, and VM4 only

ASG2:  ▼

VM2 and VM4 only

VM1, VM2, and VM4 only

VM2, VM3, and VM4 only

VM1, VM2, VM3, and VM4

Answer:

## Answer Area

ASG1:  ▼

- VM2 only
- VM2 and VM4 only
- VM2, VM3, and VM4 only

ASG2:  ▼

- VM2 and VM4 only
- VM1, VM2, and VM4 only
- VM2, VM3, and VM4 only
- VM1, VM2, VM3, and VM4

### Explanation:

ASG1: VM2 only

ASG2: VM1, VM2, VM4

A Virtual Machine can be attached to more than one Application Security Group. This helps in cases of multi-application servers.

There are only two requirements:

- All network interfaces used in an ASG must be within the same VNet
- If ASGs are used in the source and destination, they must be within the same VNet

### Question: 229

CertyIQ

You have an Azure subscription that contains an Azure key vault.

You need to configure the maximum number of days for which new keys are valid. The solution must minimize administrative effort.

What should you use?

- A. Azure Purview
- B. Key Vault properties
- C. Azure Blueprints
- D. Azure Policy

**Answer: D**

**Explanation:**

Azure Built-in policy name: Keys should not be active for longer than the specified number of day

Specify the number of days that a key should be active. Keys that are used for an extended period of time increase the probability that an attacker could compromise the key. As a good security practice, make sure that your keys have not been active longer than two years

Azure Policy built-in definitions for Key Vault

Reference:

<https://learn.microsoft.com/en-us/azure/key-vault/policy-reference>

### Question: 230

CertyIQ

You have an Azure subscription that contains an Azure Data Lake Storage Gen2 account named storage1.

You deploy an Azure Synapse Analytics workspace named synapsews1 to a managed virtual network.

You need to enable access from synapsews1 to storage1.

What should you configure?

- A. peering
- B. a private endpoint
- C. a network security group (NSG)
- D. a virtual network gateway

**Answer: B**

**Explanation:**

Managed private endpoints are private endpoints created in a Managed Virtual Network associated with your Azure Synapse workspace. Managed private endpoints establish a private link to Azure resources. Azure Synapse manages these private endpoints on your behalf. You can create Managed private endpoints from your Azure Synapse workspace to access Azure services (such as Azure Storage or Azure Cosmos DB) and Azure hosted customer/partner services.

Reference

Synapse Managed private endpoints

<https://learn.microsoft.com/en-us/azure/synapse-analytics/security/synapse-workspace-managed-private-endpoints>

### Question: 231

CertyIQ

You have a Microsoft Entra tenant named Contoso.com and an Azure Kubernetes Service (AKS) cluster AKS1.

You discover that AKS1 cannot be accessed by using accounts from Contoso.com.

You need to ensure AKS1 can be accessed by using accounts from Contoso.com. The solution must minimize administrative effort.

What should you do first?

- A.From Azure, recreate AKS1.
- B.From AKS1, upgrade the version of Kubernetes.
- C.From Microsoft Entra, add a Microsoft Entra ID P2 license.
- D.From Microsoft Entra, configure the User settings.

**Answer: A**

**Explanation:**

From Azure, recreate AKS1.

## Question: 232

CertyIQ

SIMULATION

-

You need to ensure that the events in the NetworkSecurityGroupRuleCounter log of the VNET01-Subnet0-NSG network security group (NSG) are stored in the logs1234578 Azure Storage account.

To complete this task, sign in to the Azure portal.

**Answer:**



You need to configure the diagnostic logging for the NetworkSecurityGroupRuleCounter log.

#### Alternative 1:

##### Enable logging

You can use the Azure portal, Azure PowerShell, or the Azure CLI to enable resource logging.

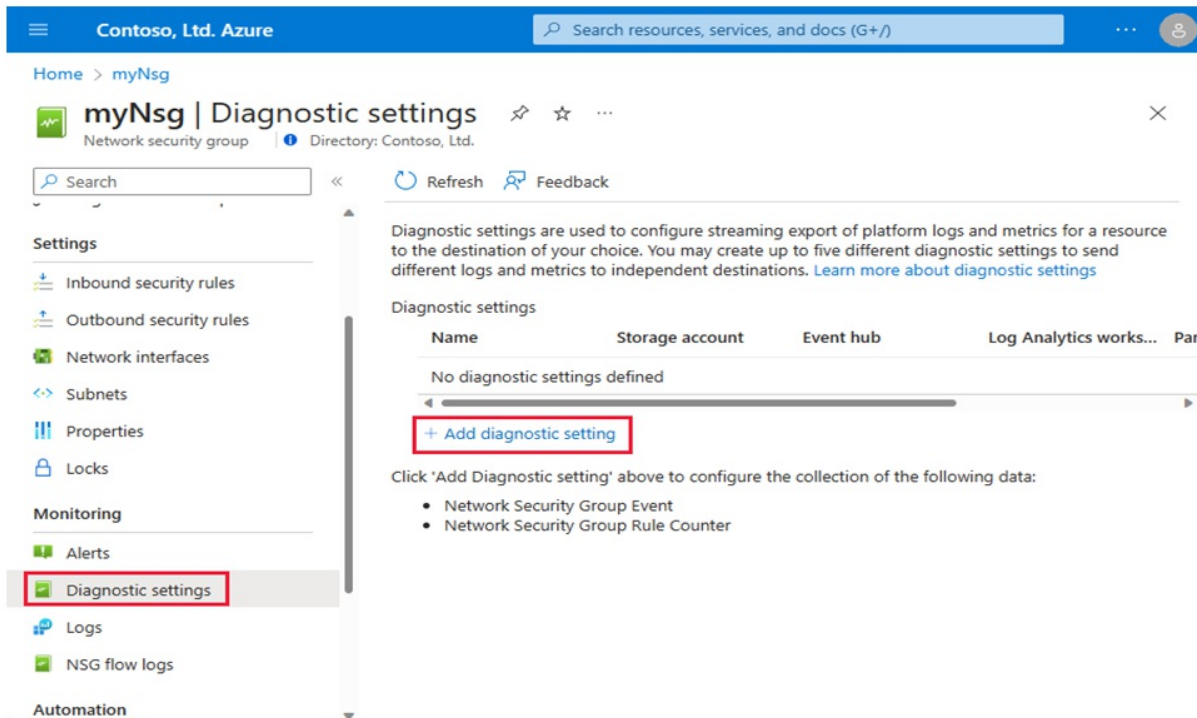
#### Azure portal

Step 1: Sign in to the Azure portal.

Step 2: In the search box at the top of the Azure portal, enter network security groups. Select Network security groups in the search results.

Step 3: Select the NSG for which to enable logging. Here select: VNET01-Subnet0-NSG

Step 4: Under Monitoring, select Diagnostic settings, and then select Add diagnostic setting:



Step 5: In Diagnostic setting, enter a name, such as myNsgDiagnostic.

Step 6: For Logs, select the **NetworkSecurityGroupRuleCounter** log .

Step 7: Under Destination details, select one or more destinations:

Send to Log Analytics workspace

\*-> Archive to a storage account (Select this one!)

Stream to an event hub

Send to partner solution

Step 8: In the **Storage account** field, select the **logs1234578** storage account.

Step 9: Click the **Save** button to save the changes.

#### Alternative 2:


1. In the Azure portal, type **Network Security Groups** in the search box, select **Network Security Groups** from the search results then select **VNET01-Subnet0-NSG**. Alternatively, browse to Network Security Groups in the left navigation pane.
2. In the properties of the Network Security Group, click on **Diagnostic Settings**.
3. Click on the **Add diagnostic setting** link.
4. Provide a name in the **Diagnostic settings name** field. It doesn't matter what name you provide for the exam.
5. In the **Log** section, select **NetworkSecurityGroupRuleCounter**.
6. In the **Destination details** section, select **Archive to a storage account**.
7. In the **Storage account** field, select the **logs1234578** storage account.
8. Click the **Save** button to save the changes.

#### Reference:

<https://learn.microsoft.com/en-us/azure/virtual-network/manage-network-security-group>

You are testing an Azure Kubernetes Service (AKS) cluster. The cluster is configured as shown in the exhibit. (Click the Exhibit tab.)

# Create Kubernetes cluster ...

 Validation passed

## Basics

Subscription	Visual Studio Enterprise Subscription
Resource group	RG1
Region	East US
Kubernetes cluster name	AKScluster
Kubernetes version	1.24.6
Automatic upgrade	Patch

## Node pools

Node pools	1
Enable virtual nodes	Disabled

## Access

Resource identity	System-assigned managed identity
Local accounts	Enabled
Authentication and Authorization	Local accounts with Kubernetes RBAC
Encryption type	(Default) Encryption at-rest with a platform-managed key

## Networking

Network configuration	Kubenet
DNS name prefix	AKScluster-dns
Load balancer	Standard
Private cluster	Disabled
Authorized IP ranges	Disabled
Network policy	None
HTTP application routing	No

You plan to deploy the cluster to production. You disable HTTP application routing.

You need to implement application routing that will provide reverse proxy and TLS termination for AKS services by using a single IP address.

What should you do?

- A.Create an AKS Ingress controller.
- B.Create an Azure Standard Load Balancer.
- C.Install the container network interface (CNI) plug-in.
- D.Create an Azure Basic Load Balancer.

**Answer: A**

**Explanation:**

An Ingress controller is typically used to manage external access to services in a Kubernetes cluster, usually via HTTP/HTTPS, and it can provide reverse proxy and TLS termination. It enables routing traffic to services based on the URL and can handle requests coming into the cluster using a single public IP.This option fits the requirements well as an Ingress controller supports reverse proxying and TLS termination.

### Question: 234

CertyIQ

You have an Azure subscription that contains a virtual network named VNet1. VNet1 contains the subnets shown in the following table.

Name	Has an associated network security group (NSG)
Subnet1	Yes
Subnet2	Yes
Subnet3	No
Subnet4	No

You create the virtual machines shown in the following table.

Name	Has an NSG associated to a network interface	Connected to
VM1	Yes	Subnet1
VM2	No	Subnet2
VM3	Yes	Subnet3
VM4	No	Subnet4

You plan to configure just-in-time (JIT) VM access for the virtual machines. The solution must minimize administrative effort.

For which virtual machines can you configure JIT VM access?

- A.VM1 only

- B.VM1 and VM2 only
- C.VM1 and VM3 only
- D.VM1, VM2, and VM3 only
- E.VM1, VM2, VM3, and VM4

**Answer: D**

**Explanation:**

VM1, VM2, and VM3 only.

**Question: 235**

**CertyIQ**

HOTSPOT

-

You have an Azure subscription.

You plan to deploy the virtual machines shown in the following table.

Name	Size	Operating system
VM1	DC4ads_v5	Windows Server 2022 Datacenter: Azure Edition
VM2	D2ads_v5	Windows Server 2022 Standard
VM3	EC4ads_v5	Windows Server 2022 Datacenter
VM4	D2ads_v5	Debian
VM5	EC4ads_v5	Ubuntu Server
VM6	DC4ads_v5	SUSE Linux Enterprise Server

You need to identify the virtual machines and operating systems that can be deployed as confidential virtual machines?

Which Windows virtual machines and which Linux virtual machines should you identify?

## Answer Area

Windows:

▼

VM1 only  
VM3 only  
VM1 and VM2 only  
VM1 and VM3 only  
VM1, VM2 and VM3

Linux:

▼

VM5 only  
VM6 only  
VM4 and VM6 only  
VM5 and VM6 only  
VM4, VM5 and VM6

Answer:

## Answer Area

Windows:

▼

VM1 only  
VM3 only  
VM1 and VM2 only  
VM1 and VM3 only  
VM1, VM2 and VM3

Linux:

▼

VM5 only  
VM6 only  
VM4 and VM6 only  
VM5 and VM6 only  
VM4, VM5 and VM6

### Question: 236

HOTSPOT -

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



Name	Type	Resource group
RG1	Resource group	Not applicable
RG2	Resource group	Not applicable
RG3	Resource group	Not applicable
SQL1	Azure SQL Database	RG3

Transparent Data Encryption (TDE) is disabled on SQL1.  
You assign policies to the resource groups as shown in the following table.

Name	Condition	Effect if condition is false	Assignment
Policy1	TDE enabled	Deny	RG1, RG2
Policy2	TDE enabled	DeployIfNotExists	RG2, RG3
Policy3	TDE enabled	Audit	RG1

You plan to deploy Azure SQL databases by using an Azure Resource Manager (ARM) template. The databases will be configured as shown in the following table.

Name	Resource group	TDE
SQL2	RG2	Disabled
SQL3	RG1	Disabled

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

Answer Area

Statements	Yes	No
SQL1 will have TDE enabled automatically.	<input type="radio"/>	<input type="radio"/>
The deployment of SQL2 will fail.	<input type="radio"/>	<input type="radio"/>
SQL3 will be deployed and marked as noncompliant.	<input type="radio"/>	<input type="radio"/>



Answer:

## Answer Area

### Statements

Yes

No

SQL1 will have TDE enabled automatically.

☐☒

The deployment of SQL2 will fail.

☒☐

SQL3 will be deployed and marked as noncompliant.

☐☒

### Explanation:

After the Resource Provider returns a success code on a Resource Manager mode request, AuditIfNotExists and DeployIfNotExists evaluate to determine whether additional compliance logging or action is required.

So overall order of evaluation: Disabled -> Append/Modify -> Deny -> Audit -> AuditIfNotExists/DeployIfNotExists.

1st: No. DeployIfNotExists will be triggered after a configurable delay when a Resource Provider handles a create or update subscription or resource request and has returned a success code. In this scenario, because SQL1 is already deployed so it can not be enabled automatically.

2nd: Yes. Deny is processed first so can't be deployed

3rd: No. Deny is processed first

Reference:

<https://learn.microsoft.com/en-us/azure/governance/policy/concepts/effects>

### Question: 237

CertyIQ

HOTSPOT -

You have an Azure subscription named Sub1. Sub1 has an Azure Storage account named storage1 that contains the resources shown in the following table.

Name	Type
Container1	Blob container
Share1	File share

You generate a shared access signature (SAS) to connect to the blob service and the file service. Which tool can you use to access the contents in Container1 and Share1 by using the SAS? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

## Answer Area

Tools for Container1:

	▼
Robocopy.exe	
Azure Storage Explorer	
File Explorer	

Tools for Share1:

	▼
Robocopy.exe	
Azure Storage Explorer	
File Explorer	

Answer:

## Answer Area

Tools for Container1:

	▼
Robocopy.exe	
Azure Storage Explorer	
File Explorer	

Tools for Share1:

	▼
Robocopy.exe	
Azure Storage Explorer	
File Explorer	

### Question: 238

CertyIQ

You have an Azure Storage account named storage1 that has a container named container1. You need to prevent the blobs in container1 from being modified. What should you do?

- A. From container1, change the access level.
- B. From container1, add an access policy.
- C. From container1, modify the Access Control (IAM) settings.
- D. From storage1, enable soft delete for blobs.

Answer: B

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blob-immutable-storage?tabs=azure-portal>

### Question: 239

CertyIQ

Your company has an Azure Active Directory (Azure AD) tenant named contoso.com. You plan to create several security alerts by using Azure Monitor. You need to prepare the Azure subscription for the alerts. What should you create first?

- A. an Azure Storage account
- B. an Azure Log Analytics workspace
- C. an Azure event hub
- D. an Azure Automation account

**Answer: B**

**Explanation:**

basically, you need LAW to store the security-related logs and use Kusto to query the logs. Base on the result of query, create security alert. Therefore, you have to create LAW first.

### Question: 240

CertyIQ

You company has an Azure subscription named Sub1. Sub1 contains an Azure web app named WebApp1 that uses Azure Application Insights. WebApp1 requires users to authenticate by using OAuth 2.0 client secrets. Developers at the company plan to create a multi-step web test app that preforms synthetic transactions emulating user traffic to Web App1. You need to ensure that web tests can run unattended. What should you do first?

- A. In Microsoft Visual Studio, modify the .webtest file.
- B. Upload the .webtest file to Application Insights.
- C. Register the web test app in Azure AD.
- D. Add a plug-in to the web test app.

**Answer: C**

**Explanation:**

The context of the question is from a Security/Access/Identities perspective, and not from developer's perspective. Check the answer here, section "Client Secret":

<https://docs.microsoft.com/en-us/azure/azure-monitor/app/availability-multistep#dealing-with-sign-in>

### Question: 241

CertyIQ

You have an Azure subscription named Subscription1. You deploy a Linux virtual machine named VM1 to Subscription1. You need to monitor the metrics and the logs of VM1. What should you use?

- A. the AzurePerformanceDiagnostics extension
- B. Azure HDInsight
- C. Linux Diagnostic Extension (LAD) 3.0
- D. Azure Analysis Services

**Answer: C**

**Explanation:**

Use the Linux diagnostic extension 4.0 to monitor metrics and logs

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-machines/extensions/diagnostics-linux>

**Question: 242**

**CertyIQ**

You onboard Azure Sentinel. You connect Azure Sentinel to Azure Security Center. You need to automate the mitigation of incidents in Azure Sentinel. The solution must minimize administrative effort.

What should you create?

- A. an alert rule
- B. a playbook
- C. a function app
- D. a runbook

**Answer: B**

**Explanation:**

A playbook can help automate and orchestrate your response, and can be set to run automatically when specific alerts or incidents are generated, by being attached to an analytics rule or an automation rule, respectively"

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook>

**Question: 243**

**CertyIQ**

You have an Azure Active Directory (Azure AD) tenant named contoso.com.

You need to configure diagnostic settings for contoso.com. The solution must meet the following requirements:

- ⇒ Retain logs for two years.
- ⇒ Query logs by using the Kusto query language.
- ⇒ Minimize administrative effort.

Where should you store the logs?

- A. an Azure event hub
- B. an Azure Log Analytics workspace
- C. an Azure Storage account

**Answer: B**

**Explanation:**

Data retention at the workspace level can be configured from 30 to 730 days (2 years) for all workspaces unless they are using the legacy Free pricing tier.

**Question: 244****CertyIQ**

You are troubleshooting a security issue for an Azure Storage account.  
You enable the diagnostic logs for the storage account.  
What should you use to retrieve the diagnostics logs?

- A. the Security & Compliance admin center
- B. Azure Security Center
- C. Azure Cosmos DB explorer
- D. AzCopy

**Answer: D****Explanation:**

If you want to download the metrics for long-term storage or to analyze them locally, you must use a tool or write some code to read the tables. You must download the minute metrics for analysis. The tables do not appear if you list all the tables in your storage account, but you can access them directly by name.

Many storage-browsing tools are aware of these tables and enable you to view them directly (see Azure Storage Client Tools for a list of available tools).

Microsoft provides several graphical user interface (GUI) tools for working with the data in your Azure Storage account. All of the tools outlined in the following table are free.

Azure Storage client tool	Supported platforms	Block Blob	Page Blob	Append Blob	Tables	Queues	Files
Azure portal	Web	Yes	Yes	Yes	Yes	Yes	Yes
Azure Storage Explorer	Windows, OSX	Yes	Yes	Yes	Yes	Yes	Yes
Microsoft Visual Studio Cloud Explorer	Windows	Yes	Yes	Yes	Yes	Yes	No

Note:

There are several versions of this question in the exam. The questions in the exam have two different correct answers:

1. Azure Storage Explorer
2. AZCopy

Other incorrect answer options you may see on the exam include the following:

1. SQL query editor in Azure
2. File Explorer in Windows
3. Azure Monitor

Reference:

<https://docs.microsoft.com/en-us/azure/storage/common/storage-analytics-metrics?toc=%2fazure%2fstorage%2fblobs%2ftoc.json> <https://docs.microsoft.com/en-us/azure/storage/common/storage-explorers>

**Question: 245**

You have an Azure subscription that contains the virtual machines shown in the following table.

Name	Operating system
VM1	Windows Server 2016
VM2	Ubuntu Server 18.04 LTS

From Azure Security Center, you turn on Auto Provisioning.  
You deploy the virtual machines shown in the following table.

Name	Operating system
VM3	Windows Server 2016
VM4	Ubuntu Server 18.04 LTS

On which virtual machines is the Microsoft Monitoring Agent installed?

- A. VM3 only
- B. VM1 and VM3 only
- C. VM3 and VM4 only
- D. VM1, VM2, VM3, and VM4

**Answer: D**

**Explanation:**

When automatic provisioning is enabled, Security Center provisions the Microsoft Monitoring Agent on all supported Azure VMs and any new ones that are created.

Supported Operating systems include: Ubuntu 14.04 LTS (x86/x64), 16.04 LTS (x86/x64), and 18.04 LTS (x64) and Windows Server 2008 R2, 2012, 2012 R2, 2016, version 1709 and 1803.

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/security-center-faq>

**Question: 246**

SIMULATION -

You need to email an alert to a user named [email protected] if the average CPU usage of a virtual machine named VM1 is greater than 70 percent for a period of 15 minutes.

To complete this task, sign in to the Azure portal.

**Answer:**

See the explanation below.

**Explanation:**

Create an alert rule on a metric with the Azure portal

1. In the portal, locate the resource, here VM1, you are interested in monitoring and select it.
2. Select Alerts (Classic) under the MONITORING section. The text and icon may vary slightly for different resources.
3. Select the Add metric alert (classic) button and fill in the fields as per below, and click OK.



Metric: CPU Percentage -

Condition: Greater than -

Period: Over last 15 minutes -

Notify via: email -

Additional administrator email(s): [email protected]

The screenshot shows the configuration for an Azure Monitor alert. It includes a dropdown for 'Condition' set to 'Greater than', a 'Threshold' input field with the value '60' and a percentage symbol, a 'Period' dropdown set to 'Over the last 5 minutes', a 'Notify via' section with a checked checkbox for 'Email owners, contributors, and readers', an 'Additional administrator email(s)' input field with the value 'admin@contoso.com', and a 'Webhook' input field with the value 'http://www.contoso.com/dowork?param'. Each input field has a green checkmark on the right side, indicating it is valid.

Reference:

<https://docs.microsoft.com/en-us/azure/sql-database/sql-database-insights-alerts-portal>

## Question: 247

CertyIQ

SIMULATION -

You need to collect all the audit failure data from the security log of a virtual machine named VM1 to an Azure Storage account.

To complete this task, sign in to the Azure portal.

This task might take several minutes to complete. You can perform other tasks while the task completes.

### Answer:

See the explanation below.

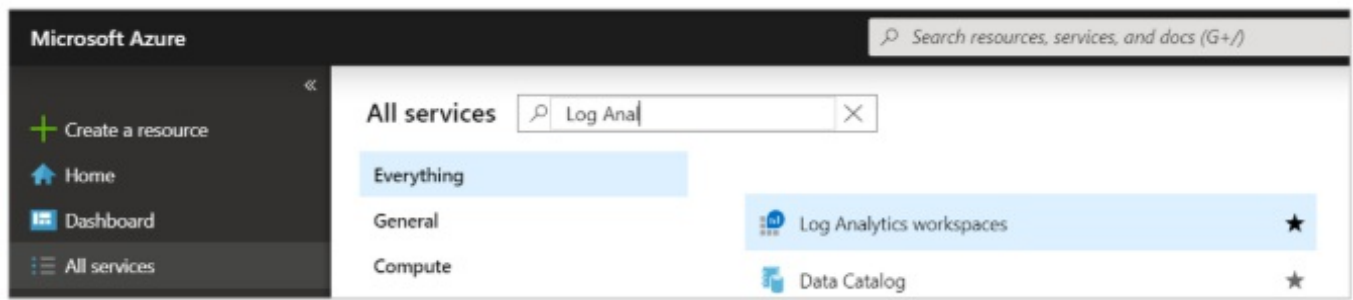
### Explanation:

Step 1: Create a workspace -

Azure Monitor can collect data directly from your Azure virtual machines into a Log Analytics workspace for detailed analysis and correlation.

1. In the Azure portal, select All services. In the list of resources, type Log Analytics. As you begin typing, the

list filters based on your input. Select Log Analytics workspaces.



2. Select Create, and then select choices for the following items:

A screenshot of the 'Log Analytics workspace' creation form in the Azure portal. The form has a title 'Log Analytics workspace' and a subtitle 'Create new or link existing workspace'. There are two radio buttons: 'Create New' (selected) and 'Link Existing'. Below this, there are four required fields marked with a red asterisk: 'Log Analytics Workspace' (with an information icon), 'Subscription', 'Resource group', and 'Location'. Each field has a dropdown menu. The 'Log Analytics Workspace' dropdown shows 'DefaultLAWorkspace' with a green checkmark. The 'Subscription' dropdown shows 'Microsoft Azure'. The 'Resource group' dropdown shows 'Prod'. The 'Location' dropdown shows 'East US'. Below the 'Resource group' dropdown, there is a link 'Create new'. At the bottom, there is a 'Pricing tier' dropdown showing 'Per GB (2018)' with a right arrow icon.

3. After providing the required information on the Log Analytics workspace pane, select OK. While the information is verified and the workspace is created, you can track its progress under Notifications from the menu.

Step 2: Enable the Log Analytics VM Extension

Installing the Log Analytics VM extension for Windows and Linux allows Azure Monitor to collect data from your Azure VMs.

1. In the Azure portal, select All services found in the upper left-hand corner. In the list of resources, type Log Analytics. As you begin typing, the list filters based on your input. Select Log Analytics workspaces.

2. In your list of Log Analytics workspaces, select DefaultWorkspace (the name you created in step 1).

3. On the left-hand menu, under Workspace Data Sources, select Virtual machines.
  4. In the list of Virtual machines, select a virtual machine you want to install the agent on. Notice that the Log Analytics connection status for the VM indicates that it is Not connected.
  5. In the details for your virtual machine, select Connect. The agent is automatically installed and configured for your Log Analytics workspace. This process takes a few minutes, during which time the Status shows Connecting.
- After you install and connect the agent, the Log Analytics connection status will be updated with This workspace.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-monitor/learn/quick-collect-azurevm>

### Question: 248

CertyIQ

You have 10 virtual machines on a single subnet that has a single network security group (NSG). You need to log the network traffic to an Azure Storage account. What should you do?

- A. Install the Network Performance Monitor solution.
- B. Create an Azure Log Analytics workspace.
- C. Enable diagnostic logging for the NSG.
- D. Enable NSG flow logs.

**Answer: D**

#### Explanation:

A network security group (NSG) enables you to filter inbound traffic to, and outbound traffic from, a virtual machine (VM). You can log network traffic that flows through an NSG with Network Watcher's NSG flow log capability. Steps include:

- Create a VM with a network security group
- Enable Network Watcher and register the Microsoft.Insights provider
- Enable a traffic flow log for an NSG, using Network Watcher's NSG flow log capability
- Download logged data

View logged data -

■

Reference:

<https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-nsg-flow-logging-portal>

### Question: 249

CertyIQ

You have an Azure subscription that contains the virtual machines shown in the following table.

Name	Operating system
VM1	Windows Server 2016
VM2	Ubuntu Server 18.04 LTS

From Azure Security Center, you turn on Auto Provisioning. You deploy the virtual machines shown in the following table.

Name	Operating system
VM3	Windows Server 2016
VM4	Ubuntu Server 18.04 LTS

On which virtual machines is the Log Analytics Agent installed?

- A. VM3 only
- B. VM1 and VM3 only
- C. VM3 and VM4 only
- D. VM1, VM2, VM3, and VM4

**Answer: D**

**Explanation:**

When automatic provisioning is On, Security Center provisions the Log Analytics Agent on all supported Azure VMs and any new ones that are created.

Supported Operating systems include: Ubuntu 14.04 LTS (x86/x64), 16.04 LTS (x86/x64), and 18.04 LTS (x64) and Windows Server 2008 R2, 2012, 2012 R2, 2016, version 1709 and 1803

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/security-center-enable-data-collection>

**Question: 250**

**CertyIQ**

HOTSPOT -

You plan to use Azure Log Analytics to collect logs from 200 servers that run Windows Server 2016.

You need to automate the deployment of the Microsoft Monitoring Agent to all the servers by using an Azure Resource Manager template.

How should you complete the template? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

## Answer Area

```
{
  "type" : "Microsoft.Compute/virtualMachines/extensions",
  "name" : "[concat(parameter('vmname'), /OMSExtension)]",
  "apiVersion" : "[variables('apiVersion')]",
  "location" : "[resourceGroup().location]",
  "dependsOn" : [
    "[concat('Microsoft.Compute/virtualMachines/', parameters('vmName'))]"
  ],
  "properties" : {
    "publisher" : "Microsoft.EnterpriseCloud.Monitoring",
    "type" : "MicrosoftMonitoringAgent",
    "typeHandlerVersion" : "1.0",
    "autoUpgradeMinorVersion" : true,
    "settings" : {
      

|                        |   |                        |
|------------------------|---|------------------------|
|                        | ▼ | : "[variable('var1')]" |
| "AzureADApplicationID" |   |                        |
| "WorkspaceID"          |   |                        |
| "WorkspaceName"        |   |                        |
| "WorkspaceURL"         |   |                        |


    },
    "protectedSettings" : {
      

|                            |   |                         |
|----------------------------|---|-------------------------|
|                            | ▼ | : "[variable ('var2')]" |
| "AzureADApplicationSecret" |   |                         |
| "StorageAccountKey"        |   |                         |
| "WorkspaceID"              |   |                         |
| "WorkspaceKey"             |   |                         |


    }
  }
}
```

Answer:

## Answer Area

```
{
  "type" : "Microsoft.Compute/virtualMachines/extensions",
  "name" : "[concat(parameter('vmname'), /OMSExtension)]",
  "apiVersion" : "[variables('apiVersion')]",
  "location" : "[resourceGroup().location]",
  "dependsOn" : [
    "[concat('Microsoft.Compute/virtualMachines/', parameters('vmName'))]"
  ],
  "properties" : {
    "publisher" : "Microsoft.EnterpriseCloud.Monitoring",
    "type" : "MicrosoftMonitoringAgent",
    "typeHandlerVersion" : "1.0",
    "autoUpgradeMinorVersion" : true,
    "settings" : {
      

|                        |   |                        |
|------------------------|---|------------------------|
|                        | ▼ | : "[variable('var1')]" |
| "AzureADApplicationID" |   |                        |
| "WorkspaceID"          |   |                        |
| "WorkspaceName"        |   |                        |
| "WorkspaceURL"         |   |                        |


    },
    "protectedSettings" : {
      

|                            |   |                         |
|----------------------------|---|-------------------------|
|                            | ▼ | : "[variable ('var2')]" |
| "AzureADApplicationSecret" |   |                         |
| "StorageAccountKey"        |   |                         |
| "WorkspaceID"              |   |                         |
| "WorkspaceKey"             |   |                         |


    }
  }
}
```

### Explanation:

#### Reference:

<https://blogs.technet.microsoft.com/manageabilityguys/2015/11/19/enabling-the-microsoft-monitoring-agent-in-windows-json-templates/>

## Question: 251

CertyIQ

### HOTSPOT -

You have an Azure subscription that contains the alerts shown in the following exhibit.



## All Alerts



+ New alert rule   Edit columns   Manage alert rules   View classic alerts   Refresh   Change state

Don't see a subscription? [Open Directory + Subscription settings](#)

* Subscription ⓘ Azure Pass - Sponsorship ▼	Resource group ⓘ Type to start filtering ... ▼	Resource type ⓘ 0 selected ▼	Resource ⓘ Type to start filtering ... ▼	Time range ⓘ Past hour ▼
Monitor service ⓘ 15 selected ▼	Monitor condition ⓘ 2 selected ▼	Severity ⓘ Sev 4 ▼	Alert state ⓘ 3 selected ▼	Smart group id ⓘ Smart group id

All Alerts   Alerts By Smart Group (Preview)

Search by name (case-insensitive)										
NAME	SEVERITY	MONITOR C...	ALERT STATE	AFFECT...	MONITOR SERV...	SIGNAL TYPE	FIRE TIME	SU...		
Alert1	Sev4	Fired	New		ActivityLog Ad...	Log	6/6/2019, 11:23:53 ...	Azure ...		
Alert1	Sev4	Fired	Acknowledged		ActivityLog Ad...	Log	6/6/2019, 11:23:52 ...	Azure ...		
Alert2	Sev4	Fired	Acknowledged		ActivityLog Ad...	Log	6/6/2019, 11:23:25 ...	Azure ...		
Alert2	Sev4	Fired	Closed		ActivityLog Ad...	Log	6/6/2019, 11:23:24 ...	Azure ...		

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

NOTE: Each correct selection is worth one point.

Hot Area:

### Answer Area

The state of Alert1 that was fired at 11:23:52

	▼
cannot be changed	
can be changed to Closed only	
can be changed to New only	
can be changed to New or Closed	

The state of Alert2 that was fired at 11:23:24

	▼
cannot be changed	
can be changed to Acknowledged only	
can be changed to New only	
can be changed to New or Acknowledged	

Answer:

## Answer Area

The state of Alert1 that was fired at 11:23:52

	▼
cannot be changed	
can be changed to Closed only	
can be changed to New only	
can be changed to New or Closed	

The state of Alert2 that was fired at 11:23:24

	▼
cannot be changed	
can be changed to Acknowledged only	
can be changed to New only	
can be changed to New or Acknowledged	

### Explanation:

the alert state can be changed to any of the alternate options, so Alert1 @ 11:23:52 which has the state of Acknowledged can be changed to New or Closed. Alert2 @ 11:23:24 with the state of Closed can be changed to New or Acknowledged.

### Question: 252

CertyIQ

You have an Azure subscription named Sub1 that is associated to an Azure Active Directory (Azure AD) tenant named contoso.com.  
You are assigned the Global administrator role for the tenant. You are responsible for managing Azure Security Center settings.  
You need to create a custom sensitivity label.  
What should you do?

- A. Create a custom sensitive information type.
- B. Elevate access for global administrators in Azure AD.
- C. Upgrade the pricing tier of the Security Center to Standard.
- D. Enable integration with Microsoft Cloud App Security.

### Answer: A

### Explanation:

First, you need to create a new sensitive information type because you can't directly modify the default rules.

Reference:

<https://docs.microsoft.com/en-us/office365/securitycompliance/customize-a-built-in-sensitive-information-type>

### Question: 253

CertyIQ

HOTSPOT -

You have the hierarchy of Azure resources shown in the following exhibit.



You create the Azure Blueprints definitions shown in the following table.

Name	Published at
Blueprint1	Tenant Root Group
Blueprint2	Subscription1

To which objects can you assign Blueprint1 and Blueprint2? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

## Answer Area

Blueprint1:

ManagementGroup1 only
ManagementGroup1, Subscription1, and RG1 only
ManagementGroup1, Subscription1, RG1, and VM1
Subscription1 only
Tenant Root Group only
Tenant Root Group, ManagementGroup1, and Subscription1 only

Blueprint2:

ManagementGroup1 only
Subscription1 and RG1 only
Subscription1 only
Subscription1, RG1, and VM1

Answer:

### Answer Area

Blueprint1:

ManagementGroup1 only
ManagementGroup1, Subscription1, and RG1 only
ManagementGroup1, Subscription1, RG1, and VM1
Subscription1 only
Tenant Root Group only
Tenant Root Group, ManagementGroup1, and Subscription1 only

Blueprint2:

ManagementGroup1 only
Subscription1 and RG1 only
Subscription1 only
Subscription1, RG1, and VM1

Explanation:

"Each Published Version of a blueprint can be assigned to an existing management group or subscription."

Blueprint1: Tenant Root Group, ManagementGroup1, and Subscription 1 only

**Question: 254**

CertyIQ

You have an Azure subscription that contains the Azure Log Analytics workspaces shown in the following table.

Name	Location	Description
Workspace1	East US	Used by Azure Sentinel
Workspace2	West US	<i>Not applicable</i>

You create the virtual machines shown in the following table.

Name	Location	Operating system	Connected to
VM1	East US	Windows Server 2019	<i>None</i>
VM2	East US	Windows Server 2019	Workspace2
VM3	West US	Windows Server 2019	<i>None</i>
VM4	West US	Windows Server 2019	Workspace2

You plan to use Azure Sentinel to monitor Windows Defender Firewall on the virtual machines.

Which virtual machines you can connect to Azure Sentinel?

- A. VM1 only
- B. VM1 and VM3 only
- C. VM1, VM2, VM3, and VM4
- D. VM1 and VM2 only

**Answer: C****Explanation:**

Azure Sentinel is built on top of a Log Analytics workspace(ref: <https://docs.microsoft.com/en-us/azure/sentinel/extend-sentinel-across-workspaces-tenants>). Windows Firewall requires a Log Analytics Agent(or MMA) which again logs to a log analytic workspace. Although at first it might appear that only VM1 and VM3 can be monitored by Sentinel, it is not correct. VM2 and VM4 can be monitored by Sentinel too by simply configuring the Log Analytics Agent to forward to Workspace1 in addition to Workspace2. If the machines were Linux VMs rather than Windows VMs this wouldn't be possible as multi-homing Linux VMs to multiple Log Analytics workspace is not supported( this limitation goes away with Azure Monitoring Agent( latest agent that will eventually replace Log Analytics Agent). HTH

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/connect-windows-firewall>

**Question: 255**

CertyIQ

HOTSPOT -

You have an Azure subscription that contains a user named Admin1 and a resource group named RG1. In Azure Monitor, you create the alert rules shown in the following table.



Name	Resource	Condition
Rule1	RG1	All security operations
Rule2	RG1	All administrative operations
Rule3	Azure subscription	All security operations by Admin1
Rule4	Azure subscription	All administrative operations by Admin1

Admin1 performs the following actions on RG1:

⇒ Adds a virtual network named VNET1

⇒ Adds a Delete lock named Lock1

Which rules will trigger an alert as a result of the actions of Admin1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

## Answer Area

Adding VNET1:

▼

Rule2 only

Rule4 only

Rule2 and Rule4 only

Rule3 and Rule4 only

Rule1, Rule2, Rule3, and Rule4

Adding Lock1:

▼

Rule2 only

Rule4 only

Rule2 and Rule4 only

Rule3 and Rule4 only

Rule1, Rule2, Rule3, and Rule4

Answer:



## Answer Area

Adding VNET1:

Rule2 only
Rule4 only
Rule2 and Rule4 only
Rule3 and Rule4 only
Rule1, Rule2, Rule3, and Rule4

Adding Lock1:

Rule2 only
Rule4 only
Rule2 and Rule4 only
Rule3 and Rule4 only
Rule1, Rule2, Rule3, and Rule4

### Question: 256

CertyIQ

You have an Azure subscription that contains 100 virtual machines and has Azure Defender enabled. You plan to perform a vulnerability scan of each virtual machine.

You need to deploy the vulnerability scanner extension to the virtual machines by using an Azure Resource Manager template.

Which two values should you specify in the code to automate the deployment of the extension to the virtual machines? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. the user-assigned managed identity
- B. the workspace ID
- C. the Azure Active Directory (Azure AD) ID
- D. the Key Vault managed storage account key
- E. the system-assigned managed identity
- F. the primary shared key

**Answer: BE**

**Explanation:**

Since we are deploying the template across several VMs and need to authenticate with the extension repository (for downloading extensions), we need to provide the VM an identity to authenticate with the repository. This is best done by assigning the VM with a "user assigned managed identity". We can set up this managed identity to have the required permissions on the extension repository via RBAC roles. The managed identity requests permissions via the Azure IMDS from the Azure AD and hence needs to know the right Tenant ID to get the token from. I believe the Azure AD ID is the same as the Tenant ID.

**Question: 257****CertyIQ**

You have an Azure subscription that contains a user named Admin1 and a virtual machine named VM1. VM1 runs Windows Server 2019 and was deployed by using an Azure Resource Manager template. VM1 is the member of a backend pool of a public Azure Basic Load Balancer.

Admin1 reports that VM1 is listed as Unsupported on the Just in time VM access blade of Azure Security Center. You need to ensure that Admin1 can enable just in time (JIT) VM access for VM1.

What should you do?

- A. Create and configure a network security group (NSG).
- B. Create and configure an additional public IP address for VM1.
- C. Replace the Basic Load Balancer with an Azure Standard Load Balancer.
- D. Assign an Azure Active Directory Premium Plan 1 license to Admin1.

**Answer: A****Explanation:**

Unsupported - VMs without JIT enabled and which don't support the feature. Your VM might be in this tab for the following reasons:

Missing network security group (NSG) - JIT requires an NSG to be configured

Classic VM - JIT supports VMs that are deployed through Azure Resource Manager, not 'classic deployment'. Learn more about classic vs Azure Resource Manager deployment models.

Other - Your VM might be in this tab if the JIT solution is disabled in the security policy of the subscription or the resource group.

Unsupported - VMs without JIT enabled and which don't support the feature. Your VM might be in this tab for the following reasons:

Missing network security group (NSG) - JIT requires an NSG to be configured

Classic VM - JIT supports VMs that are deployed through Azure Resource Manager, not 'classic deployment'. Learn more about classic vs Azure Resource Manager deployment models.

Other - Your VM might be in this tab if the JIT solution is disabled in the security policy of the subscription or the resource group.

upvoted 29 times

**Reference:**

<https://docs.microsoft.com/en-us/azure/security-center/security-center-just-in-time?tabs=jit-config-asc%2Cjit-request-asc>

**Question: 258****HOTSPOT -**

You have an Azure Sentinel workspace that contains an Azure Active Directory (Azure AD) connector, an Azure Log Analytics query named Query1, and a playbook named Playbook1.

Query1 returns a subset of security events generated by Azure AD.

You plan to create an Azure Sentinel analytic rule based on Query1 that will trigger Playbook1.

You need to ensure that you can add Playbook1 to the new rule.

What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

**Answer Area**

Create the rule and set the type to:

	▼
Fusion	
Microsoft Security incident creation	
Scheduled	

Configure the playbook to include:

	▼
A managed connector	
A system-assigned managed identity	
A trigger	
Diagnostic settings	

**Answer:**

## Answer Area

Create the rule and set the type to:

Fusion

Microsoft Security incident creation

Scheduled

Configure the playbook to include:

A managed connector

A system-assigned managed identity

A trigger

Diagnostic settings

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/tutorial-detect-threats-custom> <https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook>

### Question: 259

CertyIQ

HOTSPOT -

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

Name	Type	Attached to	NSG
NSG1	Network security group (NSG)	VM5	<i>Not applicable</i>
NSG2	Network security group (NSG)	Subnet1	<i>Not applicable</i>
Subnet1	Subnet	<i>Not applicable</i>	<i>Not applicable</i>
VM5	Virtual machine	Subnet1	NSG1

An IP address of 10.1.0.4 is assigned to VM5. VM5 does not have a public IP address.

VM5 has just in time (JIT) VM access configured as shown in the following exhibit.

### JIT VM access configuration



VM5








+ Add  Save  Discard

Configure the ports for which the just-in-time VM access will be applicable

Port	Protocol	Allowed source IPs	IP range	Time range (hours)	
3389	Any	Per request	N/A	3 hours	...

You enable JIT VM access for VM5.

NSG1 has the inbound rules shown in the following exhibit.

Priority	Name	Port	Protocol	Source	Destination	Action
100	 SecurityCenter-JITRule-...	3389	Any	Any	10.1.0.4	 Allow
1000	SecurityCenter-JITRule_341...	3389	Any	Any	10.1.0.4	 Deny
1001	RDP	3389	TCP	Any	Any	 Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	 Allow
65001	AllowAzureLoadBalancerIn...	Any	Any	AzureLoadBalancer	Any	 Allow
65500	DenyAllInBound	Any	Any	Any	Any	 Deny

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

NOTE: Each correct selection is worth one point.

Hot Area:

### Answer Area

Statements	Yes	No
Deleting the security rule that has a priority of 100 will revoke the approved JIT access request.	<input type="radio"/>	<input type="radio"/>
Remote Desktop access to VM5 is blocked.	<input type="radio"/>	<input type="radio"/>
An Azure Bastion host will enable Remote Desktop access to VM5 from the internet.	<input type="radio"/>	<input type="radio"/>

Answer:

### Answer Area

Statements	Yes	No
Deleting the security rule that has a priority of 100 will revoke the approved JIT access request.	<input checked="" type="radio"/>	<input type="radio"/>
Remote Desktop access to VM5 is blocked.	<input type="radio"/>	<input checked="" type="radio"/>
An Azure Bastion host will enable Remote Desktop access to VM5 from the internet.	<input type="radio"/>	<input checked="" type="radio"/>

Explanation:

1. In case if rule 100 is deleted manually the access will not work. So the answer is - YES
2. RDP is not blocked because rule 100 is in place and we should consider it as it is. - NO
3. Azure Bastion host is not enabling RDP from the internet. This is the key feature of Bastion - allowing access to VMs which does not have a public IP address. So the answer is - NO

### Question: 260

CertyIQ

You have an Azure Active Directory (Azure AD) tenant and a root management group.  
You create 10 Azure subscriptions and add the subscriptions to the root management group.  
You need to create an Azure Blueprints definition that will be stored in the root management group.



What should you do first?

- A. Modify the role-based access control (RBAC) role assignments for the root management group.
- B. Add an Azure Policy definition to the root management group.
- C. Create a user-assigned identity.
- D. Create a service principal.

**Answer: A**

**Explanation:**

When I tried to create a Blueprint at the root management group,

Deploy blueprint to root management group:

"You require additional permissions to manage blueprints within this management group. Contact the administrator of the management group to request Contributor rights."

Had to elevate myself to a Contributor at the root group, then I could create the blueprint.

Reference:

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

**Question: 261**

**CertyIQ**

HOTSPOT -

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

Name	Role
Admin1	Global administrator
Admin2	Group administrator
Admin3	User administrator

Contoso.com contains a group naming policy. The policy has a custom blocked word list rule that includes the word Contoso.

Which users can create a group named Contoso Sales in contoso.com? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

**Answer Area**

Users who can create a security group named Contoso Sales:

▼

Admin1 only

Admin1 and Admin2 only

Admin1 and Admin3 only

Admin1, Admin2, and Admin3

Users who can create a Microsoft 365 group named Contoso Sales:

▼

Admin1 only

Admin1 and Admin2 only

Admin1 and Admin3 only

Admin1, Admin2, and Admin3



Answer:

### Answer Area

Users who can create a security group named Contoso Sales:

Admin1 only  
Admin1 and Admin2 only  
Admin1 and Admin3 only  
Admin1, Admin2, and Admin3

Users who can create a Microsoft 365 group named Contoso Sales:

Admin1 only  
Admin1 and Admin2 only  
Admin1 and Admin3 only  
Admin1, Admin2, and Admin3

### Explanation:

- 1) Admin1,2,3 because policy naming blocks only apply to O365
- 2) Admin 1,3 because Global Admin and User Admin are exempt.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/groups-naming-policy>

## Question: 262

CertyIQ

DRAG DROP -

You have five Azure subscriptions linked to a single Azure Active Directory (Azure AD) tenant.

You create an Azure Policy initiative named SecurityPolicyInitiative1.

You identify which standard role assignments must be configured on all new resource groups.

You need to enforce SecurityPolicyInitiative1 and the role assignments when a new resource group is created. 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

### Answer Area

Publish an Azure Blueprints version

Assign an Azure blueprint.

Create a policy assignment.

Create a custom role-based access control (RBAC) role.

Create a dedicated management subscription.

Create an Azure Blueprints definition.

Create an initiative assignment.



**Answer:****Actions**

Publish an Azure Blueprints version

Assign an Azure blueprint.

Create a policy assignment.

Create a custom role-based access control (RBAC) role.

Create a dedicated management subscription.

Create an Azure Blueprints definition.

Create an initiative assignment.

**Answer Area**

Create an Azure Blueprints definition.

Publish an Azure Blueprints version

Assign an Azure blueprint.

**Explanation:****Reference:**

<https://docs.microsoft.com/en-us/azure/governance/blueprints/create-blueprint-portal> <https://docs.microsoft.com/en-us/azure/azure-australia/azure-policy>

**Question: 263****CertyIQ**

You have three on-premises servers named Server1, Server2, and Server3 that run Windows Server 2019. Server1 and Server2 are located on the internal network. Server3 is located on the perimeter network. All servers have access to Azure.

From Azure Sentinel, you install a Windows firewall data connector.

You need to collect Microsoft Defender Firewall data from the servers for Azure Sentinel.

What should you do?

- A. Create an event subscription from Server1, Server2, and Server3.
- B. Install the On-premises data gateway on each server.
- C. Install the Microsoft Monitoring Agent on each server.
- D. Install the Microsoft Monitoring Agent on Server1 and Server2. Install the On-premises data gateway on Server3.

**Answer: C****Explanation:****Reference:**

<https://docs.microsoft.com/en-us/azure/sentinel/connect-windows-firewall>

**Question: 264****CertyIQ**

You have an Azure subscription that contains several Azure SQL databases and an Azure Sentinel workspace. You need to create a saved query in the workspace to find events reported by Azure Defender for SQL.

What should you do?

- A. From Azure CLI, run the Get-AzOperationalInsightsWorkspace cmdlet.

- B. From the Azure SQL Database query editor, create a Transact-SQL query.
- C. From the Azure Sentinel workspace, create a Kusto query language query.
- D. From Microsoft SQL Server Management Studio (SSMS), create a Transact-SQL query.

**Answer: C**

**Explanation:**

From the Azure Sentinel workspace, create a Kusto query language query.

### Question: 265

CertyIQ

HOTSPOT -

You plan to use Azure Sentinel to create an analytic rule that will detect suspicious threats and automate responses.

Which components are required for the rule? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

## Answer Area

Detect suspicious threats:

	▼
A Kusto query language query	
A Transact-SQL query	
An Azure PowerShell script	
An Azure Sentinel playbook	

Automate responses:

	▼
An Azure Functions app	
An Azure PowerShell script	
An Azure Sentinel playbook	
An Azure Sentinel workbook	

**Answer:**

## Answer Area

Detect suspicious threats:

- A Kusto query language query
- A Transact-SQL query
- An Azure PowerShell script
- An Azure Sentinel playbook

Automate responses:

- An Azure Functions app
- An Azure PowerShell script
- An Azure Sentinel playbook
- An Azure Sentinel workbook

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/tutorial-detect-threats-custom> <https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook>

### Question: 266

CertyIQ

You are collecting events from Azure virtual machines to an Azure Log Analytics workspace. You plan to create alerts based on the collected events. You need to identify which Azure services can be used to create the alerts. Which two services should you identify? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

- A. Azure Monitor
- B. Azure Security Center
- C. Azure Analysis Services
- D. Azure Sentinel
- E. Azure Advisor

**Answer: AD**

**Explanation:**

AZ monitor, security centre and sentinel can all generate alerts, but security centre alerts are auto generated based on security centre policy and AZ defender settings, where as alert rules can be configured for both Az monitor and sentinel.

**Question: 267**

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 use Microsoft Defender for Cloud for the centralized policy management of three Azure subscriptions.

You use several policy definitions to manage the security of the subscriptions.

You need to deploy the policy definitions as a group to all three subscriptions.

Solution: You create an initiative and an assignment that is scoped to a management group.

Does this meet the goal?

A. Yes

B. No

**Answer: A**

**Explanation:**

Creating an initiative and an assignment scoped to a management group is a valid solution for deploying policy definitions as a group to multiple Azure subscriptions. An initiative is a container for a set of policy definitions in Azure Policy. By creating an initiative, you can manage multiple policy definitions as a single unit and apply them to a specific scope, such as a management group, which can include multiple subscriptions.

An assignment is used to assign the initiative to a specific scope, such as a management group, and enforce the policies defined in the initiative to all the resources within that scope.

Reference:

<https://docs.microsoft.com/en-us/azure/governance/policy/overview>

**Question: 268**

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 use Microsoft Defender for Cloud for the centralized policy management of three Azure subscriptions.

You use several policy definitions to manage the security of the subscriptions.

You need to deploy the policy definitions as a group to all three subscriptions.

Solution: You create a policy initiative and assignments that are scoped to resource groups.

Does this meet the goal?

A. Yes

B. No

**Answer: B**

**Explanation:**

Instead use a management group.

Management groups in Microsoft Azure solve the problem of needing to impose governance policy on more than one Azure subscription simultaneously.

Reference:

<https://4sysops.com/archives/apply-governance-policy-to-multiple-azure-subscriptions-with-management-gr>

### Question: 269

CertyIQ

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

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

You use Microsoft Defender for Cloud for the centralized policy management of three Azure subscriptions.

You use several policy definitions to manage the security of the subscriptions.

You need to deploy the policy definitions as a group to all three subscriptions.

Solution: You create a policy definition and assignments that are scoped to resource groups.

Does this meet the goal?

A. Yes

B. No

**Answer: B**

**Explanation:**

Reference:

<https://4sysops.com/archives/apply-governance-policy-to-multiple-azure-subscriptions-with-management-groups/>

### Question: 270

CertyIQ

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

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

You use Microsoft Defender for Cloud for the centralized policy management of three Azure subscriptions.

You use several policy definitions to manage the security of the subscriptions.

You need to deploy the policy definitions as a group to all three subscriptions.

Solution: You create a resource graph and an assignment that is scoped to a management group.

Does this meet the goal?

A. Yes

B. No

**Answer: B**

**Explanation:**

Management groups in Microsoft Azure solve the problem of needing to impose governance policy on more than one Azure subscription simultaneously.

However, you need to use an initiative, not a resource graph to bundle the policy definitions into a group that can be applied to the management group.

Reference:

<https://4sysops.com/archives/apply-governance-policy-to-multiple-azure-subscriptions-with-management-groups/>



## 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 AccountType == 'User' and
```

	▼	== 4625
ActivityID		
DataType		
EventID		
QuantityUnit		

```
| summarize failed_login_attempts=
```

	▼
Count(),	
Countif(),	
Makeset(),	
Split(),	

```
latest_failed_login=arg_max(TimeGenerated, Account) by Account  
| where failed_login_attempts > 5
```

Answer:

## Answer Area

```
let timeframe = 3d;  
SecurityEvent  
| where TimeGenerated > ago(3d)  
| where AccountType == 'User' and
```

	▼	== 4625
ActivityID		
DataType		
EventID		
QuantityUnit		

```
| summarize failed_login_attempts=
```

	▼
Count(),	
Countif(),	
Makeset(),	
Split(),	

```
latest_failed_login=arg_max(TimeGenerated, Account) by Account  
| where failed_login_attempts > 5
```

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
```

Reference:

<https://docs.microsoft.com/en-us/azure/azure-monitor/log-query/examples>

### Question: 272

CertyIQ

You have an Azure subscription named Sub1.

In Azure Security Center, you have a security playbook named Play1. Play1 is configured to send an email message to a user named User1.

You need to modify Play1 to send email messages to a distribution group named Alerts.

What should you use to modify Play1?

- A. Azure DevOps
- B. Azure Application Insights
- C. Azure Monitor
- D. Azure Logic Apps Designer

**Answer: D**

#### Explanation:

You can change an existing playbook in Security Center to add an action, or conditions. To do that you just need to click on the name of the playbook that you want to change, in the Playbooks tab, and Logic App Designer opens up.

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/security-center-playbooks>

### Question: 273

CertyIQ

You create a new Azure subscription.

You need to ensure that you can create custom alert rules in Azure Security Center.

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

NOTE: Each correct selection is worth one point.

- A. Onboard Azure Active Directory (Azure AD) Identity Protection.
- B. Create an Azure Storage account.
- C. Implement Azure Advisor recommendations.
- D. Create an Azure Log Analytics workspace.
- E. Upgrade the pricing tier of Security Center to Standard.

**Answer: DE**

**Explanation:**

You need to upgrade the pricing tier of Azure Security Center to standard. You can also create a new Log Analytics workspace which can be used by Azure Security Center to send data with regards to your Azure resources

**Question: 274****CertyIQ**

You have an Azure subscription named Sub1 that contains an Azure Log Analytics workspace named LAW1. You have 100 on-premises servers that run Windows Server 2012 R2 and Windows Server 2016. The servers connect to LAW1. LAW1 is configured to collect security-related performance counters from the connected servers.

You need to configure alerts based on the data collected by LAW1. The solution must meet the following requirements:

- Alert rules must support dimensions.
  - The time it takes to generate an alert must be minimized.
  - Alert notifications must be generated only once when the alert is generated and once when the alert is resolved.
- Which signal type should you use when you create the alert rules?

- A. Log
- B. Log (Saved Query)
- C. Metric
- D. Activity Log

**Answer: C****Explanation:**

Metric alerts in Azure Monitor provide a way to get notified when one of your metrics cross a threshold. Metric alerts work on a range of multi-dimensional platform metrics, custom metrics, Application Insights standard and custom metrics.

Note: Signals are emitted by the target resource and can be of several types. Metric, Activity log, Application Insights, and Log.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-monitor/platform/alerts-metric>

**Question: 275****CertyIQ**

HOTSPOT -

You have an Azure subscription that contains an Azure Sentinel workspace.

Azure Sentinel is configured to ingest logs from several Azure workloads. A third-party service management platform is used to manage incidents.

You need to identify which Azure Sentinel components to configure to meet the following requirements:

- When Azure Sentinel identifies a threat, an incident must be created.
- A ticket must be logged in the service management platform when an incident is created in Azure Sentinel.

Which component should you identify for each requirement? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

## Answer Area

When Azure Sentinel identifies a threat, an incident must be created:

	▼
Analytics	
Data connectors	
Playbooks	
Workbooks	

A ticket must be logged in the service management platform when an incident is created in Azure Sentinel:

	▼
Analytics	
Data connectors	
Playbooks	
Workbooks	

Answer:

### Answer Area

When Azure Sentinel identifies a threat, an incident must be created:

	▼
Analytics	
Data connectors	
Playbooks	
Workbooks	

A ticket must be logged in the service management platform when an incident is created in Azure Sentinel:

	▼
Analytics	
Data connectors	
Playbooks	
Workbooks	

Explanation:

Analytics rule allows grouping of alerts into an incident and playbook can be configured to log a ticket in third party system as a response to the incident

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/create-incidents-from-alerts> <https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook>

Question: 276

CertyIQ

HOTSPOT -  
You have an Azure subscription.

You need to create and deploy an Azure policy that meets the following requirements:

- When a new virtual machine is deployed, automatically install a custom security extension.
- Trigger an autogenerated remediation task for non-compliant virtual machines to install the extension.

What should you include in the policy? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

## Answer Area

Definition effect:

Append
DeployIfNotExists
EnforceOPAConstraint
EnforceRegoPolicy
Modify

Assignment remediation task:

A managed identity that has the Contributor role
A managed identity that has the User Access Administrator role
A service principal that has the Contributor role
A service principal that has the User Access Administrator role

Answer:

## Answer Area

Definition effect:

Append
DeployIfNotExists
EnforceOPAConstraint
EnforceRegoPolicy
Modify

Assignment remediation task:

A managed identity that has the Contributor role
A managed identity that has the User Access Administrator role
A service principal that has the Contributor role
A service principal that has the User Access Administrator role

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/governance/policy/how-to/remediate-resources>

## Question: 277

CertyIQ

You have an Azure subscription named Subscription1 that contains the resources shown in the following table.



Name	Type	Category
Initiative1	Initiative definition	Security Center
Initiative2	Initiative definition	My Custom Category
Policy1	Policy definition	Security Center
Policy2	Policy definition	My Custom Category

You need to identify which initiatives and policies you can add to Subscription1 by using Azure Security Center. What should you identify?

- A. Policy1 and Policy2 only
- B. Initiative1 only
- C. Initiative1 and Initiative2 only
- D. Initiative1, Initiative2, Policy1, and Policy2

**Answer: C**

**Explanation:**

Initiative1 and Initiative2 only " as ASC does not support the integration of policies as is, just initiatives (which is a set of policies)

### Question: 278

CertyIQ

You have an Azure subscription named Sub1.  
In Azure Security Center, you have a workflow automation named WF1. WF1 is configured to send an email message to a user named User1.  
You need to modify WF1 to send email messages to a distribution group named Alerts.  
What should you use to modify WF1?

- A. Azure Application Insights
- B. Azure Monitor
- C. Azure Logic Apps Designer
- D. Azure DevOps

**Answer: C**

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/workflow-automation> <https://docs.microsoft.com/en-us/learn/modules/resolve-threats-with-azure-security-center/6-exercise-configure-playbook>

### Question: 279

CertyIQ

You have an Azure resource group that contains 100 virtual machines.  
You have an initiative named Initiative1 that contains multiple policy definitions. Initiative1 is assigned to the resource group.  
You need to identify which resources do NOT match the policy definitions.  
What should you do?

- A. From Azure Security Center, view the Regulatory compliance assessment.
- B. From the Policy blade of the Azure Active Directory admin center, select Compliance.



C. From Azure Security Center, view the Secure Score.

D. From the Policy blade of the Azure Active Directory admin center, select Assignments.

**Answer: B**

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/azure/governance/policy/how-to/get-compliance-data#portal>

### Question: 280

CertyIQ

You have an Azure subscription named Subscription1.

You need to view which security settings are assigned to Subscription1 by default.

Which Azure policy or initiative definition should you review?

- A. the Audit diagnostic setting policy definition
- B. the Enable Monitoring in Azure Security Center initiative definition
- C. the Enable Azure Monitor for VMs initiative definition
- D. the Azure Monitor solution 'Security and Audit' must be deployed policy definition

**Answer: B**

**Explanation:**

the Enable Monitoring in Azure Security Center (Microsoft Defender for cloud) initiative definition

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/tutorial-security-policy>

<https://docs.microsoft.com/en-us/azure/security-center/policy-reference>

### Question: 281

CertyIQ

DRAG DROP -

You have an Azure Sentinel workspace that has an Azure Active Directory (Azure AD) data connector.

You are threat hunting suspicious traffic from a specific IP address.

You need to annotate an intermediate event stored in the workspace and be able to reference the IP address when navigating through the investigation graph.

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

## Answer Area

Add the query to Favorites.

From the Azure Sentinel workspace, run an Azure Log Analytics query.

In a Jupyter notebook, create a reference to the IP address.

Add a bookmark and assign a tag.

Add a bookmark and map an entity.

From Azure Monitor, run an Azure Log Analytics query.

Select a query result.



Answer:

## Actions

## Answer Area

Add the query to Favorites.

From the Azure Sentinel workspace, run an Azure Log Analytics query.

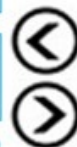
In a Jupyter notebook, create a reference to the IP address.

Add a bookmark and assign a tag.

Add a bookmark and map an entity.

From Azure Monitor, run an Azure Log Analytics query.

Select a query result.



From the Azure Sentinel workspace, run an Azure Log Analytics query.

Select a query result.

Add a bookmark and map an entity.

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/bookmarks>

## HOTSPOT -

You have 20 Azure subscriptions and a security group named Group1. The subscriptions are children of the root management group.

Each subscription contains a resource group named RG1.

You need to ensure that for each subscription RG1 meets the following requirements:

- The members of Group1 are assigned the Owner role.
- The modification of permissions to RG1 is prevented.

What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

### Answer Area

Configure role-based access control (RBAC) role assignments by using:

	▼
Azure Blueprints	
Azure Policy	
Azure Security Center	

Prevent the modification of permissions to RG1 by using:

	▼
A resource lock	
A role-based access control (RBAC) role assignment at the resource group level	
Azure Blueprint assignments in locking mode	

Answer:

### Answer Area

Configure role-based access control (RBAC) role assignments by using:

	▼
Azure Blueprints	
Azure Policy	
Azure Security Center	

Prevent the modification of permissions to RG1 by using:

	▼
A resource lock	
A role-based access control (RBAC) role assignment at the resource group level	
Azure Blueprint assignments in locking mode	

## Question: 283

CertyIQ

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

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

You use Microsoft Defender for Cloud for the centralized policy management of three Azure subscriptions.

You use several policy definitions to manage the security of the subscriptions.

You need to deploy the policy definitions as a group to all three subscriptions.

Solution: You create a policy initiative and an assignment that is scoped to the Tenant Root Group management group.

Does this meet the goal?

A. Yes

B. No

**Answer: A**

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/azure/governance/policy/overview> <https://4sysops.com/archives/apply-governance-policy-to-multiple-azure-subscriptions-with-management-groups/>

### Question: 284

CertyIQ

You have an Azure environment.

You need to identify any Azure configurations and workloads that are non-compliant with ISO 27001:2013 standards.

What should you use?

A. Azure Sentinel

B. Azure Active Directory (Azure AD) Identity Protection

C. Microsoft Defender for Cloud

D. Microsoft Defender for Identity

**Answer: C**

**Explanation:**

Microsoft Defender for Cloud helps streamline the process for meeting regulatory compliance requirements, using the regulatory compliance dashboard.

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/security-center-compliance-dashboard>

### Question: 285

CertyIQ

DRAG DROP -

You have an Azure subscription that contains 100 virtual machines. Azure Diagnostics is enabled on all the virtual machines.

You are planning the monitoring of Azure services in the subscription.

You need to retrieve the following details:

- ⇒ Identify the user who deleted a virtual machine three weeks ago.
- ⇒ Query the security events of a virtual machine that runs Windows Server 2016.

What should you use in Azure Monitor? To answer, drag the appropriate configuration settings to the correct details. Each configuration setting may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:

## Settings

## Answer Area

Activity log

Logs

Metrics

Service Health

Identify the user who deleted a virtual machine three weeks ago:

Query the security events of a virtual machine that runs Windows Server 2016:

Answer:

## Settings

## Answer Area

Activity log

Logs

Metrics

Service Health

Identify the user who deleted a virtual machine three weeks ago:

Query the security events of a virtual machine that runs Windows Server 2016:

Activity log

Logs

### Explanation:

Box1: Activity log -

Azure activity logs provide insight into the operations that were performed on resources in your subscription.

Activity logs were previously known as audit logs or

operational logs, because they report control-plane events for your subscriptions.

Activity logs help you determine the what, who, and when for write operations (that is, PUT, POST, or DELETE).

Box 2: Logs -

Log Integration collects Azure diagnostics from your Windows virtual machines, Azure activity logs, Azure Security Center alerts, and Azure resource provider logs. This integration provides a unified dashboard for all your assets, whether they're on-premises or in the cloud, so that you can aggregate, correlate, analyze, and alert for security events.

Reference:

<https://docs.microsoft.com/en-us/azure/security/azure-log-audit>

### Question: 286

CertyIQ

HOTSPOT -

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



Name	Type	Resource group
RG1	Resource group	<i>Not applicable</i>
VM1	Virtual machine	RG1
VM2	Virtual machine	RG1
ActionGroup1	Action group	RG1

VM1 and VM2 are stopped.

You create an alert rule that has the following settings:

- Resource: RG1
- Condition: All Administrative operations
- Actions: Action groups configured for this alert rule: ActionGroup1
- Alert rule name: Alert1

You create an action rule that has the following settings:

- Scope: VM1
- Filter criteria: Resource Type = "Virtual Machines"
- Define on this scope: Suppression
- Suppression config: From now (always)
- Name: ActionRule1

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

Note: Each correct selection is worth one point.

Hot Area:

### Answer area

Statements	Yes	No
If you start VM1, an alert is triggered.	<input type="radio"/>	<input type="radio"/>
If you start VM2, an alert is triggered.	<input type="radio"/>	<input type="radio"/>
If you add a tag to RG1, an alert is triggered.	<input type="radio"/>	<input type="radio"/>

Answer:

### Answer area

Statements	Yes	No
If you start VM1, an alert is triggered.	<input type="radio"/>	<input checked="" type="radio"/>
If you start VM2, an alert is triggered.	<input checked="" type="radio"/>	<input type="radio"/>
If you add a tag to RG1, an alert is triggered.	<input type="radio"/>	<input checked="" type="radio"/>

Explanation:



Box 1: NO

The scope for the action rule is set to VM1 and is set to suppress alerts indefinitely.

Box 2: YES

The scope for the action rule is not set to VM2.

Box 3: NO

Adding a tag is not an administrative operation.

References:

<https://docs.microsoft.com/en-us/azure/azure-monitor/platform/alerts-activity-log>

<https://docs.microsoft.com/en-us/azure/azure-monitor/platform/alerts-action-rules>

### Question: 287

CertyIQ

DRAG DROP -

You have an Azure subscription named Sub1 that contains an Azure Log Analytics workspace named LAW1.

You have 500 Azure virtual machines that run Windows Server 2016 and are enrolled in LAW1.

You plan to add the System Update Assessment solution to LAW1.

You need to ensure that System Update Assessment-related logs are uploaded to LAW1 from 100 of the virtual machines only.

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

Create a new workspace.

Apply the scope configuration to the solution.

Create a scope configuration.

Create a computer group.

Create a data source.

#### Answer Area

Answer:

**Actions**

Create a new workspace.

**Answer Area**

Create a computer group.

Create a scope configuration.

Apply the scope configuration to the solution.

Create a data source.

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/azure/azure-monitor/insights/solution-targeting>

**Question: 288****CertyIQ**

You have an Azure subscription named Sub1 that contains the virtual machines shown in the following table.

Name	Resource group
VM1	RG1
VM2	RG2
VM3	RG1
VM4	RG2

You need to ensure that the virtual machines in RG1 have the Remote Desktop port closed until an authorized user requests access.

What should you configure?

- A. Azure Active Directory (Azure AD) Privileged Identity Management (PIM)
- B. an application security group
- C. Azure Active Directory (Azure AD) conditional access
- D. just in time (JIT) VM access

**Answer: D****Explanation:**

Just-in-time (JIT) virtual machine (VM) access can be used to lock down inbound traffic to your Azure VMs, reducing exposure to attacks while providing easy access to connect to VMs when needed.

Note: When just-in-time is enabled, Security Center locks down inbound traffic to your Azure VMs by creating an NSG rule. You select the ports on the VM to which inbound traffic will be locked down. These ports are controlled by the just-in-time solution.

When a user requests access to a VM, Security Center checks that the user has Role-Based Access Control (RBAC) permissions that permit them to successfully request access to a VM. If the request is approved, Security Center automatically configures the Network Security Groups (NSGs) and Azure Firewall to allow inbound traffic to the selected ports and requested source IP addresses or ranges, for the amount of time that was specified. After the time has expired, Security Center restores the NSGs to their previous states. Those connections that are already established are not

being interrupted, however.

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/security-center-just-in-time>

### Question: 289

CertyIQ

SIMULATION -

You need to ensure that web1234578 is protected from malware by using Microsoft Antimalware for Virtual Machines and is scanned every Friday at 01:00.

To complete this task, sign in to the Azure portal.

#### Answer:

See the explanation below.

#### Explanation:

You need to install and configure the Microsoft Antimalware extension on the virtual machine named web1234578.

1. In the Azure portal, type Virtual Machines in the search box, select Virtual Machines from the search results then select web1234578. Alternatively, browse to Virtual Machines in the left navigation pane.
2. In the properties of web11597200, click on Extensions.
3. Click the Add button to add an Extension.
4. Scroll down the list of extensions and select Microsoft Antimalware.
5. Click the Create button. This will open the settings pane for the Microsoft Antimalware Extension.
6. In the Scan day field, select Friday.
7. In the Scan time field, enter 60. The scan time is measured in minutes after midnight so 60 would be 01:00, 120 would be 02:00 etc.
8. Click the OK button to save the configuration and install the extension.

### Question: 290

CertyIQ

SIMULATION -

You need to ensure that the events in the NetworkSecurityGroupRuleCounter log of the VNET01-Subnet0-NSG network security group (NSG) are stored in the logs1234578 Azure Storage account for 30 days.

To complete this task, sign in to the Azure portal.

#### Answer:

See the explanation below.

#### Explanation:

You need to configure the diagnostic logging for the NetworkSecurityGroupRuleCounter log.

1. In the Azure portal, type Network Security Groups in the search box, select Network Security Groups from the search results then select VNET01-Subnet0-NSG. Alternatively, browse to Network Security Groups in the left navigation pane.
2. In the properties of the Network Security Group, click on Diagnostic Settings.
3. Click on the Add diagnostic setting link.
4. Provide a name in the Diagnostic settings name field. It doesn't matter what name you provide for the exam.
5. In the Log section, select NetworkSecurityGroupRuleCounter.
6. In the Destination details section, select Archive to a storage account.
7. In the Storage account field, select the logs1234578 storage account.
8. In the Retention (days) field, enter 30.
9. Click the Save button to save the changes.

Question: 291

HOTSPOT -

On Monday, you configure an email notification in Azure Security Center to email notifications to [email protected] about alerts that have a severity level of Low, Medium, or High.

On Tuesday, Security Center generates the security alerts shown in the following table.

Time	Description	Severity
01:00	Failed RDP brute force attack	Medium
01:01	Successful RDP brute force attack	High
06:10	Suspicious process executed	High
09:00	Malicious SQL activity	High
11:15	Network communication with a malicious machine detected	Low
13:30	Suspicious process executed	High
14:00	Failed RDP brute force attack	Medium
16:01	Successful RDP brute force attack	High
23:20	Possible outgoing spam activity detected	Low
23:25	Modified system binary discovered in dump file	High
23:30	Malicious SQL activity	High

How many email notifications will [email protected] receive on Tuesday? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Total number of Security Center email notifications about an RDP  
brute force attack on Tuesday:

▼

1
2
3
4

Total number of Security Center email notifications on Tuesday:

▼

3
4
7
9
11

Answer:

## Answer Area

Total number of Security Center email notifications about an RDP brute force attack on Tuesday:

	▼
1	
2	
3	
4	

Total number of Security Center email notifications on Tuesday:

	▼
3	
4	
7	
9	
11	

### Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/security-center-provide-security-contact-details>

## Question: 292

CertyIQ

You are troubleshooting a security issue for an Azure Storage account. You enable the diagnostic logs for the storage account. What should you use to retrieve the diagnostics logs?

- A. Azure Security Center
- B. Azure Monitor
- C. the Security admin center
- D. Azure Storage Explorer

### Answer: D

#### Explanation:

If you want to download the metrics for long-term storage or to analyze them locally, you must use a tool or write some code to read the tables. You must download the minute metrics for analysis. The tables do not appear if you list all the tables in your storage account, but you can access them directly by name.

Many storage-browsing tools are aware of these tables and enable you to view them directly (see Azure Storage Client Tools for a list of available tools).

Microsoft provides several graphical user interface (GUI) tools for working with the data in your Azure Storage account. All of the tools outlined in the following table are free.

Note:

There are several versions of this question in the exam. The questions in the exam have two different correct answers:

1. Azure Storage Explorer

2. AZCopy

Other incorrect answer options you may see on the exam include the following:

1. Azure Monitor

2. The Security & Compliance admin center

3. Azure Cosmos DB explorer

4. Azure Monitor

Reference:

[https://docs.microsoft.com/en-us/azure/storage/common/storage-analytics-metrics?  
toc=%2fazure%2fstorage%2fblobs%2ftoc.json](https://docs.microsoft.com/en-us/azure/storage/common/storage-analytics-metrics?toc=%2fazure%2fstorage%2fblobs%2ftoc.json) [https://docs.microsoft.com/en-  
us/azure/storage/common/storage-explorers](https://docs.microsoft.com/en-us/azure/storage/common/storage-explorers)

### Question: 293

CertyIQ

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

Name	Type
VM1	Virtual machine
VNET1	Virtual network
storage1	Storage account
Vault1	Key vault

You plan to enable Azure Defender for the subscription.  
Which resources can be protected by using Azure Defender?

- A.VM1, VNET1, storage1, and Vault1
- B.VM1, VNET1, and storage1 only
- C.VM1, storage1, and Vault1 only
- D.VM1 and VNET1 only
- E.VM1 and storage1 only

**Answer: C**

**Explanation:**

C. VM1, storage1, and Vault1 only

Answer is C

### Question: 294

CertyIQ

DRAG DROP -

You have an Azure subscription that contains the following resources:

- ⇒ A network virtual appliance (NVA) that runs non-Microsoft firewall software and routes all outbound traffic from



the virtual machines to the internet

- An Azure function that contains a script to manage the firewall rules of the NVA
- Azure Security Center standard tier enabled for all virtual machines
- An Azure Sentinel workspace
- 30 virtual machines

You need to ensure that when a high-priority alert is generated in Security Center for a virtual machine, an incident is created in Azure Sentinel and then a script is initiated to configure a firewall rule for the NVA.

How should you configure Azure Sentinel to meet the requirements? To answer, drag the appropriate components to the correct requirements. Each component may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:

#### Components

- A data connector for Security Center
- A data connector for the firewall software
- A playbook
- A rule
- A Security Events connector
- A workbook

#### Answer Area

Enable alert notifications from Security Center:

Component

Create an incident:

Component

Initiate a script to configure the firewall rule:

Component

#### Answer:

##### Components

- 
- A data connector for the firewall software
- 
- 
- A Security Events connector
- A workbook

##### Answer Area

Enable alert notifications from Security Center:

A data connector for Security Center

Create an incident:

A rule

Initiate a script to configure the firewall rule:

A playbook

#### Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/create-incidents-from-alerts> <https://docs.microsoft.com/en-us/azure/sentinel/connect-azure-security-center>

#### Question: 295

CertyIQ

You have an Azure subscription that contains a resource group named RG1 and a security group named ServerAdmins. RG1 contains 10 virtual machines, a virtual network named VNET1, and a network security group (NSG) named NSG1. ServerAdmins can access the virtual machines by using RDP.

You need to ensure that NSG1 only allows RDP connections to the virtual machines for a maximum of 60 minutes when a member of ServerAdmins requests access.

What should you configure?

- A. an Azure policy assigned to RG1
- B. a just in time (JIT) VM access policy in Microsoft Defender for Cloud
- C. an Azure Active Directory (Azure AD) Privileged Identity Management (PIM) role assignment

D. an Azure Bastion host on VNET1

**Answer: B**

**Explanation:**

JIT can limit the time admins can access the servers.

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/just-in-time-explained>

**Question: 296**

**CertyIQ**

HOTSPOT -

You have an Azure subscription named Subscription1 that contains the resources shown in the following table.

Name	Type	Description
EventHub1	Azure Event Hubs	<b>Not applicable</b>
Adf1	Azure Data Factory	<b>Not applicable</b>
NVA1	Network virtual appliance (NVA)	The NVA sends security event messages in the Common Event Format (CEF).

You have an Azure subscription named Subscription2 that contains the following resources:

- An Azure Sentinel workspace
- An Azure Event Grid instance

You need to ingest the CEF messages from the NVA1 to Azure Sentinel.

What should you configure for each subscription? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

**Answer Area**

Subscription1:

Subscription2:

**Answer:**

**Answer Area**

Subscription1:

Subscription2:

**Explanation:**

Logs analytics agent and Sentinel data connector

<https://docs.microsoft.com/en-us/azure/sentinel/connect-cef-agent?tabs=rsyslog>

**Question: 297****CertyIQ**

HOTSPOT -

You have an Azure subscription named Subscription1 that contains a resource group named RG1 and a user named User1. User1 is assigned the Owner role for RG1.

You create an Azure Blueprints definition named Blueprint1 that includes a resource group named RG2 as shown in the following exhibit.

**Edit blueprint****Basics** Artifacts

Add artifacts to the blueprint. Add resource groups to organize where the artifacts should be deployed and assigned.

NAME	ARTIFACT TYPE	PARAMETERS
▼  Subscription		
+ Add artifact...		
▼  RG2	Resource group	2 out of 2 parameters populated
User1 (User1@sk200628outlook.onmicrosoft.com) : Tag Contributor	Role assignment	1 out of 1 parameters populated
+ Add artifact...		

You assign Blueprint1 to Subscription1 by using the following settings:

▸ Lock assignment: Read Only

▸ Managed Identity: System assigned

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

NOTE: Each correct selection is worth one point.

Hot Area:

**Answer Area**

Statements	Yes	No
A locking mode of Read Only will be assigned to RG1.	<input type="radio"/>	<input type="radio"/>
User1 can add tags to RG2.	<input type="radio"/>	<input type="radio"/>
You can remove User1 from the Tag Contributor role for RG2.	<input type="radio"/>	<input type="radio"/>

**Answer:**

## Answer Area

### Statements

Yes

No

A locking mode of Read Only will be assigned to RG1.

☐☒

User1 can add tags to RG2.

☐☒

You can remove User1 from the Tag Contributor role for RG2.

☐☒

### Explanation:

1. Blueprint doesn't work on existing resources.
2. RG2 is read-only and "The resource group is read only and tags on the resource group can't be modified. "
3. The newly created RG2 is read-only and nothing can be changed before you changed/deleted blueprint assignment.

## Question: 298

CertyIQ

You have an Azure Sentinel deployment.  
You need to create a scheduled query rule named Rule1.  
What should you use to define the query rule logic for Rule1?

- A. a Transact-SQL statement
- B. a JSON definition
- C. GraphQL
- D. a Kusto query

**Answer: D**

### Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/tutorial-detect-threats-custom>

## Question: 299

CertyIQ

You have an Azure subscription named Subscription1 that contains a resource group named RG1 and the users shown in the following table.

Name	User principal name (UPN)	Type
User1	User1@outlook.com	Guest
User2	User2@outlook.com	Guest

You perform the following tasks:

- Assign User1 the Network Contributor role for Subscription1.
- Assign User2 the Contributor role for RG1.

To Subscription1 and RG1, you assign the following policy definition: External accounts with write permissions should be removed from your subscription.

What is the Compliance State of the policy assignments?

- A. The Compliance State of both policy assignments is Non-compliant.
- B. The Compliance State of the policy assignment to Subscription1 is Compliant, and the Compliance State of the policy assignment to RG1 is Non-compliant.
- C. The Compliance State of the policy assignment to Subscription1 is Non-compliant, and the Compliance State of the policy assignment to RG1 is Compliant.
- D. The Compliance State of both policy assignments is Compliant.

**Answer: A**

**Explanation:**

The Compliance State of both policy assignments is Non-compliant.

### Question: 300

CertyIQ

HOTSPOT -

You have an Azure Sentinel workspace that has the following data connectors:

- ⇒ Azure Active Directory Identity Protection
- ⇒ Common Event Format (CEF)

Azure Firewall -

■ You need to ensure that data is being ingested from each connector.

From the Logs query window, which table should you query for each connector? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Azure Active Directory Identity Protection:

	▼
AzureDiagnostics	
CommonSecurityLog	
SecurityAlert	
SecurityEvent	
Syslog	

Azure Firewall:

	▼
AzureDiagnostics	
CommonSecurityLog	
SecurityAlert	
SecurityEvent	
Syslog	

CEF:

	▼
AzureDiagnostics	
CommonSecurityLog	
SecurityAlert	
SecurityEvent	
Syslog	

Answer:



## Answer Area

Azure Active Directory Identity Protection:

	▼
AzureDiagnostics	
CommonSecurityLog	
SecurityAlert	
SecurityEvent	
Syslog	

Azure Firewall:

	▼
AzureDiagnostics	
CommonSecurityLog	
SecurityAlert	
SecurityEvent	
Syslog	

CEF:

	▼
AzureDiagnostics	
CommonSecurityLog	
SecurityAlert	
SecurityEvent	
Syslog	

### Explanation:

1. Log Analytics table(s) SecurityAlert
2. Log Analytics table(s) AzureDiagnostics
3. CEF, set up the Syslog agent and then configure the CEF data flow. After successful configuration, the data appears in the CommonSecurityLog table.

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/connect-azure-ad-identity-protection>

<https://docs.microsoft.com/en-us/azure/sentinel/connect-azure-firewall> <https://docs.microsoft.com/en-us/azure/sentinel/connect-data-sources>

## Question: 301

CertyIQ

You have 10 on-premises servers that run Windows Server 2019.  
You plan to implement Azure Security Center vulnerability scanning for the servers.  
What should you install on the servers first?

- A. the Azure Arc enabled servers Connected Machine agent
- B. the Microsoft Defender for Endpoint agent
- C. the Security Events data connector in Azure Sentinel
- D. the Microsoft Endpoint Configuration Manager client

**Answer: A**

**Explanation:**

To deploy the vulnerability assessment scanner to your on-premises and multi-cloud machines, connect them to Azure first with Azure Arc as described in [Connect your non-Azure machines to Defender for Cloud](#).

Defender for Cloud's integrated vulnerability assessment solution works seamlessly with Azure Arc. When you've deployed Azure Arc, your machines will appear in Defender for Cloud and no Log Analytics agent is required.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-arc/servers/agent-overview> <https://docs.microsoft.com/en-us/azure/security-center/deploy-vulnerability-assessment-vm>

**Question: 302**

**CertyIQ**

HOTSPOT -

You have an Azure subscription that contains three storage accounts, an Azure SQL managed instance named SQL1, and three Azure SQL databases.

The storage accounts are configured as shown in the following table.

Name	Type	Performance
storage1	StorageV2	Standard
storage2	BlobStorage	Standard
storage3	StorageV2	Premium

SQL1 has the following settings:

- Auditing: On
- Audit log destination: storage1

The Azure SQL databases are configured as shown in the following table.

Name	On server	Auditing	Audit log destination
DB1	SQL1	Off	None
DB2	SQL1	On	storage2
DB3	SQL1	Off	None

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

NOTE: Each correct selection is worth one point.

Hot Area:

## Answer Area

Statements	Yes	No
Audit events for DB1 are written to storage1.	<input type="radio"/>	<input type="radio"/>
Audit events for DB2 are written to storage1 and storage2.	<input type="radio"/>	<input type="radio"/>
Storage3 can be used as an audit log destination for DB3.	<input type="radio"/>	<input type="radio"/>

Answer:

### Answer Area

Statements	Yes	No
Audit events for DB1 are written to storage1.	<input checked="" type="radio"/>	<input type="radio"/>
Audit events for DB2 are written to storage1 and storage2.	<input checked="" type="radio"/>	<input type="radio"/>
Storage3 can be used as an audit log destination for DB3.	<input checked="" type="radio"/>	<input type="radio"/>

Explanation:

Reference:

<https://learn.microsoft.com/en-us/azure/azure-sql/database/auditing-overview?view=azuresql>

Premium storage with BlockBlobStorage is supported. Standard storage is supported. However, for audit to write to a storage account behind a VNet or firewall, you must have a general-purpose v2 storage account.

### Question: 303

CertyIQ

You have an Azure subscription name Sub1 that contains an Azure Policy definition named Policy1. Policy1 has the following settings:

- Definition location: Tenant Root Group
- Category: Monitoring

You need to ensure that resources that are noncompliant with Policy1 are listed in the Azure Security Center dashboard.

What should you do first?

- A. Change the Category of Policy1 to Security Center.
- B. Add Policy1 to a custom initiative.
- C. Change the Definition location of Policy1 to Sub1.

D. Assign Policy1 to Sub1.

**Answer: B**

**Explanation:**

"you can add your own custom initiatives. You'll then receive recommendations if your environment doesn't follow the policies you create. Any custom initiatives you create will appear alongside the built-in initiatives in the regulatory compliance dashboard."

In my opinion the option D is wrong as the policy has been already assigned (to Tenant Root Group) - "As discussed in the Azure Policy documentation, when you specify a location for your custom initiative, it must be a management group or a subscription."

<https://docs.microsoft.com/en-us/azure/defender-for-cloud/custom-security-policies>

### Question: 304

CertyIQ

You have an Azure subscription.

You plan to create a workflow automation in Azure Security Center that will automatically remediate a security vulnerability.

What should you create first?

- A. an automation account
- B. a managed identity
- C. an Azure logic app
- D. an Azure function app
- E. an alert rule

**Answer: C**

**Explanation:**

When you add a 'Add workflow automation' in step 2B of this create and assign workflow, you can either select an existing Logic App or Create one, regardless it is needed for assigning an 'Add workflow automation'

b. The triggers that will initiate this automatic workflow. For example, you might want your Logic App to run when a security alert that contains "SQL" is generated.

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/workflow-automation>

### Question: 305

CertyIQ

SIMULATION -

A user named Debbie has the Azure app installed on her mobile device.

You need to ensure that [email protected] is alerted when a resource lock is deleted.

To complete this task, sign in to the Azure portal.

**Answer:**

See the explanation below.

**Explanation:**

You need to configure an alert rule in Azure Monitor.

1. Type Monitor into the search box and select Monitor from the search results.
2. Click on Alerts.
3. Click on +New Alert Rule.
4. In the Scope section, click on the Select resource link.
5. In the Filter by resource type box, type locks and select Management locks (locks) from the filtered results.
6. Select the subscription then click the Done button.
7. In the Condition section, click on the Select condition link.
8. Select the Delete management locks condition then click the Done button.
9. In the Action group section, click on the Select action group link.
10. Click the Create action group button to create a new action group.
11. Give the group a name such as Debbie Mobile App (it doesn't matter what name you enter for the exam) then click the Next: Notifications > button.
12. In the Notification type box, select the Email/SMS message/Push/Voice option.
13. In the Email/SMS message/Push/Voice window, tick the Azure app Push Notifications checkbox and enter [email protected] in the Azure account email field.
14. Click the OK button to close the window.
15. Enter a name such as Debbie Mobile App in the notification name box.
16. Click the Review & Create button then click the Create button to create the action group.
17. Back in the Create alert rule window, in the Alert rule details section, enter a name such as Management lock deletion in the Alert rule name field.
18. Click the Create alert rule button to create the alert rule.

**Question: 306**

CertyIQ

**SIMULATION -**

You plan to connect several Windows servers to the WS12345678 Azure Log Analytics workspace. You need to ensure that the events in the System event logs are collected automatically to the workspace after you connect the Windows servers. To complete this task, sign in to the Azure portal and modify the Azure resources.

**Answer:**

See the explanation below.

**Explanation:**

Azure Monitor can collect events from the Windows event logs or Linux Syslog and performance counters that you specify for longer term analysis and reporting, and take action when a particular condition is detected. Follow these steps to configure collection of events from the Windows system log and Linux Syslog, and several common performance counters to start with.

**Data collection from Windows VM -**

1. In the Azure portal, locate the WS12345678 Azure Log Analytics workspace then select Advanced settings.



# DefaultLAWorkspace

Log Analytics workspace



Overview



Activity log



Access control (IAM)



Tags



Diagnose and solve problems

## Settings



Locks



Export template



Advanced settings

2. Select Data, and then select Windows Event Logs.
3. You add an event log by typing in the name of the log. Type System and then select the plus sign +.
4. In the table, check the severities Error and Warning. (for this question, select all severities to ensure that ALL logs are collected).
5. Select Save at the top of the page to save the configuration.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-monitor/learn/quick-collect-azurevm>

### Question: 307

CertyIQ

SIMULATION -

You need to ensure that the AzureBackupReport log for the Vault1 Recovery Services vault is stored in the WS12345678 Azure Log Analytics workspace.

To complete this task, sign in to the Azure portal and modify the Azure resources.

Answer:



See the explanation below.

**Explanation:**

1. In the Azure portal, type Recovery Services Vaults in the search box, select Recovery Services Vaults from the search results then select Vault1.  
Alternatively, browse to Recovery Services Vaults in the left navigation pane.
2. In the properties of Vault1, scroll down to the Monitoring section and select Diagnostic Settings.
3. Click the Add a diagnostic setting link.
4. Enter a name in the Diagnostic settings name box.
5. In the Log section, select AzureBackupReport.

### Category details

#### log

☐ AzureBackupReport

☐ CoreAzureBackup

☐ AddonAzureBackupJobs

☐ AddonAzureBackupAlerts

☐ AddonAzureBackupPolicy

6. In the Destination details section, select Send to log analytics

### Destination details

☐ Send to Log Analytics

☐ Archive to a storage account

☐ Stream to an event hub

7. Select the WS12345678 Azure Log Analytics workspace.

8. Click the Save button to save the changes.

Reference:

<https://docs.microsoft.com/en-us/azure/backup/backup-azure-diagnostic-events>

### Question: 308

CertyIQ

SIMULATION -

You need to ensure that the audit logs from the SQLdb1 Azure SQL database are stored in the WS12345678 Azure Log Analytics workspace.

To complete this task, sign in to the Azure portal and modify the Azure resources.

#### Answer:

See explanation below.

#### Explanation:

1. In the Azure portal, type SQL in the search box, select SQL databases from the search results then select SQLdb1. Alternatively, browse to SQL databases in the left navigation pane.
2. In the properties of SQLdb1, scroll down to the Security section and select Auditing.
3. Turn auditing on if it isn't already, tick the Log Analytics checkbox then click on Configure.

#### Auditing ⓘ

ON

OFF

Audit log destination (choose at least one):

☐

Storage

☒

Log Analytics (Preview)

---

Log Analytics details

Configure

---

☐

Event Hub (Preview)

4. Select the WS12345678 Azure Log Analytics workspace.

5. Click Save to save the changes.

### Question: 309

CertyIQ

HOTSPOT -

You are configuring just in time (JIT) VM access to a Windows Server 2019 Azure virtual machine.

You need to grant users PowerShell access to the virtual machine by using JIT VM access.

What should you configure? To answer, select the appropriate options in the answer area.

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

Answer Area

Permission that must be granted to users on VM:

	▼
Read	
Update	
View	
Write	

TCP port that must be allowed:

	▼
22	
25	
3389	
5986	

Answer:

Answer Area

Permission that must be granted to users on VM:

	▼
Read	
Update	
View	
Write	

TCP port that must be allowed:

	▼
22	
25	
3389	
5986	

Explanation:

READ  
5986

Question: 310

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

Name	Type	Region	Resource group
SQL1	Azure SQL database	East US	RG1
Analytics1	Azure Log Analytics workspace	East US	RG1
Analytics2	Azure Log Analytics workspace	East US	RG2
Analytics3	Azure Log Analytics workspace	West Europe	RG1

You create the Azure Storage accounts shown in the following table.

Name	Region	Resource group	Storage account type	Access tier (default)
Storage1	East US	RG1	Blob	Cool
Storage2	East US	RG2	General purpose V1	<i>Not applicable</i>
Storage3	West Europe	RG1	General purpose V2	Hot

You need to configure auditing for SQL1.

Which storage accounts and Log Analytics workspaces can you use as the audit log destination? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

### Answer Area

Storage accounts that can be used as the audit log destination:

▼

Storage1 only

Storage2 only

Storage1 and Storage2 only

Storage1, Storage2, and Storage3

Log Analytics workspaces that can be used as the audit log destination:

▼

Analytics1 only

Analytics1 and Analytics2 only

Analytics1 and Analytics3 only

Analytics1, Analytics2, and Analytics3

Answer:

### Answer Area

Storage accounts that can be used as the audit log destination:

▼

Storage1 only

Storage2 only

Storage1 and Storage2 only

Storage1, Storage2, and Storage3

Log Analytics workspaces that can be used as the audit log destination:

▼

Analytics1 only

Analytics1 and Analytics2 only

Analytics1 and Analytics3 only

Analytics1, Analytics2, and Analytics3

Explanation:

Storage 1 and 2

Log analytics 1,2 and 3

<https://docs.microsoft.com/en-us/azure/azure-sql/database/audit-log-format#:~:text=Blob%20audit,in%20the%20Azure%20storage%20account.>

### Question: 311

CertyIQ

You are troubleshooting a security issue for an Azure Storage account. You enable the diagnostic logs for the storage account. What should you use to retrieve the diagnostics logs?

- A. Azure Storage Explorer
- B. SQL query editor in Azure
- C. File Explorer in Windows
- D. Azure Security Center

**Answer: A**

#### Explanation:

If you want to download the metrics for long-term storage or to analyze them locally, you must use a tool or write some code to read the tables. You must download the minute metrics for analysis. The tables do not appear if you list all the tables in your storage account, but you can access them directly by name.

Many storage-browsing tools are aware of these tables and enable you to view them directly (see Azure Storage Client Tools for a list of available tools).

Microsoft provides several graphical user interface (GUI) tools for working with the data in your Azure Storage account. All of the tools outlined in the following table are free.

Azure Storage client tool	Supported platforms	Block Blob	Page Blob	Append Blob	Tables	Queues	Files
Azure portal	Web	Yes	Yes	Yes	Yes	Yes	Yes
Azure Storage Explorer	Windows, OSX	Yes	Yes	Yes	Yes	Yes	Yes
Microsoft Visual Studio Cloud Explorer	Windows	Yes	Yes	Yes	Yes	Yes	No

Note:

There are several versions of this question in the exam. The questions in the exam have two different correct answers:

1. Azure Storage Explorer
2. AZCopy

Other incorrect answer options you may see on the exam include the following:

1. Azure Monitor
2. The Security & Compliance admin center
3. Azure Cosmos DB explorer
4. Azure Monitor

Reference:

<https://docs.microsoft.com/en-us/azure/storage/common/storage-analytics-metrics?toc=%2fazure%2fstorage%2fblobs%2ftoc.json> <https://docs.microsoft.com/en-us/azure/storage/common/storage-explorers>

**Question: 312**

You are troubleshooting a security issue for an Azure Storage account.  
You enable Azure Storage Analytics logs and archive it to a storage account.  
What should you use to retrieve the diagnostics logs?

- A. Azure Cosmos DB explorer
- B. SQL query editor in Azure
- C. AzCopy
- D. the Security admin center

**Answer: C****Explanation:**

Files are saved on a storage account, you can utilize Az-copy to retrieve the Files.

<https://docs.microsoft.com/en-us/azure/storage/common/storage-use-azcopy-v10>

**Question: 313**

You have an Azure Sentinel workspace.  
You need to create a playbook.  
Which two triggers will start the playbook? Each correct answer presents a complete solution.  
NOTE: Each correct selection is worth one point.

- A. An Azure Sentinel scheduled query rule is executed.
- B. An Azure Sentinel data connector is added.
- C. An Azure Sentinel alert is generated.
- D. An Azure Sentinel hunting query result is returned.
- E. An Azure Sentinel incident is created.

**Answer: CE****Explanation:**

C. An Azure Sentinel alert is generated. E: An Azure Sentinel Incident is created

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook>

**Question: 314**

You are troubleshooting a security issue for an Azure Storage account.  
You enable Azure Storage Analytics logs and archive it to a storage account.  
What should you use to retrieve the diagnostics logs?

- A. Azure Monitor
- B. SQL query editor in Azure
- C. File Explorer in Windows
- D. Azure Storage Explorer



**Answer: D**

**Explanation:**

Its either AzCopy or Storage Explorer, we have seen this question numerous times. Very easy to remember.

### Question: 315

CertyIQ

You have an Azure Active Directory (Azure AD) tenant that contains a user named User1.

You plan to enable passwordless authentication for the tenant.

You need to ensure that User1 can enable the combined registration experience. The solution must use the principle of least privilege.

Which role should you assign to User1?

- A. Security administrator
- B. Privileged role administrator
- C. Authentication administrator
- D. Global administrator

**Answer: D**

**Explanation:**

Sign in to the Azure portal as a user administrator or global administrator.

### Question: 316

CertyIQ

You are troubleshooting a security issue for an Azure Storage account.

You enable Azure Storage Analytics logs and archive it to a storage account.

What should you use to retrieve the diagnostics logs?

- A. Azure Cosmos DB explorer
- B. Azure Monitor
- C. Microsoft Defender for Cloud
- D. Azure Storage Explorer

**Answer: D**

**Explanation:**

One of the simplest ways to set/get an Azure Storage Blob's metadata is by using the cross-platform Microsoft Azure Storage Explorer, which is a standalone app from Microsoft that allows you to easily work with Azure Storage data on Windows, macOS and Linux.

Note: All logs are stored in block blobs in a container named \$logs, which is automatically created when Storage Analytics is enabled for a storage account.

If you use your storage-browsing tool to navigate to the container directly, you will see all the blobs that contain your logging data. Most storage browsing tools enable you to view the metadata of blobs; you can also read this information using PowerShell or programmatically.

Reference:

<https://azure.microsoft.com/en-us/features/storage-explorer/>

<https://docs.microsoft.com/en-us/azure/storage/common/storage-analytics-logging>

**Question: 317**

CertyIQ

You have the Azure resources shown in the following table.

Name	Type	Parent
Management1	Management group	Tenant Root Group
Subscription1	Subscription	Management1
RG1	Resource group	Subscription1
RG2	Resource group	Subscription1
VM1	Virtual machine	RG1
VM2	Virtual machine	RG2

You need to meet the following requirements:

- ⇒ Internet-facing virtual machines must be protected by using network security groups (NSGs).
- ⇒ All the virtual machines must have disk encryption enabled.

What is the minimum number of security policies that you should create in Microsoft Defender for Cloud?

- A. 1
- B. 2
- C. 3
- D. 4

**Answer: B****Explanation:**

just apply it to the scope to the subscription or management group

**Question: 318**

CertyIQ

HOTSPOT -

You have an Azure subscription that contains an Azure key vault. The role assignments for the key vault are shown in the following exhibit.

```
[
  {
    "RoleAssignmentId": "3336fcbf-33d8-4c8a-85b6-d8edd964762b",
    "Scope": "/subscriptions/76c42af2-b40d-48fd-bf3b-de37baaa7ffa",
    "DisplayName": "User1",
    "SignInName": "User1@contoso.com",
    "RoleDefinitionName": "Owner",
    ...
  },
  {
    "RoleAssignment": "9d080a14-246e-4580-8b8b-077bfec22f7c",
    "Scope": "/subscriptions/76c42af2-b40d-48fd-bf3b-de37baaa7ffa/resourceGroups/RG1/providers/Microsoft.KeyVault/vaults/KeyVault1",
    "DisplayName": "User2",
    "SignInName": "User2@contoso.com",
    "RoleDefinitionName": "Key Vault Crypto Officer",
    ...
  },
  {
    "RoleAssignmentId": "0d61eae6-4612-4ee2-88f3-fb6dab84eb10",
    "Scope": "/subscriptions/76c42af2-b40d-48fd-bf3b-de37baaa7ffa/resourceGroups/RG1/providers/Microsoft.KeyVault/vaults/KeyVault1",
    "DisplayName": "User3",
    "SignInName": "User3@contoso.com",
    "RoleDefinitionName": "Key Vault Secrets Officer",
    ...
  },
  {
    "RoleAssignmentId": "f1e46302-c5d0-4519-9ee7-128594eea97c",
    "Scope": "/subscriptions/76c42af2-b40d-48fd-bf3b-de37baaa7ffa/resourceGroups/RG3/providers/Microsoft.KeyVault/vaults/KeyVault1/keys/Key1",
    "DisplayName": "User4",
    "SignInName": "User4@contoso.com",
    "RoleDefinitionName": "Key Vault Administrator",
    ...
  }
]
```

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

NOTE: Each correct selection is worth one point.

Hot Area:

## Answer Area

**[Answer choice]** can create keys in the key vault.

	▼
Only User1	
Only User2	
Only User1 and User4	
Only User1, User2, and User4	
User1, User2, User3, and User4	

**[Answer choice]** can create secrets in the key vault.

	▼
Only User3	
Only User1 and User3	
Only User3 and User4	
Only User1, User3, and User4	
User1, User2, User3, and User4	

Answer:

## Answer Area

[Answer choice] can create keys in the key vault.

	▼
Only User1	
Only User2	
Only User1 and User4	
Only User1, User2, and User4	
User1, User2, User3, and User4	

[Answer choice] can create secrets in the key vault.

	▼
Only User3	
Only User1 and User3	
Only User3 and User4	
Only User1, User3, and User4	
User1, User2, User3, and User4	

### Explanation:

User1 - has ownership at subscription level therefore has access to the control plane of the key vault but not to the data plane. therefore User1 can manage RBAC permissions but cannot create/access keys or secrets (unless they can grant themselves 'Key Administrator' access and do this, which again does not show up in this RBACs listed so we cannot assume that)

- Therefore User1 has not access to the keys or secrets in this vault

User2 - Is a Key Vault Crypto officer for the KeyVault1. so according to this:<https://learn.microsoft.com/en-us/azure/key-vault/general/rbac-guide?tabs=azure-cli#azure-built-in-roles-for-key-vault-data-plane-operations>, they can manage keys (but not access secrets or manage permissions)

User3 - Is a Secrets officer for the KeyVault1 scope. they can access secrets data in this key vault

User4 - Here's a tricky one. while they are indeed given 'Key Vault Administrator', notice the scope is set to "../KeyVault1/Keys/Key1". So they should only be able to work with that key.

1st box - Only User2

2nd box - Only User3

### Question: 319

CertyIQ

HOTSPOT -

You have an Azure subscription that contains a blob container named cont1. Cont1 has the access policies shown in the following exhibit.

## Stored access policies

Identifier	Start time	Expiry time	Permissions
Policy1			r ...

+ Add policy

## Immutable blob storage ⓘ

Identifier	Retention interval	State
Time-based retention	20 days	Unlocked ...

+ Add policy

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

NOTE: Each correct selection is worth one point.

Hot Area:

## Answer Area

The maximum number of additional stored access policies that you can add to cont1 is

	▼
1	
2	
4	
7	
15	

The maximum number of additional immutable blob storage policies that you can add to cont1 is

	▼
1	
2	
4	
7	
15	



Answer:

## Answer Area

The maximum number of additional stored access policies that you can add to cont1 is

	▼
1	
2	
4	
7	
15	

The maximum number of additional immutable blob storage policies that you can add to cont1 is

	▼
1	
2	
4	
7	
15	

### Explanation:

Box 1: 4 -

A container can have up to 5 stored access policies.

Maximum number of stored access policies per blob container: 5

Box 2: 1 -

Blob version supports one version-level immutability policy and one legal hold. A policy on a blob version can override a default policy specified on the account or container.

Reference:

<https://docs.microsoft.com/en-us/azure/storage/blobs/scalability-targets> <https://docs.microsoft.com/en-us/azure/storage/blobs/immutable-storage-overview>

### Question: 320

CertyIQ

You have an Azure subscription that contains a resource group named RG1 and the network security groups (NSGs) shown in the following table.

Name	Location	Flow logs status
NSG1	West Europe	Off
NSG2	West Europe	Off

You create the Azure policy shown in the following exhibit.



# Assign policy ...

Basics

Parameters

Remediation

Non-compliance messages

Review + create

## Basics

Scope

Azure Pass - Sponsorship/RG1

Exclusions

Azure Pass - Sponsorship/RG1/NSG1

Policy definition

Flow logs should be enabled for every network security group

Assignment name

Flow logs should be enabled for every network security group

Description

Description1

Policy enforcement

Enabled

Assigned by

Admin1

## Parameters

effect

Audit

## Remediation

Create managed identity

Yes

Managed identity location

westeurope

Create a remediation task

No

## Non-compliance messages

Default non-compliance message

Message1

You assign the policy to RG1.

What will occur if you assign the policy to NSG1 and NSG2?

- A. Flow logs will be enabled for NSG2 only.
- B. Flow logs will be disabled for NSG1 and NSG2.
- C. Flow logs will be enabled for NSG1 and NSG2.
- D. Flow logs will be enabled for NSG1 only.

**Answer: B**

**Explanation:**

This is an audit policy with an exception for NSG1. Since Network Flow Log is disabled on NSG1 and NSG2 it remains disabled. You need DeployIfNotExists effect to activate NFL.

We are launching two built-in policies for deploying NSG Flow Logs

- An Audit policy: Flag NSGs without Flow logs enabled
- A DeployIfNotExists policy: Enable Flow logs on NSGs where it is disabled

Get started with our tutorial for using the above policies.

Reference:

<https://azure.microsoft.com/en-us/updates/nsg-flow-logs-built-in-azure-policy/>

### Question: 321

CertyIQ

HOTSPOT

-

You have an Azure Active Directory (Azure AD) tenant named contoso.com that has Azure Active Directory Premium Plan 1 licenses.

You need to create a group named Group1 that will be assigned the Global reader role.

Which portal should you use to create Group1, and which type of group should you create? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

### Answer Area

Portal:

▼

The Azure Active Directory admin center only  
The Microsoft 365 admin center only  
The Azure Active Directory admin center on the Microsoft 365 admin center

Group type:

▼

Security only  
Microsoft 365 only  
Security or mail-enabled security only  
Security or Microsoft 365 only  
Security, Microsoft 365, or mail-enabled security

Answer:

## Answer Area

Portal:  ▼

Group type:  ▼

### Question: 322

CertyIQ

HOTSPOT

You have a management group named MG1 that contains an Azure subscription and a resource group named RG1. RG1 contains a virtual machine named VM1.

You have the custom Azure roles shown in the following table.

Name	Scoped to
Role1	MG1
Role2	RG1

The permissions for Role1 are shown in the following role definition file.

```
"permissions": [  
  {  
    "Actions": [  
    ],  
    "notActions": [  
      "Microsoft.Compute/virtualMachines/delete"  
    ],  
    "dataActions": [],  
    "notDataActions": []  
  }  
]
```

The permissions for Role2 are shown in the following role definition file.

```
"permissions": [
  {
    "actions": [
      "Microsoft.Compute/virtualMachines/*"
    ],
    "notActions": [],
    "dataActions": [],
    "notDataActions": []
  }
]
```

You assign the roles to the users shown in the following table.

Name	Role
User1	Role1
User2	Role1, Role2
User3	Role2

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

NOTE: Each correct selection is worth one point.

## Answer Area

Statements	Yes	No
User1 can delete VM1.	<input type="radio"/>	<input type="radio"/>
User2 can delete VM1.	<input type="radio"/>	<input type="radio"/>
User3 can delete VM1.	<input type="radio"/>	<input type="radio"/>

Answer:

## Answer Area

Statements	Yes	No
User1 can delete VM1.	<input type="radio"/>	<input checked="" type="radio"/>
User2 can delete VM1.	<input checked="" type="radio"/>	<input type="radio"/>
User3 can delete VM1.	<input checked="" type="radio"/>	<input type="radio"/>

### Explanation:

no

yes

yes

NotActions are not DENY actions. They're only used to scope down \* action by removing one or many actions from \* (which is usually less lines to write that listing all available actions when creating a custom role).

### Question: 323

CertyIQ

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

You need to prevent nonprivileged Azure AD users from creating service principles in Azure AD.

What should you do in the Azure Active Directory admin center of the tenant?

- A. From the User settings blade, set Users can register applications to No.
- B. From the Properties blade, set Access management for Azure resources to No.
- C. From the User settings blade, set Restrict access to Azure AD administration portal to Yes.
- D. From the Properties blade, set Enable Security defaults to Yes.

**Answer: A**

### Explanation:

From the User settings blade, set Users can register applications to No.

### Question: 324

CertyIQ

HOTSPOT

-

You have an Azure subscription that contains the following Azure firewall:

- Name: Fw1
- Azure region: UK West
- Private IP address: 10.1.3.4
- Public IP address: 23.236.62.147

The subscription contains the virtual networks shown in the following table.

Name	Location	IP address space	Peered with
Vnet1	UK West	10.1.0.0/16	Vnet2
Vnet2	East US	10.2.0.0/16	Vnet1, Vnet3
Vnet3	West US	10.3.0.0/16	Vnet2,

The subscription contains the subnets shown in the following table.

Name	Virtual network	IP address range
Subnet1-1	Vnet1	10.1.1.0/24
Subnet1-2	Vnet1	10.1.2.0/24
AzureFirewallSubnet	Vnet1	10.1.3.0/24
Subnet2-1	Vnet2	10.2.1.0/24
Subnet3-1	Vnet3	10.3.1.0/24

The subscription contains the routes shown in the following table.

Name	Subnet	IP address prefix	Next hop type	Next hop IP address
Rt1	Subnet1-1	0.0.0.0/0	Virtual appliance	10.1.3.4
Rt2	Subnet1-2	10.1.1.0/24	Virtual appliance	10.1.3.4
Rt3	Subnet2-1	10.1.1.0/24	Virtual appliance	10.1.3.4
Rt4	Subnet3-1	10.2.1.0/24	Virtual appliance	10.1.3.4

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

NOTE: Each correct selection is worth one point.

Statements	Yes	No
Traffic from Subnet1-1 to Subnet 1-2 is routed through Fw1.	<input type="radio"/>	<input type="radio"/>
Traffic from Subnet2-1 to Subnet 1-1 is routed through Fw1.	<input type="radio"/>	<input type="radio"/>
Traffic from Subnet3-1 to the internet is routed through Fw1.	<input type="radio"/>	<input type="radio"/>

Answer:



**Statements****Yes****No**

Traffic from Subnet1-1 to Subnet 1-2 is routed through Fw1.

☒☐

Traffic from Subnet2-1 to Subnet 1-1 is routed through Fw1.

☒☐

Traffic from Subnet3-1 to the internet is routed through Fw1.

☐☒**Explanation:**

Yes: Rt1 will route from Subnet1-1 to any IP (0.0.0.0/0) including Subnet2-1 to the FW (10.1.3.4)

Yes: Rt3 will route from Subnet2-1 to Subnet1-1 (10.1.1.0/24) to the FW (10.1.3.4)

No: There is no configured route from Subnet3-1 to the internet via FW, thus it will go directly to the internet bypassing the FW.

**Question: 325****CertyIQ**

HOTSPOT

-

You have an Azure subscription that contains a user named User1 and a storage account named storage1. The storage1 account contains the resources shown in the following table.

Name	Type
container1	Container
folder1	File Share
table1	Table

In storage1, you create a shared access signature (SAS) named SAS1 as shown in the following exhibit.

Allowed services ⓘ

☐ Blob ☒ File ☐ Queue ☐ Table

Allowed resource types ⓘ

☒ Service ☒ Container ☒ Object

Allowed permissions ⓘ

☒ Read ☒ Write ☒ Delete ☒ List ☐ Add ☒ Create ☐ Update ☐ Process ☐ Immutable storage

Blob versioning permissions ⓘ

☐ Enables deletion of versions

Allowed blob index permissions ⓘ

☐ Read/Write ☐ Filter

Start and expiry date/time ⓘ

Start

End

Allowed IP addresses ⓘ

Allowed protocols ⓘ

☒ HTTPS only ☐ HTTPS and HTTP

Preferred routing tier ⓘ

☒ Basic (default) ☐ Microsoft network routing ☐ Internet routing

Some routing options are disabled because the endpoints are not published.

Signing key ⓘ

To which resources can User1 write on July 1, 2022 by using SAS1 and key1? To answer select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

## Answer Area

SAS1

	▼
folder1 only container and folder1 only folder1 and table1 only container1 and table1 only container1, folder1 and table1	

Key1

	▼
folder1 only container and folder1 only folder1 and table1 only container1 and table1 only container1, folder1 and table1	

Answer:

## Answer Area

SAS1

	▼
folder1 only	
container and folder1 only	
folder1 and table1 only	
container1 and table1 only	
container1, folder1 and table1	

Key1

	▼
folder1 only	
container and folder1 only	
folder1 and table1 only	
container1 and table1 only	
container1, folder1 and table1	

### Explanation:

SAS1: folder1

KEY1: container1, folder1, table1

Don't think of a container mentioned there as blob container. Think of it as something that will have child elements (objects in this case).

In context of blobs, container will refer to blob container which will contain blobs.

In context of file service, container will refer to share which will contain files & directories.

In context of table service, container will refer to table which will contain entities.

In context of queue service, container will refer to queue which will contain messages.

Reference:

<https://stackoverflow.com/questions/43446426/relationship-between-azure-sas-allowed-services-and-allowed-resource-types>

### Question: 326

CertyIQ

You have an Azure subscription that contains a managed identity named Identity1 and the Azure key vaults shown in the following table.

Name	Permission model
KeyVault1	Vault access policy
KeyVault2	Azure role-based access control (Azure RBAC)

KeyVault1 contains an access policy that grants Identity1 the following key permissions:

- Get
- List
- Wrap
- Unwrap

You need to provide Identity1 with the same permissions for KeyVault2. The solution must use the principle of least privilege.

Which role should you assign to Identity1?

- A. Key Vault Crypto Service Encryption User
- B. Key Vault Crypto User
- C. Key Vault Reader
- D. Key Vault Crypto Officer

**Answer: A**

**Explanation:**

Key Vault Crypto Service Encryption User

"dataActions": [

"Microsoft.KeyVault/vaults/keys/read",

List keys in the specified vault, or read properties and public material of a key. For asymmetric keys, this operation exposes public key and includes ability to perform public key algorithms such as encrypt and verify signature. Private keys and symmetric keys are never exposed.

"Microsoft.KeyVault/vaults/keys/wrap/action",

Wraps a symmetric key with a Key Vault key. Note that if the Key Vault key is asymmetric, this operation can be performed by principals with read access.

"Microsoft.KeyVault/vaults/keys/unwrap/action"

Unwraps a symmetric key with a Key Vault key.

## Question: 327

CertyIQ

HOTSPOT

-

You have an Azure subscription that contains a user named User1. User1 is assigned the Reader role for the subscription.

You plan to create a custom role named Role1 and assign Role1 to User1.

You need to ensure that User1 can create and manage application security groups by using Azure portal.

Which two permissions should you add to Role1? To answer, select the appropriate permissions in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

**Add permissions**

<b>Microsoft Monitoring Insights</b> Microsoft.SecurityGraph	<b>Microsoft Monitoring Insights</b> Enable your workforce to be productive on all their devices, while keeping your organization's information protected.	<b>Microsoft Monitoring Insights</b> Microsoft.DynamicsTelemetry	<b>Microsoft Network</b> Connect cloud and on-premises infrastructure and services to provide your customers and users the best.
<b>Microsoft Operations Management</b> A simplified management solution for any enterprise	<b>Microsoft Policy Insights</b> Summarize policy states for the subscription level policy definition.	<b>Microsoft Portal</b> Build, manage, and monitor all Azure products in a single, unified console.	<b>Microsoft Power BI Dedicated</b> Manage Power BI Premium dedicated capacities for exclusive use by an organization.
<b>Microsoft Power Platform</b> Microsoft.PowerPlatform	<b>Microsoft Project Babylon</b> Microsoft.ProjectBabylon	<b>Microsoft Purview</b> Microsoft.Purview	<b>Microsoft Resource Graph</b> Powerful tool to query, explore, and analyze your cloud resources at scale.

**Answer:**

**Answer Area**

**Add permissions**

<b>Microsoft Monitoring Insights</b> Microsoft.SecurityGraph	<b>Microsoft Monitoring Insights</b> Enable your workforce to be productive on all their devices, while keeping your organization's information protected.	<b>Microsoft Monitoring Insights</b> Microsoft.DynamicsTelemetry	<b>Microsoft Network</b> Connect cloud and on-premises infrastructure and services to provide your customers and users the best.
<b>Microsoft Operations Management</b> A simplified management solution for any enterprise	<b>Microsoft Policy Insights</b> Summarize policy states for the subscription level policy definition.	<b>Microsoft Portal</b> Build, manage, and monitor all Azure products in a single, unified console.	<b>Microsoft Power BI Dedicated</b> Manage Power BI Premium dedicated capacities for exclusive use by an organization.
<b>Microsoft Power Platform</b> Microsoft.PowerPlatform	<b>Microsoft Project Babylon</b> Microsoft.ProjectBabylon	<b>Microsoft Purview</b> Microsoft.Purview	<b>Microsoft Resource Graph</b> Powerful tool to query, explore, and analyze your cloud resources at scale.

**Question: 328**

CertyIQ

You have an Azure subscription named Sub1.

In Microsoft Defender for Cloud, you have a workflow automation named WF1. WF1 is configured to send an email message to a user named User1.

You need to modify WF1 to send email messages to a distribution group named Alerts.

What should you use to modify WF1?

- A. Azure Logic Apps Designer
- B. Azure Application Insights
- C. Azure DevOps
- D. Azure Monitor

**Answer: A**

**Explanation:**

A is correct! When you work with Azure Logic Apps in the Azure portal, you can edit your workflows visually or programmatically.

<https://learn.microsoft.com/en-us/azure/logic-apps/designer-overview>



### Question: 329

#### DRAG DROP

You have an Azure subscription that contains a resource group named RG1 and an Azure policy named Policy1.

You need to assign Policy1 to RG1.

How should you complete the script? To answer, drag the appropriate values to the correct targets. Each value may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

#### Values

Get-AzPolicyAssignment

Get-AzPolicyDefinition

Get-AzPolicySetDefinition

New-AzPolicyAssignment

New-AzPolicyDefinition

#### Answer Area

```
$rg = Get-AzResourceGroup -Name 'RG1'
```

```
$Policy = [Value] -Name 'Policy1'
```

```
[Value] -Name 'AuditStorageAccounts' -PolicyDefinition
```

```
$Policy -Scope $rg.ResourceID
```

#### Answer:

#### Answer Area

```
$rg = Get-AzResourceGroup -Name 'RG1'
```

```
$Policy = Get-AzPolicyDefinition -Name 'Policy1'
```

```
New-AzPolicyAssignment -Name 'AuditStorageAccounts' -PolicyDefinition
```

```
$Policy -Scope $rg.ResourceID
```

## HOTSPOT

-

You have an Azure subscription named Sub1 that contains the resource groups shown in the following table.

Name	Location
RG1	West US
RG2	EAST US

You create the Azure Policy definition shown in the following exhibit.

```
{
  "mode": "All",
  "policyRule": {
    "if": {
      "anyOf": [
        {
          "field": "location",
          "notEquals": "[resourceGroup().location]"
        },
        {
          "field": "name",
          "notContains": "obj"
        }
      ]
    },
    "then": {
      "effect": "deny"
    }
  },
  "parameters": {}
}
```

You assign the policy to Sub1.

You plan to create the resources shown in the following table.

Name	Type	Location	Resource Group
IPobject1	Public IP address	East US	RG2
obj1	Resource group	West US	<i>Not applicable</i>
OBJ3	Virtual network	West US	RG1

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

NOTE: Each correct selection is worth one point.

### Answer Area

Statements	Yes	No
You can create IPobject1.	<input type="radio"/>	<input type="radio"/>
You can create obj1.	<input type="radio"/>	<input type="radio"/>
You can create OBJ3.	<input type="radio"/>	<input type="radio"/>

Answer:

### Answer Area

Statements	Yes	No
You can create IPobject1.	<input checked="" type="radio"/>	<input type="radio"/>
You can create obj1.	<input type="radio"/>	<input checked="" type="radio"/>
You can create OBJ3.	<input checked="" type="radio"/>	<input type="radio"/>

### Question: 331

CertyIQ

Your on-premises network contains a Hyper-V virtual machine named VM1.

You need to use Azure Arc to onboard VM1 to Microsoft Defender for Cloud.

What should you install first?

- A.the guest configuration agent
- B.the Azure Monitor agent
- C.the Log Analytics agent
- D.the Azure Connected Machine agent

**Answer: D**

**Explanation:**

It should be D

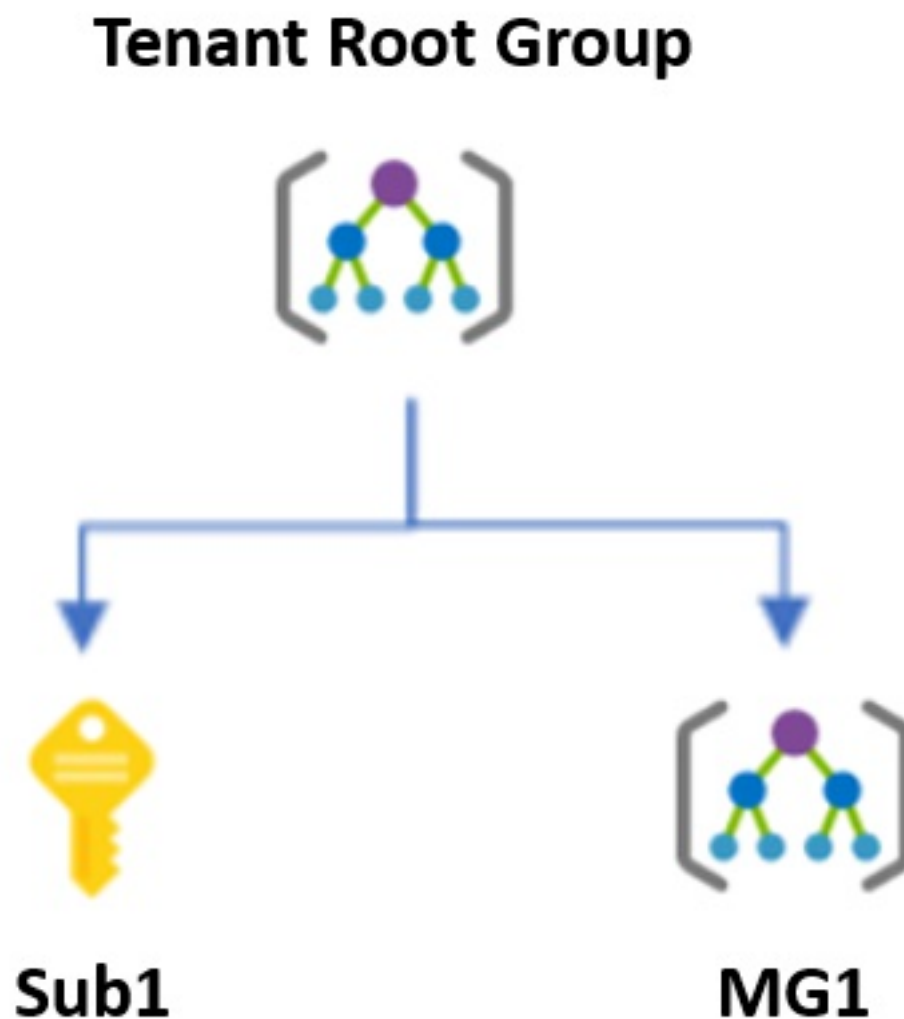
The Azure Connected Machine agent enables you to manage your Windows and Linux machines hosted outside of Azure on your corporate network or other cloud providers.

**Question: 332**

**CertyIQ**

You have an Azure subscription named Sub1 that uses Microsoft Defender for Cloud.

You have the management group hierarchy shown in the following exhibit.



You create the definitions shown in the following table.

Name	Location	Type
Policy1	Sub1	Policy
Initiative1	Tenant Root Group	Initiative
Initiative2	Sub1	Initiative
Initiative3	MG1	Initiative

You need to use Defender for Cloud to add a security policy.

Which definitions can you use as a security policy?

- A. Policy1 only
- B. Policy1 and Initiative1 only
- C. Initiative1 and Initiative2 only
- D. Initiative1, Initiative2, and Initiative3 only
- E. Policy1, Initiative1, Initiative2, and Initiative3

**Answer: B**

**Explanation:**

B. Policy1 and Initiative1 only

### Question: 333

CertyIQ

You have an Azure subscription that contains a Microsoft Defender External Attack Surface Management (Defender EASM) resource named EASM1. EASM1 has discovery enabled and contains several inventory assets.

You need to identify which inventory assets are vulnerable to the most critical web app security risks.

Which Defender EASM dashboard should you use?

- A. Security Posture
- B. OWASP Top 10
- C. Attack Surface Summary
- D. GDPR Compliance

**Answer: B**

**Explanation:**

<https://learn.microsoft.com/en-us/azure/external-attack-surface-management/understanding-dashboards#owasp-top-10-dashboard>

### Question: 334

CertyIQ

You have an Azure subscription that uses Microsoft Defender for Cloud.

You need to use Defender for Cloud to review regulatory compliance with the Azure CIS 1.4.0 standard. The solution must minimize administrative effort.

What should you do first?

- A. Assign an Azure policy.
- B. Disable one of the Out of the box standards.
- C. Manually add the Azure CIS 1.4.0 standard.
- D. Add a custom initiative.

**Answer: A**

**Explanation:**

Assign an Azure policy.

### Question: 335

CertyIQ

You have an Azure subscription that contains an Azure key vault named Vault1 and a virtual machine named VM1.

VM1 is connected to a virtual network named VNet1.

You need to allow access to Vault1 only from VM1.

What should you do in the Networking settings of Vault1?

- A. From the Firewalls and virtual networks tab, add the IP address of VM1.
- B. From the Private endpoint connections tab, create a private endpoint for VM1.
- C. From the Firewalls and virtual networks tab, add VNet1.
- D. From the Firewalls and virtual networks tab, set Allow trusted Microsoft services to bypass this firewall to Yes for Vault1.

**Answer: C**

**Explanation:**

From the Firewalls and virtual networks tab, add VNet1.

### Question: 336

CertyIQ

You have an Azure subscription.

You create a new virtual network named VNet1.

You plan to deploy an Azure web app named App1 that will use VNet1 and will be reachable by using private IP addresses. The solution must support inbound and outbound network traffic.

What should you do?

- A. Create an Azure App Service Hybrid Connection.
- B. Create an Azure application gateway.
- C. Create an App Service Environment.
- D. Configure regional virtual network integration.



**Answer: C**

**Explanation:**

By creating an ASE, you can deploy App1 and configure it to use VNet1, which will allow the app to use private IP addresses and support inbound and outbound network traffic.

**Question: 337**

CertyIQ

You have an Azure subscription and the computers shown in the following table.

Name	Operating system	Description
VM1	Windows Server 2012 R2	Azure virtual machine
VM2	Red Hat Enterprise Linux (RHEL) 8.2	Azure virtual machine
Server1	Windows Server 2019	On-premises physical computer connected to Microsoft Defender for Cloud
VMSS1_0	Windows Server 2022	Azure virtual machine in a virtual machine scale set

You need to perform a vulnerability scan of the computers by using Microsoft Defender for Cloud.

Which computers can you scan?

- A.VM1 only
- B.VM1 and VM2 only
- C.Server1 and VMSS1\_0 only
- D.VM1, VM2, and Server1 only
- E.VM1, VM2, Server 1, and VMSS1\_0

**Answer: D**

**Explanation:**

you have to install the vulnerability scanner on the VMSS1\_0 first.

[https://learn.microsoft.com/en-us/answers/questions/820846/microsoft-defender-cloud-for-virtual-machine-scalereference?WT.mc\\_id=AZ-MVP-5000120](https://learn.microsoft.com/en-us/answers/questions/820846/microsoft-defender-cloud-for-virtual-machine-scalereference?WT.mc_id=AZ-MVP-5000120)

**Question: 338**

CertyIQ

You have an Azure subscription that uses Microsoft Defender for Cloud. The subscription contains the Azure Policy definitions shown in the following table.

Name	Type	Category
Policy1	Policy	Regulatory Compliance
Policy2	Policy	Security Center
Initiative1	Initiative	Regulatory Compliance
Initiative2	Initiative	Security Center

Which definitions can be assigned as a security policy in Defender for Cloud?

- A. Policy1 and Policy2 only
- B. Initiative1 and Initiative2 only
- C. Policy1 and Initiative1 only
- D. Policy2 and Initiative2 only
- E. Policy1, Policy2, Initiative1, and Initiative2

**Answer: B**

**Explanation:**

B. Initiative1 and Initiative2 only

### Question: 339

CertyIQ

HOTSPOT

-

On Monday, you configure an email notification in Microsoft Defender for Cloud to notify [email protected] about alerts that have a severity level of Low, Medium, or High.

On Tuesday, Microsoft Defender for Cloud generates the security alerts shown in the following table.

Time	Description	Severity
01:00	Failed RDP brute force attack	Medium
01:01	Successful RDP brute force attack	High
06:10	Suspicious process executed	High
09:00	Malicious SQL activity	High
11:15	Network communication with a malicious machine detected	Low
13:30	Suspicious process executed	High
14:00	Failed RDP brute force attack	Medium
16:01	Successful RDP brute force attack	High
23:20	Possible outgoing spam activity detected	Low
23:25	Modified system binary discovered in dump file	High
23:30	Malicious SQL activity	High

How many email notifications will [email protected] receive on Tuesday? To answer, select the appropriate options

in the answer area.

NOTE: Each correct selection is worth one point.

### Answer Area

Total number of Microsoft Defender for Cloud email notifications about an RDP brute force attack on Tuesday:

▼

1

2

3

4

Total number of Microsoft Defender for Cloud email notifications on Tuesday:

▼

3

4

7

9

11

Answer:

### Answer Area

Total number of Microsoft Defender for Cloud email notifications about an RDP brute force attack on Tuesday:

▼

1

2

3

4

Total number of Microsoft Defender for Cloud email notifications on Tuesday:

▼

3

4

7

9

11

Explanation:

Box1: 4Box2: 7 Is correct.

### Question: 340

You have an Azure subscription that uses Microsoft Defender for Cloud.

You have accounts for the following cloud services:

- Alibaba Cloud
- Amazon Web Services (AWS)
- Google Cloud Platform (GCP)

What can you add to Defender for Cloud?

- A.AWS only
- B.Alibaba Cloud and AWS only
- C.Alibaba Cloud and GCP only
- D.AWS and GCP only
- E.Alibaba Cloud, AWS, and GCP

**Answer: D**

**Explanation:**

Started to feel lonely on these questions, since there are no comments yet:) Ans D: AWS, GCP

### Question: 341

CertyIQ

You have an Azure subscription.

You plan to map an online infrastructure and perform vulnerability scanning for the following:

- ASNs
- Hostnames
- IP addresses
- SSL certificates

What should you use?

- A.Microsoft Defender for Cloud
- B.Microsoft Defender External Attack Surface Management (Defender EASM)
- C.Microsoft Defender for Identity
- D.Microsoft Defender for Endpoint

**Answer: B**

**Explanation:**

Correct Answer: B. Microsoft Defender External Attack Surface Management (Defender EASM)  
<https://learn.microsoft.com/en-us/azure/external-attack-surface-management/>

### Question: 342

CertyIQ

HOTSPOT

-

You have an Azure subscription that uses Microsoft Defender for Cloud.

You plan to use the Secure Score Over Time workbook.

You need to configure the Continuous export settings for the Defender for Cloud data.

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

NOTE: Each correct selection is worth one point.

Answer Area



Settings | Continuous export ...

Visual Studio Enterprise Subscription



Save



Continuous export

Configure streaming export setting of Defender for Cloud data to multiple export targets. Exporting Defender for Cloud's data also enables you to use experiences such as integration with 3rd-party SIEM and Azure Data Explorer. [Learn More >](#)

Event hub   Log Analytics workspace

Export enabled   On   Off

Exported data types

<input type="checkbox"/> Security recommendations	No selected recommendation
<input checked="" type="checkbox"/> Secure score ⓘ	Overall score,Control score
Controls	All controls selected
<input type="checkbox"/> Security alerts	No selected severities
<input type="checkbox"/> Regulatory compliance	No selected standards

Export frequency

<input checked="" type="checkbox"/> Streaming updates ⓘ
<input type="checkbox"/> Snapshots (Preview) ⓘ

Answer:



## Settings | Continuous export ...

Visual Studio Enterprise Subscription

Save



## Continuous export

Configure streaming export setting of Defender for Cloud data to multiple export targets.

Exporting Defender for Cloud's data also enables you to use experiences such as integration with 3rd-party SIEM and Azure Data Explorer.

[Learn More >](#)Event hub Log Analytics workspace

Export enabled

On

Off

## Exported data types

☐ Security recommendations No selected recommendation ☒ Secure score ⓘ Overall score,Control score

Controls

All controls selected ☐ Security alerts No selected severities ☐ Regulatory compliance No selected standards

## Export frequency

☒ Streaming updates ⓘ☐ Snapshots (Preview) ⓘ

## Question: 343

CertyIQ

You are troubleshooting a security issue for an Azure Storage account.

You enable Azure Storage Analytics logs and archive it to a storage account.

What should you use to retrieve the diagnostics logs?

- A.Azure Cosmos DB explorer
- B.SQL query editor in Azure
- C.AzCopy
- D.File Explorer in Windows

**Answer: C****Explanation:**

This question appeared many times, the answer is C. AzCopy



**Question: 344****CertyIQ**

You have an Azure subscription that uses Microsoft Defender for Cloud.

You have an Amazon Web Services (AWS) account.

You need to ensure that when you deploy a new AWS Elastic Compute Cloud (EC2) instance, the Microsoft Defender for Servers agent installs automatically.

What should you configure first?

- A.the classic cloud connector
- B.the Azure Monitor agent
- C.the Log Analytics agent
- D.the native cloud connector

**Answer: D****Explanation:**

D. To protect your AWS-based resources, you can connect an AWS account with either Native or Classic Cloud Connector. Native cloud connector is the recommended way and provides an agentless connection to your AWS account that can extend with Defender for Cloud's Defender plans to secure the AWS resources.<https://learn.microsoft.com/en-us/azure/defender-for-cloud/quickstart-onboard-aws?pivot=env-settings>

**Question: 345****CertyIQ**

HOTSPOT

-

You have an Azure subscription that contains a Microsoft Defender External Attack Surface Management (Defender EASM) resource named EASM1. EASM1 contains the inventory assets shown in the following table.

Name	Type	State
VM1	Host	Approved Inventory
VM2	Host	Dependency
VM3	Host	Monitor Only
VM4	Host	Candidate

Which assets are scanned daily, and which assets will display in the default dashboard charts? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

## Answer Area

Scanned daily:

▼

- VM1 only
- VM1 and VM2 only
- VM1, VM2, and VM3 only
- VM1, VM2, VM3, and VM4

Display in the default dashboard charts:

▼

- VM1 only
- VM1 and VM2 only
- VM1, VM2, and VM3 only
- VM1, VM2, VM3, and VM4

Answer:

### Answer Area

Scanned daily:

▼

- VM1 only
- VM1 and VM2 only
- VM1, VM2, and VM3 only
- VM1, VM2, VM3, and VM4

Display in the default dashboard charts:

▼

- VM1 only
- VM1 and VM2 only
- VM1, VM2, and VM3 only
- VM1, VM2, VM3, and VM4

Explanation:

Both should be VM1 only.

<https://learn.microsoft.com/en-us/azure/external-attack-surface-management/understanding-inventory-assets>

You have an Azure subscription that uses Microsoft Defender for Cloud.

You have an Amazon Web Services (AWS) account named AWS1 that is connected to Defender for Cloud.

You need to ensure that AWS1 uses AWS Foundational Security Best Practices. The solution must minimize administrative effort.

What should you do in Defender for Cloud?

- A. Assign a built-in compliance standard.
- B. Create a new custom standard.
- C. Assign a built-in assessment.
- D. Create a new custom assessment.

**Answer: A**

**Explanation:**

A. The regulatory compliance dashboard shows your compliance with built-in standards specific to AWS, including AWS CIS, AWS PCI DSS, and AWS Foundational Security Best Practices. <https://learn.microsoft.com/en-us/azure/defender-for-cloud/quickstart-onboard-aws?pivots=env-settings>

### Question: 347

CertyIQ

HOTSPOT

-

You plan to deploy a custom policy initiative for Microsoft Defender for Cloud.

You need to identify all the resource groups that have a Delete lock.

How should you complete the policy definition? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

## Answer Area

...

```
"policyRule": {
  "if": {
    "field": "type",
    "equals": 
  },
  "then": {
    "effect": "auditIfNotExists",
    "details": {
      "type": "Microsoft.Authorization/locks",
       : {
        "existenceCondition": "value",
        "operations": "value",
        "field": "Microsoft.Authorization/locks/level",
        "equals": "CanNotDelete"
      }
    }
  }
}
```

...

Answer:

## Answer Area

...

```
"policyRule": {  
  "if": {  
    "field": "type",  
    "equals": "Microsoft.Resources/subscriptions",  
  },  
  "then": {  
    "effect": "auditIfNotExists",  
    "details": {  
      "type": "Microsoft.Authorization/locks",  
      "existenceCondition": {  
        "field": "Microsoft.Authorization/locks/level",  
        "equals": "CanNotDelete"  
      }  
    }  
  }  
}
```

### Explanation:

<https://learn.microsoft.com/en-us/azure/defender-for-cloud/custom-security-policies?pivots=azure-portal>

## Question: 348

CertyIQ

You are troubleshooting a security issue for an Azure Storage account.

You enable Azure Storage Analytics logs and archive it to a storage account.

What should you use to retrieve the diagnostics logs?

- A.the Microsoft 365 Defender portal
- B.SQL query editor in Azure
- C.Azure Monitor
- D.Azure Storage Explorer

**Answer: D**

**Explanation:**

D. Azure Storage Explorer

**Question: 349****CertyIQ**

You have an Azure subscription that contains a Microsoft Defender External Attack Surface Management (Defender EASM) resource named EASM1.

You review the Attack Surface Summary dashboard.

You need to identify the following insights:

- Deprecated technologies that are no longer supported
- Infrastructure that will soon expire

Which section of the dashboard should you review?

- A.Securing the Cloud
- B.Sensitive Services
- C.Attack Surface Priorities
- D.attack surface composition

**Answer: C****Explanation:**

Correct C. Attack Surface Priorities.

<https://learn.microsoft.com/en-us/azure/external-attack-surface-management/understanding-dashboards>

**Question: 350****CertyIQ**

You have an Azure subscription.

You plan to deploy Microsoft Defender External Attack Surface Management (Defender EASM) to identify and monitor externally facing assets.

You create a new Defender EASM instance named EASM1.

What should you do next?

- A.Create a custom attack surface.
- B.Add a Log Analytics workspace.
- C.Add a discovery group.
- D.Import seeds from an organization.

**Answer: D****Explanation:**

Import seeds from an organization.

Reference:



### Question: 351

CertyIQ

You have an Azure subscription that contains an Azure Key Vault Standard key vault named Vault1. Vault1 hosts a 2048-bit RSA key named key1.

You need to ensure that key1 is rotated every 90 days.

What should you do first?

- A. Create a key rotation policy.
- B. Modify the Access policies settings of Vault1.
- C. Upgrade Vault1 to Key Vault Premium.
- D. Recreate key1 as an EC key.

**Answer: A**

**Explanation:**

Create a key rotation policy.

Reference:

<https://learn.microsoft.com/en-us/azure/key-vault/managed-hsm/key-rotation>

### Question: 352

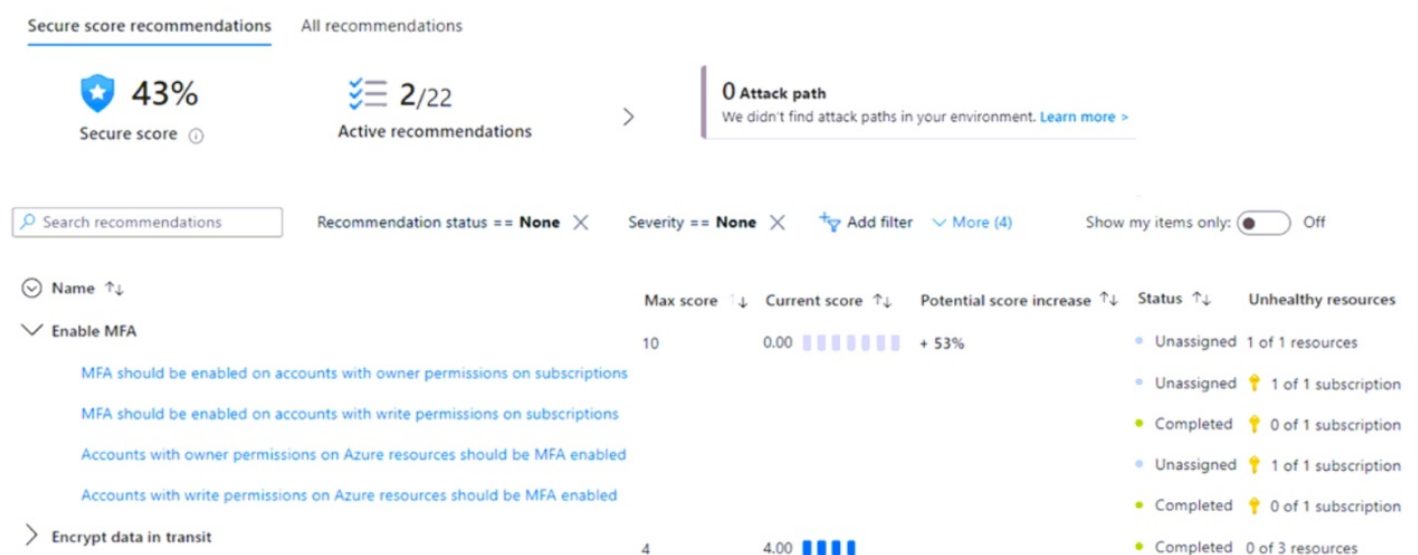
CertyIQ

You have an Azure subscription named Sub1 that has Security defaults disabled. The subscription contains the following users:

- Five users that have owner permissions for Sub1.
- Ten users that have owner permissions for Azure resources.

None of the users have multi-factor authentication (MFA) enabled.

Sub1 has the secure score as shown in the Secure Score exhibit. (Click the Secure Score tab.)



You plan to enable MFA for the following users:

- Five users that have owner permission for Sub1.
- Five users that have owner permissions for Azure resources.

By how many points will the secure score increase after you perform the planned changes?

- A.0
- B.5
- C.7.5
- D.10
- E.14

Answer: C

Explanation:

Current score = [Score per resource] \* [Number of healthy resources]  
 Five users that have owner permissions for Sub1 = 5 x 5/5  
 Five users that have owner permissions for Azure resources = 5 x 5/10  
 Total score = 5 + 2.5 = 7.5

<https://learn.microsoft.com/en-us/azure/defender-for-cloud/secure-score-security-controls>

### Question: 353



DRAG DROP

You have two Azure subscriptions named Sub1 and Sub2. Sub1 contains a resource group named RG1 and an Azure policy named Policy1.

You need to remediate the non-compliant resources in Sub1 based on Policy1.

How should you complete the PowerShell script? To answer, drag the appropriate values to the correct targets. Each value may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

#### Values

#### Answer Area

Get-AzPolicyRemediation	\$policyAssignmentI = "/subscriptions/f0710c27-9663-4c05-19f8-1b4be01e86a5/providers/Microsoft.Authorization/policyAssignments/2deae24764b447c29af7c309"
Set-AzContext	
Set-AzResourceGroup	<input type="text"/> -Subscription "Sub1"
Start-AzPolicyComplianceScan	<input type="text"/> -PolicyAssignmentId \$policyAssignmentId
Start-AzPolicyRemediation	-Name "policy1" -ResourceDiscoveryMode ReEvaluateCompliance

Answer:

## Answer Area

```
$policyAssignmentId = "/subscriptions/f0710c27-9663-4c05-19f8-1b4be01e86a5/providers/Microsoft.Authorization/policyAssignments/2deae24764b447c29af7c309"
```

```
Set-AzContext -Subscription "Sub1"
```

```
Start-AzPolicyRemediation -PolicyAssignmentId $policyAssignmentId  
-Name "policy1" -ResourceDiscoveryMode  
ReEvaluateCompliance
```

### Explanation:

Set-Az Context.

Start-Az Policy Remediation.

## Question: 354

CertyIQ

You have an Azure subscription that uses Microsoft Defender for Cloud.

You need to add a custom security recommendation to Defender for Cloud. The recommendation must be assigned the custom severity rating of the subscription.

What should you create?

- A.an exemption
- B.an initiative definition
- C.a policy definition
- D.an assignment

### Answer: C

### Explanation:

Correct answer is C:a policy definition.

## Question: 355

CertyIQ

HOTSPOT

-

You have an Azure key vault.

You need to delegate administrative access to the key vault to meet the following requirements:

- Provide a user named User1 with the ability to set access policies for the key vault.
- Provide a user named User2 with the ability to add and delete certificates in the key vault.
- Use the principle of least privilege.

What should you use to assign access to each user? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

## Answer Area

User1:

- RBAC only
- Key vault access policy only
- RBAC and key vault access policy

User2:

- RBAC only
- Key vault access policy only
- RBAC and key vault access policy

Answer:

### Answer Area

User1:

- RBAC only**
- Key vault access policy only
- RBAC and key vault access policy

User2:

- RBAC only
- Key vault access policy only
- RBAC and key vault access policy**

Explanation:

RBAC Only.

RBAC and Key Vault access policy.

Question: 356

CertyIQ

HOTSPOT

-

You have an Azure subscription named Sub1 that contains two resource groups named RGnet and NET.

You have the Azure Policy definition shown in the following exhibit.

```

1  {
2      "properties": {
3          "mode": "all",
4          "parameters": {
5          },
6          "policyRule": {
7              "if": {
8                  "allOf": [{
9                      "value": "[resourceGroup().name]",
10                     "contains": "net"
11                 },
12                 {
13                     "field": "type",
14                     "notLike": "Microsoft.Network/*"
15                 }
16             ]
17         },
18         "then": {
19             "effect": "deny"
20         }
21     }
22 }
23 }

```

You assign the policy definition to Sub1 and NET.

You plan to deploy the resources shown in the following table.

Name	Type
VNet1	Virtual network
ASG1	Application security group
storage1	Storage account

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

NOTE: Each correct selection is worth one point.

## Answer Area

Statements	Yes	No
You can deploy VNet1 to RGnet.	<input type="radio"/>	<input type="radio"/>
You can deploy ASG1 to NET.	<input type="radio"/>	<input type="radio"/>
You can deploy storage1 to RGnet.	<input type="radio"/>	<input type="radio"/>

Answer:

### Answer Area

Statements	Yes	No
You can deploy VNet1 to RGnet.	<input checked="" type="radio"/>	<input type="radio"/>
You can deploy ASG1 to NET.	<input checked="" type="radio"/>	<input type="radio"/>
You can deploy storage1 to RGnet.	<input type="radio"/>	<input checked="" type="radio"/>

Explanation:

Yes

Yes

No

### Question: 357

CertyIQ

Your company has an Azure subscription named Sub1.

You plan to create several security alerts by using Azure Monitor.

You need to prepare Sub1 for the alerts.

What should you create first?

- A.an Azure Automation account
- B.an Azure event hub
- C.an Azure Log Analytics workspace
- D.an Azure Storage account



**Answer: C**

**Explanation:**

an Azure Log Analytics workspace.

**Question: 358**

**CertyIQ**

You have an Azure subscription that contains the Azure App Service web apps shown in the following table.

Name	Resource group	Location	App Service plan	Operation system
App1	RG1	East US	ASP1	Windows
App2	RG1	East US	ASP2	Linux
App3	RG2	East US	ASP3	Windows
App4	RG1	Central US	ASP4	Windows

You upload a private key certificate named Cert1.pfx to App1.

Which apps can use Cert1?

- A.App1 only
- B.App1 and App2 only
- C.App1 and App4 only
- D.App1, App2, and App3 only
- E.App1, App2, App3, and App4

**Answer: A**

**Explanation:**

Correct answer is A:App1 only.

**Question: 359**

**CertyIQ**

You have an Azure subscription that uses Microsoft Defender for Cloud.

You have an Amazon Web Services (AWS) account.

You need to add the AWS account to Defender for Cloud.

What should you do first?

- A.From Defender for Cloud, configure the Environment settings.
- B.From the AWS account, enable a security hub.
- C.From Defender for Cloud, configure the Security solutions settings.
- D.From the Azure portal, add the AWS enterprise application.

**Answer: A**

**Explanation:**

### Question: 360

CertyIQ

You have an Azure subscription that contains an Azure key vault.

You create a storage account named storage1.

You plan to store data in the following storage1 services:

- Azure Files
- Azure Blob storage
- Azure Table storage
- Azure Queue storage

For which two services can you configure data encryption by using the keys stored in the key vault? Each correct answer presents a complete solution,

NOTE: Each correct selection is worth one point.

- A.Blob storage
- B.Table storage
- C.Queue storage
- D.Azure Files

**Answer: AD**

**Explanation:**

- A.Blob storage.
- D.Azure Files.

### Question: 361

CertyIQ

You have an Azure subscription that contains an Azure SQL database named SQL1 and an Azure key vault named KeyVault1. KeyVault1 stores the keys shown in the following table.

Name	Type	RSA key size	Elliptic curve name
Key1	RSA	2048	Not applicable
Key2	RSA	3072	Not applicable
Key3	RSA	4096	Not applicable
Key4	EC	Not applicable	P-512

You need to configure Transparent Data Encryption (TDE). TDE will use a customer-managed key for SQL1. Which keys can you use?

- A.Key2 only
- B.Key1 only
- C.Key2 and Key3 only
- D.Key1, Key2, Key3, and Key4

E.Key1 and Key2 only

**Answer: E**

**Explanation:**

The key must be an asymmetric, RSA or RSA HSM key. The supported key lengths are 2048-bit and 3072-bit.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-sql/database/transparent-data-encryption-byok-overview>

### Question: 362

CertyIQ

SIMULATION -

You plan to use Azure Disk Encryption for several virtual machine disks.

You need to ensure that Azure Disk Encryption can retrieve secrets from the KeyVault12345678 Azure key vault. To complete this task, sign in to the Azure portal and modify the Azure resources.

**Answer:**

See the explanation below.

**Explanation:**

1. In the Azure portal, type Key Vaults in the search box, select Key Vaults from the search results then select KeyVault12345678. Alternatively, browse to Key Vaults in the left navigation pane.
2. In the Key Vault properties, scroll down to the Settings section and select Access Policies.
3. Select the Azure Disk Encryption for volume encryption

Enable Access to:

- ☐ Azure Virtual Machines for deployment ⓘ
- ☐ Azure Resource Manager for template deployment ⓘ
- ☒ Azure Disk Encryption for volume encryption ⓘ

4. Click Save to save the changes.

### Question: 363

CertyIQ

HOTSPOT -

You have an Azure subscription that contains a web app named App1 and an Azure key vault named Vault1.

You need to configure App1 to store and access the secrets in Vault1.

How should you configure App1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

## Answer Area

Configure App1 to authenticate by using a:

Key
Certificate
Passphrase
Managed identity

Configure Key Vault reference for App1 from the:

Extensions blade
General settings tab
TLS/SSL setting blade
Application settings tab

Answer:

## Answer Area

Configure App1 to authenticate by using a:

Key
Certificate
Passphrase
Managed identity

Configure Key Vault reference for App1 from the:

Extensions blade
General settings tab
TLS/SSL setting blade
Application settings tab

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/app-service/overview-managed-identity?tabs=dotnet>

### Question: 364

CertyIQ

HOTSPOT -

You have an Azure key vault named KeyVault1 that contains the items shown in the following table.

Name	Type
Item1	Key
Item2	Secret
Policy1	Access policy

In KeyVault1, the following events occur in sequence:

- ⇒ Item1 is deleted.
- ⇒ Item2 and Policy1 are deleted.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
You can recover Policy1.	<input type="radio"/>	<input type="radio"/>
You can add a new key named Item1.	<input type="radio"/>	<input type="radio"/>
You can recover Item2.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
You can recover Policy1.	<input type="radio"/>	<input checked="" type="radio"/>
You can add a new key named Item1.	<input type="radio"/>	<input checked="" type="radio"/>
You can recover Item2.	<input checked="" type="radio"/>	<input type="radio"/>

Explanation:

Box1: No -

Policies cannot be recovered.

Box2: Soft delete is enabled by default on all key vaults. You cannot add a new key named Item1 because an object named Item1 exists in a soft-deleted state.

Box3: Soft delete is now enabled by default on all key vaults so you can recover Item2.

Reference:

<https://docs.microsoft.com/en-us/azure/key-vault/general/soft-delete-overview> <https://docs.microsoft.com/en-us/azure/key-vault/general/soft-delete-change>

### Question: 365

CertyIQ

You have an Azure SQL Database server named SQL1.

For SQL1, you turn on Azure Defender for SQL to detect all threat detection types.

Which action will Azure Defender for SQL detect as a threat?

- A. A user updates more than 50 percent of the records in a table.
- B. A user attempts to sign in as SELECT \* FROM table1.
- C. A user is added to the db\_owner database role.
- D. A user deletes more than 100 records from the same table.

**Answer: B**

**Explanation:**

Advanced Threat Protection can detect potential SQL injections: This alert is triggered when an active exploit happens against an identified application vulnerability to SQL injection. This means the attacker is trying to inject malicious SQL statements using the vulnerable application code or stored procedures.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-sql/database/azure-defender-for-sql>

### Question: 366

CertyIQ

HOTSPOT -

You have the Azure Information Protection labels as shown in the following table.

Name	Use condition	Label is applied	Pattern	Case sensitivity
Label1	Condition1	Automatically	White	On
Label2	Condition2	Automatically	Black	Off

You have the Azure Information Protection policies as shown in the following table.

Name	Applies to	Use label	Set the default label
Global	<i>Not applicable</i>	<i>None</i>	None
Policy1	User1	Label1	None
Policy2	User1	Label2	None

You need to identify how Azure Information Protection will label files.

What should you identify? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



## Answer Area

If User1 creates a Microsoft Word file that includes the text "Black and White", the file will be assigned:

	▼
No label	
Label1 only	
Label2 only	
Label1 and Label2	

If User1 creates a Microsoft Notepad file that includes the text "Black or white", the file will be assigned:

	▼
No label	
Label1 only	
Label2 only	
Label1 and Label2	

Answer:

### Answer Area

If User1 creates a Microsoft Word file that includes the text "Black and White", the file will be assigned:

	▼
No label	
Label1 only	
Label2 only	
Label1 and Label2	

If User1 creates a Microsoft Notepad file that includes the text "Black or white", the file will be assigned:

	▼
No label	
Label1 only	
Label2 only	
Label1 and Label2	

#### Explanation:

Box 1: Label 2 only -

How multiple conditions are evaluated when they apply to more than one label

1. The labels are ordered for evaluation, according to their position that you specify in the policy: The label positioned first has the lowest position (least sensitive) and the label positioned last has the highest position (most sensitive).
2. The most sensitive label is applied.
3. The last sublabel is applied.

Box 2: No Label -

Automatic classification applies to Word, Excel, and PowerPoint when documents are saved, and apply to Outlook when emails are sent. Automatic classification does not apply to Microsoft Notepad.

Reference:

<https://docs.microsoft.com/en-us/azure/information-protection/configure-policy-classification>

**Question: 367****CertyIQ**

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.

Reference:

<https://docs.microsoft.com/en-us/azure/devops/repos/git/branch-policies?view=azure-devops&viewFallbackFrom=vsts>

**Question: 368****CertyIQ**

SIMULATION -

You need to ensure that User2-1234578 has all the key permissions for KeyVault1234578.

To complete this task, sign in to the Azure portal and modify the Azure resources.

**Answer:**

See the explanation below.

**Explanation:**

You need to assign the user the Key Vault Secrets Officer role.

1. In the Azure portal, type Key Vaults in the search box, select Key Vaults from the search results then select KeyVault1234578. Alternatively, browse to Key Vaults in the left navigation pane.
2. In the key vault properties, select Access control (IAM).
3. In the Add a role assignment section, click the Add button.
4. In the Role box, select the Key Vault Secrets Officer role from the drop-down list.
5. In the Select box, start typing User2-1234578 and select User2-1234578 from the search results.
6. Click the Save button to save the changes.

**Question: 369****CertyIQ**

You have an Azure web app named WebApp1.

You upload a certificate to WebApp1.

You need to make the certificate accessible to the app code of WebApp1.

What should you do?

- A. Add a user-assigned managed identity to WebApp1.
- B. Add an app setting to the WebApp1 configuration.

- C. Enable system-assigned managed identity for WebApp1.
- D. Configure the TLS/SSL binding for WebApp1.

**Answer: B**

**Explanation:**

To access a certificate in your app code, add its thumbprint to the WEBSITE\_LOAD\_CERTIFICATES app setting, by running the following command in the Cloud Shell:

Azure CLI

Copy

Try It

```
az webapp config appsettings set --name <app-name> --resource-group <resource-group-name> --settings WEBSITE_LOAD_CERTIFICATES=<comma-separated-certificate-thumbprints>
```

Reference:

<https://docs.microsoft.com/en-us/azure/app-service/configure-ssl-certificate-in-code>

**Question: 370**



HOTSPOT -  
You have the Azure key vaults shown in the following table.

Name	Location	Azure subscription name
KV1	West US	Subscription1
KV2	West US	Subscription1
KV3	East US	Subscription1
KV4	West US	Subscription2
KV5	East US	Subscription2

KV1 stores a secret named Secret1 and a key for a managed storage account named Key1.  
You back up Secret1 and Key1.  
To which key vaults can you restore each backup? To answer, select the appropriate options in the answer area.  
NOTE: Each correct selection is worth one point.  
Hot Area:

## Answer Area

You can restore the Secret1 backup to:

	▼
KV1 only	
KV1 and KV2 only	
KV1, KV2 and KV3 only	
KV1, KV2 and KV4 only	
KV1, KV2, KV3, KV4, and KV5	

You can restore the Key1 backup to:

	▼
KV1 only	
KV1 and KV2 only	
KV1, KV2 and KV3 only	
KV1, KV2 and KV4 only	
KV1, KV2, KV3, KV4, and KV5	

Answer:

## Answer Area

You can restore the Secret1 backup to:

	▼
KV1 only	
KV1 and KV2 only	
KV1, KV2 and KV3 only	
KV1, KV2 and KV4 only	
KV1, KV2, KV3, KV4, and KV5	

You can restore the Key1 backup to:

	▼
KV1 only	
KV1 and KV2 only	
KV1, KV2 and KV3 only	
KV1, KV2 and KV4 only	
KV1, KV2, KV3, KV4, and KV5	

**Explanation:**

The backups can only be restored to key vaults in the same subscription and same geography. You can restore to a different region in the same geography.

### Question: 371

CertyIQ

HOTSPOT -

You have an Azure subscription that contains an Azure key vault named Vault1.

On January 1, 2019, Vault1 stores the following secrets. All dates are in mm/dd/yy format.

Enabled : False  
Expires :  
NotBefore : 5/1/19 12:00:00 AM  
Created : 12/20/18 2:55:00 PM  
Updated : 12/20/18 2:55:00 PM  
ContentType :  
Tags :  
TagsTable :  
VaultName : vault1  
Name : Password1  
Version :  
Id : https://vault1.vault.azure.net:443/secrets/Password1

Enabled : True  
Expires : 5/1/19 12:00:00 AM  
NotBefore : 3/1/19 12:00:00 AM  
Created : 12/20/18 3:00:00 PM  
Updated : 12/20/18 3:00:00 PM  
ContentType :  
Tags :  
TagsTable :  
VaultName : vault1  
Name : Password2  
Version :  
Id : https://vault1.vault.azure.net:443/secrets/Password2

When can each secret be used by an application? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

### Answer Area

Password1:

	▼
Never	
Always	
Only after May 1, 2019	

Password2:

	▼
Never	
Always	
Only between March 1, 2019 and May 1, 2019	

Answer:

## Answer Area

Password1:

▼

Never

Always

Only after May 1, 2019

Password2:

▼

Never

Always

Only between March 1, 2019 and May 1, 2019

### Explanation:

Box 1: Never -

Password1 is disabled.

Box 2: Only between March 1, 2019 and May 1,

Password2:

```
Expires      : 5/1/19 12:00:00 AM
NotBefore    : 3/1/19 12:00:00 AM
```

Reference:

<https://docs.microsoft.com/en-us/powershell/module/azurerm.keyvault/set-azurekeyvaultsecretattribute>

## Question: 372

CertyIQ

You have an Azure web app named webapp1.

You need to configure continuous deployment for webapp1 by using an Azure Repo.

What should you create first?

- A. an Azure Application Insights service
- B. an Azure DevOps organization
- C. an Azure Storage account
- D. an Azure DevTest Labs lab

**Answer: B**

### Explanation:

To use Azure Repos, make sure your Azure DevOps organization is linked to your Azure subscription.

Reference:

<https://docs.microsoft.com/en-us/azure/app-service/deploy-continuous-deployment>

## Question: 373

CertyIQ

Your company has an Azure subscription named Sub1 that is associated to an Azure Active Directory (Azure AD) tenant named contoso.com.

The company develops an application named App1. App1 is registered in Azure AD.

You need to ensure that App1 can access secrets in Azure Key Vault on behalf of the application users.

What should you configure?



- A. an application permission without admin consent
- B. a delegated permission without admin consent
- C. a delegated permission that requires admin consent
- D. an application permission that requires admin consent

**Answer: B**

**Explanation:**

Delegated permissions - Your client application needs to access the web API as the signed-in user, but with access limited by the selected permission. This type of permission can be granted by a user unless the permission requires administrator consent.

Incorrect Answers:

A, D: Application permissions - Your client application needs to access the web API directly as itself (no user context). This type of permission requires administrator consent and is also not available for public (desktop and mobile) client applications.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-configure-app-access-web-apis>

**Question: 374**

**CertyIQ**

DRAG DROP -

Your company has an Azure Active Directory (Azure AD) tenant named contoso.com.

The company is developing an application named App1. App1 will run as a service on server that runs Windows Server 2016. App1 will authenticate to contoso.com and access Microsoft Graph to read directory data.

You need to delegate the minimum required permissions to App1.

Which three actions should you perform in sequence from the Azure portal? 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**

**Answer Area**

Grant permissions

Add a delegated permission.

Configure Azure AD Application Proxy.

Add an application permission.

Create an app registration.



**Answer:**

## Actions

Grant permissions

Add a delegated permission.

Configure Azure AD Application Proxy.

Add an application permission.

Create an app registration.

## Answer Area

Create an app registration.

Add an application permission.

Grant permissions



### Explanation:

Step 1: Create an app registration

First the application must be created/registered.

Step 2: Add an application permission

Application permissions are used by apps that run without a signed-in user present.

Step 3: Grant permissions -

Incorrect Answers:

Delegated permission -

Delegated permissions are used by apps that have a signed-in user present.

Application Proxy:

Azure Active Directory's Application Proxy provides secure remote access to on-premises web applications.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/develop/v2-permissions-and-consent>

### Question: 375

CertyIQ

Your company has an Azure subscription named Sub1 that is associated to an Azure Active Directory (Azure AD) tenant named contoso.com.

The company develops a mobile application named App1. App1 uses the OAuth 2 implicit grant type to acquire Azure AD access tokens.

You need to register App1 in Azure AD.

What information should you obtain from the developer to register the application?

- A. a redirect URI
- B. a reply URL
- C. a key
- D. an application ID

**Answer: A**

### Explanation:

For Native Applications you need to provide a Redirect URI, which Azure AD will use to return token responses.

Reference:

**Question: 376****CertyIQ**

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.

Reference:

<https://docs.microsoft.com/bs-latn-ba/azure/governance/policy/how-to/remediate-resources>**Question: 377****CertyIQ**

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.	

Answer:

## 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.	

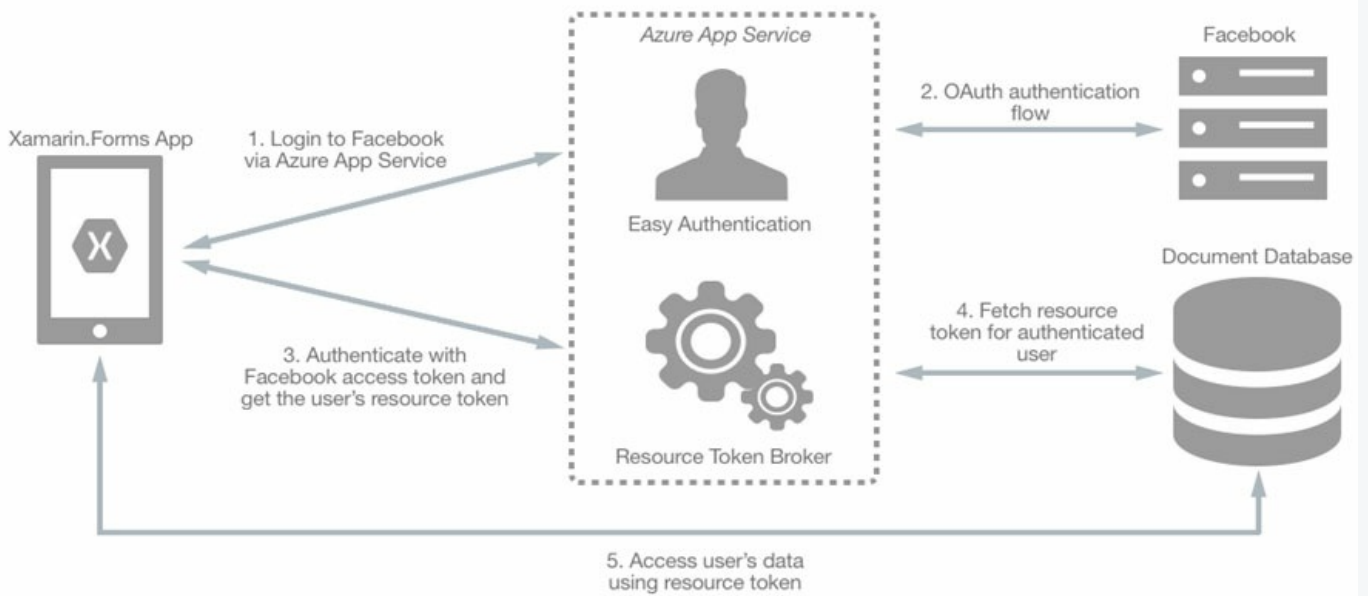
### Explanation:

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:



Reference:

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

### Question: 378

CertyIQ

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-AzKeyVault -VaultName 'KeyVault1' -ResourceGroupName 'RG1'
```

-Location 'East US'

	▼
-EnabledForDeployment	
-EnablePurgeProtection	
-Tag	

	▼
-Confirm	
-DefaultProfile	
-EnableSoftDelete	
-SKU	

Answer:

### Answer Area

```
New-AzKeyVault -VaultName 'KeyVault1' -ResourceGroupName 'RG1'
```

-Location 'East US'

	▼
-EnabledForDeployment	
-EnablePurgeProtection	
-Tag	

	▼
-Confirm	
-DefaultProfile	
-EnableSoftDelete	
-SKU	

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.

Reference:

<https://docs.microsoft.com/en-us/powershell/module/azurerm.keyvault/new-azurermkeyvault>

### Question: 379

CertyIQ

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: C**

**Explanation:**

Azure role is needed for the Management plane through RBAC (Key Vault). Access to the Data plane (secrets reside in Data plane) is through access policy.

### Question: 380

CertyIQ

You have an Azure SQL database.

You implement Always Encrypted.

You need to ensure that application developers can retrieve and decrypt data in the database.

Which two pieces of information should you provide to the developers? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. a stored access policy
- B. a shared access signature (SAS)
- C. the column encryption key
- D. user credentials
- E. the column master key

**Answer: CE**

**Explanation:**

Always Encrypted uses two types of keys: column encryption keys and column master keys. A column encryption key is used to encrypt data in an encrypted column. A column master key is a key-protecting key that encrypts one or more column encryption keys.



Reference:

<https://docs.microsoft.com/en-us/sql/relational-databases/security/encryption/always-encrypted-database-engine>

### Question: 381

CertyIQ

You have a hybrid configuration of Azure Active Directory (Azure AD). All users have computers that run Windows 10 and are hybrid Azure AD joined. You have an Azure SQL database that is configured to support Azure AD authentication. Database developers must connect to the SQL database by using Microsoft SQL Server Management Studio (SSMS) and authenticate by using their on-premises Active Directory account. You need to tell the developers which authentication method to use to connect to the SQL database from SSMS. The solution must minimize authentication prompts. Which authentication method should you instruct the developers to use?

- A. SQL Login
- B. Active Directory " Universal with MFA support
- C. Active Directory " Integrated
- D. Active Directory " Password

**Answer: C**

#### Explanation:

Azure AD can be the initial Azure AD managed domain. Azure AD can also be an on-premises Active Directory Domain Services that is federated with the Azure AD.

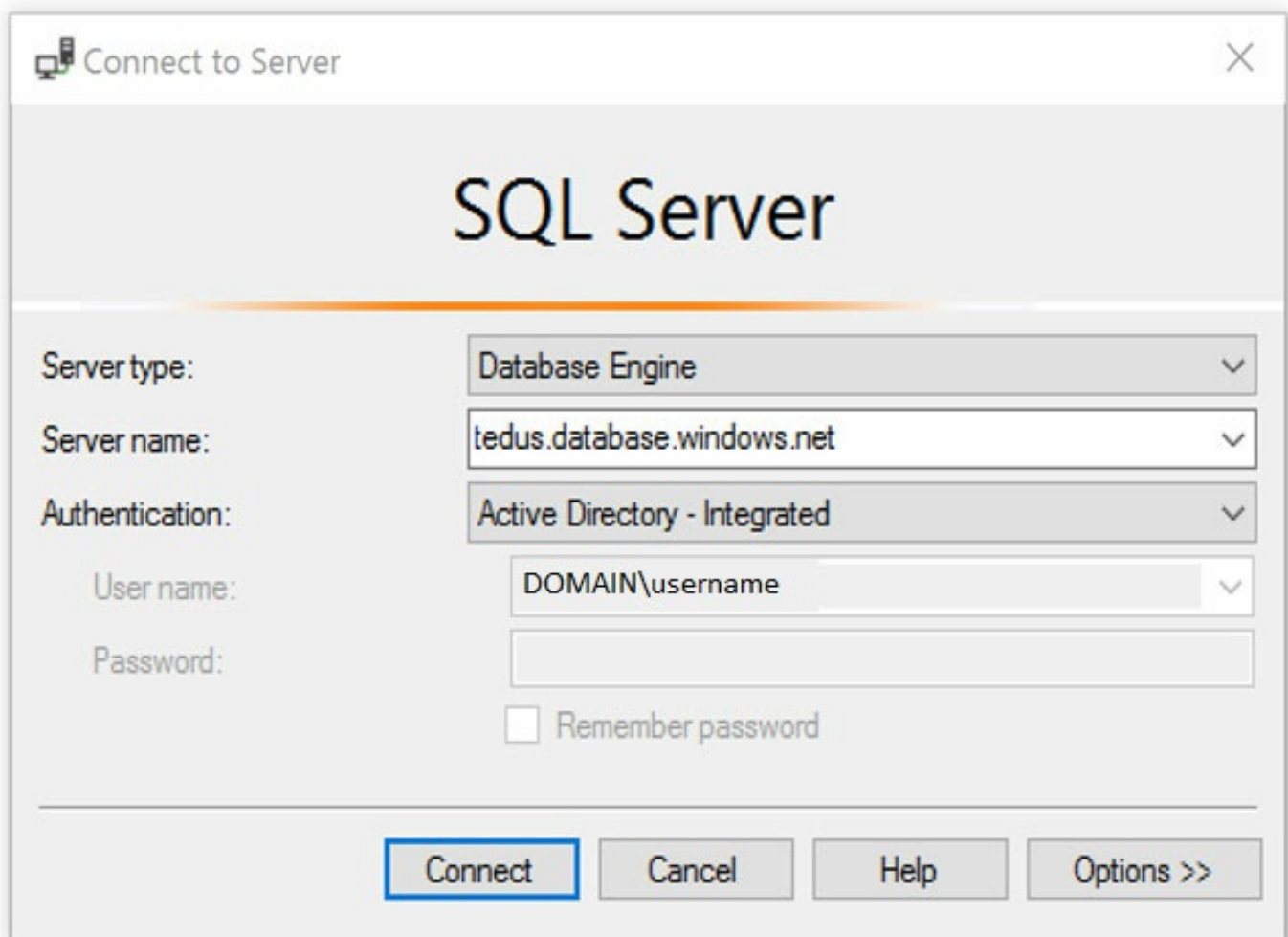
Using an Azure AD identity to connect using SSMS or SSDT

The following procedures show you how to connect to a SQL database with an Azure AD identity using SQL Server Management Studio or SQL Server Database Tools.

Active Directory integrated authentication

Use this method if you are logged in to Windows using your Azure Active Directory credentials from a federated domain.

1. Start Management Studio or Data Tools and in the Connect to Server (or Connect to Database Engine) dialog box, in the Authentication box, select Active Directory - Integrated. No password is needed or can be entered because your existing credentials will be presented for the connection.



2. Select the Options button, and on the Connection Properties page, in the Connect to database box, type the name of the user database you want to connect to.

(The AD domain name or tenant ID option is only supported for Universal with MFA connection options, otherwise it is greyed out.)

Reference:

<https://docs.microsoft.com/en-us/azure/azure-sql/database/authentication-aad-configure?tabs=azure-power-shell>

### Question: 382

CertyIQ

DRAG DROP -

You have an Azure subscription named Sub1 that contains an Azure Storage account named contosostorage1 and an Azure key vault named Contosokeyvault1.

You plan to create an Azure Automation runbook that will rotate the keys of contosostorage1 and store them in Contosokeyvault1.

You need to implement prerequisites to ensure that you can implement the runbook.

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

Run Set-AzKeyVaultAccessPolicy.

Create an Azure Automation account.

Import PowerShell modules to the Azure Automation account.

Create a user-assigned managed identity.

Create a connection resource in the Azure Automation account.

## Answer Area



Answer:

### Actions

Run Set-AzKeyVaultAccessPolicy.

Create an Azure Automation account.

Import PowerShell modules to the Azure Automation account.

Create a user-assigned managed identity.

Create a connection resource in the Azure Automation account.

### Answer Area

Create an Azure Automation account.

Import PowerShell modules to the Azure Automation account.

Run Set-AzKeyVaultAccessPolicy.



### Explanation:

Step 1: Create an Azure Automation account

Runbooks live within the Azure Automation account and can execute PowerShell scripts.

Step 2: Import PowerShell modules to the Azure Automation account

Under 'Assets' from the Azure Automation account Resources section select 'to add in Modules to the runbook. To execute key vault cmdlets in the runbook, we need to add AzureRM.profile and AzureRM.key vault.

Step 3: Run Set-AzKeyVaultAccessPolicy (Gives the Azure Run As account access to the Key Vault)

## Question: 383

### HOTSPOT -

You have an Azure Storage account that contains a blob container named container1 and a client application named App1.

You need to enable App1 access to container1 by using Azure Active Directory (Azure AD) authentication.

What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

## Answer Area

From Azure AD:

	▼
Register App1.	
Create an access package.	
Implement an application proxy.	
Modify the authentication methods.	

From the storage account:

	▼
Add a private endpoint.	
Regenerate the access key.	
Configure Access control (IAM).	
Generate a shared access signature (SAS).	

Answer:

## Answer Area

From Azure AD:

	▼
Register App1.	
Create an access package.	
Implement an application proxy.	
Modify the authentication methods.	

From the storage account:

	▼
Add a private endpoint.	
Regenerate the access key.	
Configure Access control (IAM).	
Generate a shared access signature (SAS).	

Explanation:

Reference:

<https://azure.microsoft.com/en-in/blog/announcing-the-preview-of-aad-authentication-for-storage/> <https://github.com/MicrosoftDocs/azure-docs/blob/master/articles/storage/common/storage-auth-aad-app.md>

**Question: 384**

HOTSPOT -

You have an Azure subscription that contains an Azure key vault named ContosoKey1.

You create users and assign them roles as shown in the following table.

Name	Subscription role assignment	ContosoKey1 role assignment
User1	Owner	None
User2	Security Admin	None
User3	None	User Access Administrator
User4	None	Key Vault Contributor

You need to identify which users can perform the following actions:

▫ Delegate permissions for ContosoKey1.

▫ Configure network access to ContosoKey1.

Which users should you identify? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

**Answer Area**

Delegate permissions for ContosoKey1:

	▼
User1 only	
User1 and User2 only	
User1 and User3 only	
User1 and User4 only	
User1, User2, and User3 only	
User1, User2, User3, and User4	

Configure network access to ContosoKey1:

	▼
User1 only	
User1 and User2 only	
User1 and User3 only	
User1 and User4 only	
User1, User2, and User3 only	
User1, User2, User3, and User4	

Answer:



## Answer Area

Delegate permissions for ContosoKey1:

	▼
User1 only	
User1 and User2 only	
User1 and User3 only	
User1 and User4 only	
User1, User2, and User3 only	
User1, User2, User3, and User4	

Configure network access to ContosoKey1:

	▼
User1 only	
User1 and User2 only	
User1 and User3 only	
User1 and User4 only	
User1, User2, and User3 only	
User1, User2, User3, and User4	

### Explanation:

Delegate permissions for ContosoKey1: User 1 and User 3

Configure network access to ContosoKey1: User 1 and User 4

Key Vault Contributor role definition includes Microsoft.KeyVault/\*, which means it has full rights and can therefore modify network access

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

### Question: 385

CertyIQ

You have an Azure subscription that contains four Azure SQL managed instances. You need to evaluate the vulnerability of the managed instances to SQL injection attacks. What should you do first?

- A. Create an Azure Sentinel workspace.
- B. Enable Advanced Data Security.
- C. Add the SQL Health Check solution to Azure Monitor.
- D. Create an Azure Advanced Threat Protection (ATP) instance.

**Answer: B**

### Explanation:

Advanced data security for SQL that is now Microsoft Azure Defender for SQL



**Question: 386**

DRAG DROP -

You have an Azure subscription named Sub1. Sub1 contains an Azure virtual machine named VM1 that runs Windows Server 2016.

You need to encrypt VM1 disks by using Azure Disk Encryption.

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**

Run Set-AzStorageAccount.

Create an Azure key vault.

Configure access policies for the Azure key vault.

Configure secrets for the Azure key vault.

Run Set-AzVMDiskEncryptionExtension.

**Answer Area**



**Answer:****Actions**

Run Set-AzStorageAccount.



Configure secrets for the Azure key vault.

**Answer Area**

Create an Azure key vault.

Configure access policies for the Azure key vault.

Run Set-AzVMDiskEncryptionExtension.

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-machines/windows/encrypt-disks>

**Question: 387**

You have an Azure subscription that contains a virtual machine named VM1.

You create an Azure key vault that has the following configurations:

- ⇒ Name: Vault5
- ⇒ Region: West US
- ⇒ Resource group: RG1

You need to use Vault5 to enable Azure Disk Encryption on VM1. The solution must support backing up VM1 by using Azure Backup.

Which key vault settings should you configure?

- A. Access policies
- B. Secrets

- C. Keys
- D. Locks

**Answer: A**

**Explanation:**

Access Policies.

Reference:

<https://docs.microsoft.com/en-us/azure/key-vault/key-vault-secure-your-key-vault>

**Question: 388**

CertyIQ

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

Name	Type	Region	Resource group
sa1	Azure Storage account	East US	RG1
VM1	Azure virtual machine	East US	RG2
KV1	Azure key vault	East US 2	RG1
SQL1	Azure SQL database	East US 2	RG2

You need to ensure that you can provide VM1 with secure access to a database on SQL1 by using a contained database user.

What should you do?

- A. Enable a managed identity on VM1.
- B. Create a secret in KV1.
- C. Configure a service endpoint on SQL1.
- D. Create a key in KV1.

**Answer: A**

**Explanation:**

A. Enable a managed identity on VM1.

**Question: 389**

CertyIQ

You have an Azure subscription named Sub1 that contains the Azure key vaults shown in the following table:

Name	Region	Resource group
Vault1	West Europe	RG1
Vault2	East US	RG1
Vault3	West Europe	RG2
Vault4	East US	RG2

In Sub1, you create a virtual machine that has the following configurations:

- Name: VM1
  - Size: DS2v2
  - Resource group: RG1
  - Region: West Europe
  - Operating system: Windows Server 2016
- You plan to enable Azure Disk Encryption on VM1.

In which key vaults can you store the encryption key for VM1?

- A. Vault1 or Vault3 only
- B. Vault1, Vault2, Vault3, or Vault4
- C. Vault1 only
- D. Vault1 or Vault2 only

**Answer: A**

**Explanation:**

In order to make sure the encryption secrets don't cross regional boundaries, Azure Disk Encryption needs the Key Vault and the VMs to be co-located in the same region. Create and use a Key Vault that is in the same region as the VM to be encrypted.

Reference:

<https://docs.microsoft.com/en-us/azure/security/azure-security-disk-encryption-prerequisites>

**Question: 390**

**CertyIQ**

HOTSPOT -

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

Name	Type
User1	Azure Active Directory (Azure AD) user
User2	Azure Active Directory (Azure AD) user
Group1	Azure Active Directory (Azure AD) group
Vault1	Azure key vault

User1 is a member of Group1. Group1 and User2 are assigned the Key Vault Contributor role for Vault1.

On January 1, 2019, you create a secret in Vault1. The secret is configured as shown in the exhibit. The date format YYYY-MM-DD is used on the exhibit. (Click the Exhibit tab.)

## Create a secret

### Upload options

Manual



\* Name

Password1



\* Value

• • • • • • • • • •



Content type (optional)

Set activation date?



Activation Date

2019-03-01



12:00:00 AM

(UTC+02:00) --- Current Time Zone ---



Set expiration date?



Expiration Date

2020-03-01



12:00:00 AM

(UTC+02:00) --- Current Time Zone ---



Enabled?

Yes

No

User2 is assigned an access policy to Vault1. The policy has the following configurations:

- Key Management Operations: Get, List, and Restore
- Cryptographic Operations: Decrypt and Unwrap Key
- Secret Management Operations: Get, List, and Restore

Group1 is assigned an access policy to Vault1. The policy has the following configurations:

- Key Management Operations: Get and Recover
- Secret Management Operations: List, Backup, and Recover

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

NOTE: Each correct selection is worth one point.

Hot Area:

## Answer Area

Statements	Yes	No
On January 1, 2019, User1 can view the value of Password1.	<input type="radio"/>	<input type="radio"/>
On June 1, 2019, User2 can view the value of Password1.	<input type="radio"/>	<input type="radio"/>
On June 1, 2019, User1 can view the value of Password1.	<input type="radio"/>	<input type="radio"/>

Answer:

## Answer Area

Statements	Yes	No
On January 1, 2019, User1 can view the value of Password1.	<input type="radio"/>	<input checked="" type="radio"/>
On June 1, 2019, User2 can view the value of Password1.	<input checked="" type="radio"/>	<input type="radio"/>
On June 1, 2019, User1 can view the value of Password1.	<input type="radio"/>	<input checked="" type="radio"/>

### Explanation:

1) On Jan 1 2019 User 1 can view the password 1 - No (Error: Either this secret is disabled or you do not have the "Get" secret permission.)

2) On June 1 2019 User2 can view the password1 - YES

3) On June 1 2019 User1 can view the Password1 - No

User 2 can see the Value no issues regardless of date because he has GET Secret Permission

## Question: 391

CertyIQ

HOTSPOT -

You have an Azure Active Directory (Azure AD) tenant named contoso1812.onmicrosoft.com that contains the users shown in the following table.

Name	Username	Type
User1	User1@contoso1812.onmicrosoft.com	Member
User2	User2@contoso1812.onmicrosoft.com	Member
User3	User3@contoso1812.onmicrosoft.com	Member
User4	User4@outlook.com	Guest

You create an Azure Information Protection label named Label1. The Protection settings for Label1 are configured



as shown in the exhibit. (Click the Exhibit tab.)

# Protection

Contoso1812 - Azure Information Protection

## Protections settings

Azure (cloud key)

HYOK (AD RMS)

Select the protection action type 

- ☒ Set permissions
- ☐ Set user-defined permissions (Preview)

USERS	PERMISSIONS
AuthenticatedUsers	Viewer
User1@contoso1812.onmicrosoft.com	Co-Author
User2@contoso1812.onmicrosoft.com	Reviewer

[+Add permissions](#)

Label1 is applied to a file named File1.  
For each of the following statements, select Yes if the statement is true, Otherwise, select No.  
NOTE: Each correct selection is worth one point.  
Hot Area:

## Answer Area

Statements	Yes	No
User1 can print File1.	<input type="radio"/>	<input type="radio"/>
User3 can read File1.	<input type="radio"/>	<input type="radio"/>
User4 can print File1.	<input type="radio"/>	<input type="radio"/>



Answer:

## Answer Area

Statements	Yes	No
User1 can print File1.	<input checked="" type="radio"/>	<input type="radio"/>
User3 can read File1.	<input checked="" type="radio"/>	<input type="radio"/>
User4 can print File1.	<input type="radio"/>	<input checked="" type="radio"/>

### Explanation:

- 1) YES - User 1 is a co-author, therefore can: View, Open, Read; Save; Edit Content, Edit; Copy; View Rights; Allow Macros; Save As, Export; Print; Reply; Reply All; Forward.
- 2) YES - User 3 is an AuthenticatedUser and therefore a viewer, so can: View, Open, Read; View Rights; Reply; Reply All; Allow Macros.
- 3) NO - User 4 is a guest, and has no permissions to this file.

<https://docs.microsoft.com/en-us/azure/information-protection/configure-usage-right>

### Question: 392

CertyIQ

#### SIMULATION -

You need to prevent HTTP connections to the rg1lod1234578n1 Azure Storage account.  
To complete this task, sign in to the Azure portal.

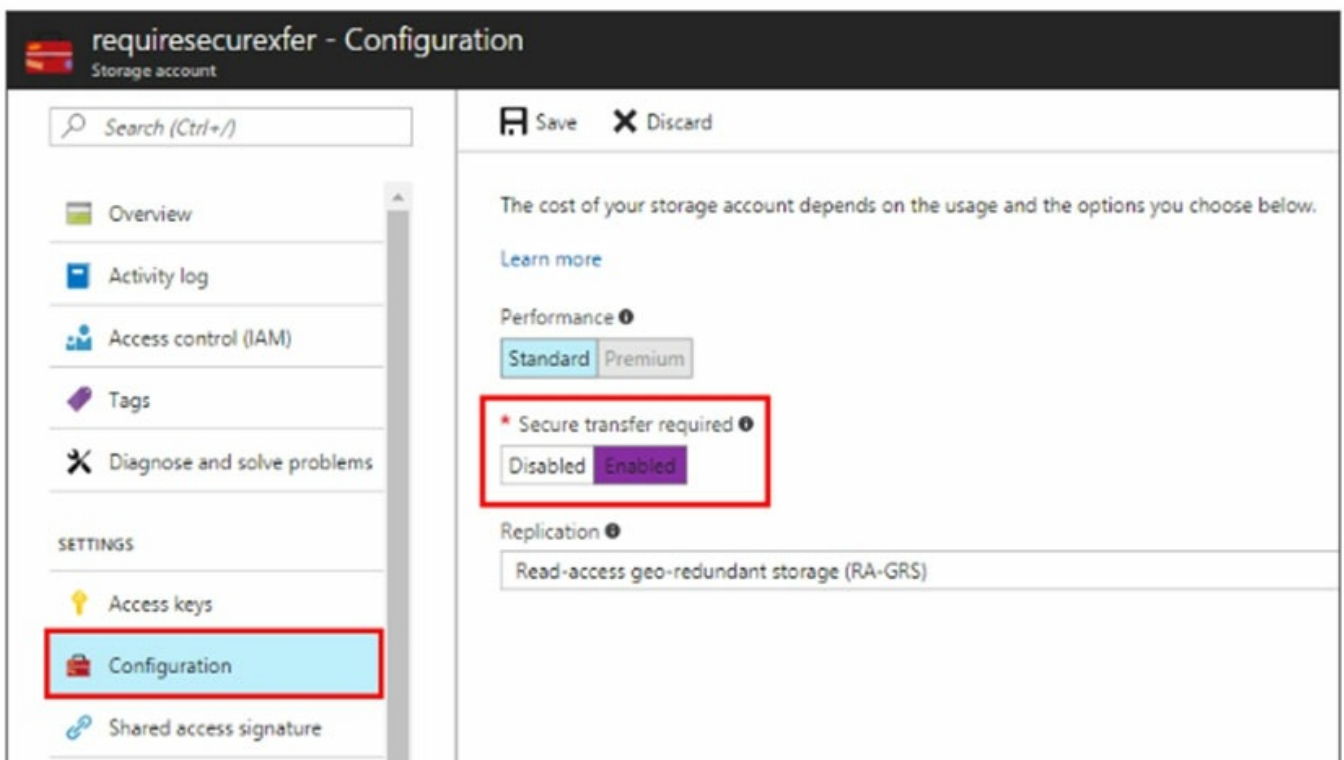
### Answer:

See the explanation below.

### Explanation:

The "Secure transfer required" feature is now supported in Azure Storage account. This feature enhances the security of your storage account by enforcing all requests to your account through a secure connection. This feature is disabled by default.

1. In Azure Portal select you Azure Storage account rg1lod12345678n1.
2. Select Configuration, and Secure Transfer required.



Reference:

<https://techcommunity.microsoft.com/t5/Azure/quot-Secure-transfer-required-quot-is-available-in-Azure-Storage/m-p/82475>

### Question: 393

CertyIQ

DRAG DROP -

Your network contains an on-premises Active Directory domain named contoso.com. The domain contains a user named User1.

You have an Azure subscription that is linked to an Azure Active Directory (Azure AD) tenant named contoso.com. The tenant contains an Azure Storage account named storage1. Storage1 contains an Azure file share named share1.

Currently, the domain and the tenant are not integrated.

You need to ensure that User1 can access share1 by using his domain credentials.

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

#### Answer Area

Create a private link to storage1.

Enable Active Directory Domain Services (AD DS) authentication on storage1.

Implement Azure AD Connect.

Create a service endpoint to storage1.

Assign share-level permissions for share1.

Answer:

### Actions

Create a private link to storage1.

Create a service endpoint to storage1.

### Answer Area

Implement Azure AD Connect.

Enable Active Directory Domain Services (AD DS) authentication on storage1.

Assign share-level permissions for share1.

### Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/storage/files/storage-files-identity-auth-active-directory-enable>

## Question: 394

CertyIQ

SIMULATION -

You need to ensure that the rg1lod1234578n1 Azure Storage account is encrypted by using a key stored in the KeyVault12345678 Azure key vault.

To complete this task, sign in to the Azure portal.



### Answer:

See the explanation below.

### Explanation:

Step 1: To enable customer-managed keys in the Azure portal, follow these steps:

1. Navigate to your storage account rg1lod1234578n1
2. On the Settings blade for the storage account, click Encryption. Select the Use your own key option, as shown in the following figure.

 Save  Discard

Storage service encryption protects your data at rest. Azure Storage encrypts your data as it's written in our datacenters, and automatically decrypts it for you as you access it.

By default, data is encrypted using Microsoft Managed Keys for Azure Blobs, Tables, Files and Queues. You may choose to bring your own key for encryption for Azure Blobs and Files. Encryption for Tables and Queues will always use Microsoft Managed Keys.

Please note that after enabling Storage Service Encryption, only new data will be encrypted, and any existing files in this storage account will retroactively get encrypted by a background encryption process.

[Learn more](#)

Your storage account is currently encrypted with Microsoft managed key by default. You can choose to use your own key.

☒ Use your own key

Step 2: Specify a key from a key vault

To specify a key from a key vault, first make sure that you have a key vault that contains a key. To specify a key from a key vault, follow these steps:

4. Choose the Select from Key Vault option.

5. Choose the key vault KeyVault1234578 containing the key you want to use.

6. Choose the key from the key vault.

Save Discard

Storage service encryption protects your data at rest. Azure Storage encrypts your data as it's written in our datacenters, and automatically decrypts it for you as you access it.

By default, data is encrypted using Microsoft Managed Keys for Azure Blobs, Tables, Files and Queues. You may choose to bring your own key for encryption for Azure Blobs and Files. Encryption for Tables and Queues will always use Microsoft Managed Keys.

Please note that after enabling Storage Service Encryption, only new data will be encrypted, and any existing files in this storage account will retroactively get encrypted by a background encryption process.

[Learn more](#)

Your storage account is currently encrypted with Microsoft managed key by default. You can choose to use your own key.

☒ Use your own key

Encryption key

☐ Enter key URI

☒ Select from Key Vault

\* Key Vault

<key-vault>

>

\* Encryption key

<key>

>

! <storage-account> will be granted access to the selected key vault. Both soft delete and purge protection will be enabled on the key vault and cannot be disabled. [Learn more](#)

Reference:

<https://docs.microsoft.com/en-us/azure/storage/common/storage-encryption-keys-portal>

### Question: 395

CertyIQ

You have a web app named WebApp1.  
You create a web application firewall (WAF) policy named WAF1.  
You need to protect WebApp1 by using WAF1.  
What should you do first?

- A. Deploy an Azure Front Door.
- B. Add an extension to WebApp1.
- C. Deploy Azure Firewall.

**Answer: A**

**Explanation:**

WAF is supported by both Application Gateway and Front Door

Reference:

<https://docs.microsoft.com/en-us/azure/frontdoor/quickstart-create-front-door>

### Question: 396

CertyIQ

You have an Azure subscription that contains an Azure SQL database named sql1.  
You plan to audit sql1.  
You need to configure the audit log destination. The solution must meet the following requirements:

- Support querying events by using the Kusto query language.
- Minimize administrative effort.

What should you configure?

- A. an event hub
- B. a storage account
- C. a Log Analytics workspace

**Answer: C**

**Explanation:**

Key phrase: ⇨ Support querying events by using the Kusto query language.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/tutorial-log-analytics-wizard>

**Question: 397**

CertyIQ

DRAG DROP -

You have an Azure subscription.

You plan to create a storage account.

You need to use customer-managed keys to encrypt the tables in the storage account.

From Azure Cloud Shell, which three cmdlets should you run in sequence? To answer, move the appropriate cmdlets from the list of cmdlets to the answer area and arrange them in the correct order.

Select and Place:

**Cmdlets**

**Answer Area**

New-AzStorageAccountKey

New-AzStorageTable

Register-AzProviderFeature

New-AzStorageAccount

Register-AzResourceProvider



**Answer:**

**Cmdlets**

**Answer Area**

Register-AzProviderFeature

Register-AzResourceProvider



New-AzStorageAccount

New-AzStorageAccountKey

New-AzStorageTable



**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/azure/storage/common/customer-managed-keys-configure-key-vault?tabs=powershell>

**Question: 398**

CertyIQ



## HOTSPOT -

You have an Azure subscription that contains the following resources:

- An Azure key vault
- An Azure SQL database named Database1

Two Azure App Service web apps named AppSrv1 and AppSrv2 that are configured to use system-assigned managed identities and access Database1

You need to implement an encryption solution for Database1 that meets the following requirements:

- The data in a column named Discount in Database1 must be encrypted so that only AppSrv1 can decrypt the data.
- AppSrv1 and AppSrv2 must be authorized by using managed identities to obtain cryptographic keys.

How should you configure the encryption settings for Database1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

### Answer Area

To configure the encryption of Database1:

- Always Encrypted by using Azure Key Vault.
- Always Encrypted by using the Windows Certificate Store.
- Transparent Data Encryption (TDE) by using Azure Key Vault integration.
- Transparent Data Encryption (TDE) by using Bring Your Own Key (BYOK).

To obtain the cryptographic keys:

- Create an access policy in Azure Key Vault.
- Generate a key on an HSM device.
- Import App Service certificates to AppSrv1 and AppSrv2.
- Register an enterprise application in Azure AD.

Answer:

### Answer Area

To configure the encryption of Database1:

- Always Encrypted by using Azure Key Vault.
- Always Encrypted by using the Windows Certificate Store.
- Transparent Data Encryption (TDE) by using Azure Key Vault integration.
- Transparent Data Encryption (TDE) by using Bring Your Own Key (BYOK).

To obtain the cryptographic keys:

- Create an access policy in Azure Key Vault.
- Generate a key on an HSM device.
- Import App Service certificates to AppSrv1 and AppSrv2.
- Register an enterprise application in Azure AD.

Explanation:

Always Encrypted by Using Azure Key Vault

Create an Access Policy in azure Key vault

<https://docs.microsoft.com/en-us/azure/azure-sql/database/always-encrypted-azure-key-vault-configure?tabs=azure-powershell#create-a-key-vault-to-store-your-keys>



You have an Azure subscription that contains the storage accounts shown in the following table.

Name	Type
storage1	Azure Blob storage
storage2	Azure Files SMB
storage3	Azure Table storage

You need to configure authorization access.  
Which authorization types can you use for each storage account? To answer, select the appropriate options in the answer area.  
NOTE: Each correct selection is worth one point.  
Hot Area:

**Answer Area**

storage1:

Shared Key only

Shared access signature (SAS) only

Azure Active Directory (Azure AD) only

Shared Key and shared access signature (SAS) only

Shared Key, shared access signature (SAS), and Azure Active Directory (Azure AD)

storage2:

Shared Key only

Shared access signature (SAS) only

Shared Key and shared access signature (SAS)

storage3:

Shared Key only

Shared access signature (SAS) only

Azure Active Directory (Azure AD) only

Shared Key and shared access signature (SAS) only

Shared Key, shared access signature (SAS), and Azure Active Directory (Azure AD)

**Answer:**

### Answer Area

storage1:

- Shared Key only
- Shared access signature (SAS) only
- Azure Active Directory (Azure AD) only
- Shared Key and shared access signature (SAS) only
- Shared Key, shared access signature (SAS), and Azure Active Directory (Azure AD)

storage2:

- Shared Key only
- Shared access signature (SAS) only
- Shared Key and shared access signature (SAS)

storage3:

- Shared Key only
- Shared access signature (SAS) only
- Azure Active Directory (Azure AD) only
- Shared Key and shared access signature (SAS) only
- Shared Key, shared access signature (SAS), and Azure Active Directory (Azure AD)

#### Explanation:

Azure Blobs - Shared Key, Shared Access Signature (SAS), Azure Active Directory (AAD)

Azure Files SMB - Shared Key only

Azure Tables - Shared Key, Shared Access Signature (SAS), Azure Active Directory (AAD)

Reference:

<https://docs.microsoft.com/en-us/azure/storage/common/authorize-data-access>

### Question: 400

CertyIQ

DRAG DROP -

You have an Azure Storage account named storage1 and an Azure virtual machine named VM1. VM1 has a premium SSD managed disk.

You need to enable Azure Disk Encryption for VM1.

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

- Run the `Set-AzVMDiskEncryptionExtension` cmdlet.
- Set the Key Vault access policy to **Enable access to Azure Virtual Machines for deployment**.
- Set the Key Vault access policy to **Enable access to Azure Disk Encryption for volume encryption**.
- Generate a key vault certificate.
- Create an Azure key vault.
- Configure storage1 to use a customer-managed key.

#### Answer Area

Answer:

#### Actions

Set the Key Vault access policy to <b>Enable access to Azure Virtual Machines for deployment</b> .
Generate a key vault certificate.
Configure storage1 to use a customer-managed key.

#### Answer Area

Create an Azure key vault.
Set the Key Vault access policy to <b>Enable access to Azure Disk Encryption for volume encryption</b> .
Run the <code>Set-AzVMDiskEncryptionExtension</code> cmdlet.

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-machines/windows/disk-encryption-key-vault>

#### Question: 401

CertyIQ

SIMULATION -

You need to enable Advanced Data Security for the SQLdb1 Azure SQL database. The solution must ensure that Azure Advanced Threat Protection (ATP) alerts are sent to [email protected]  
To complete this task, sign in to the Azure portal and modify the Azure resources.

Answer:

See the explanation below.

#### Explanation:

1. In the Azure portal, type SQL in the search box, select SQL databases from the search results then select SQLdb1. Alternatively, browse to SQL databases in the left navigation pane.
2. In the properties of SQLdb1, scroll down to the Security section and select Advanced data security.
3. Click on the Settings icon.
4. Tick the Enable Advanced Data Security at the database level checkbox.
5. Click Yes at the confirmation prompt.
6. In the Storage account select a storage account if one isn't selected by default.
7. Under Advanced Threat Protection Settings, enter [email protected] in the Send alerts to box.
8. Click the Save button to save the changes.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-sql/database/advanced-data-security>

#### Question: 402

CertyIQ

SIMULATION -

You need to configure a weekly backup of an Azure SQL database named Homepage. The backup must be retained for eight weeks.  
To complete this task, sign in to the Azure portal.

**Answer:**

See the explanation below.

**Explanation:**

You need to configure the backup policy for the Azure SQL database.

1. In the Azure portal, type Azure SQL Database in the search box, select Azure SQL Database from the search results then select Homepage. Alternatively, browse to Azure SQL Database in the left navigation pane.
2. Select the server hosting the Homepage database and click on Manage backups.
3. Click on Configure policies.
4. Ensure that the Weekly Backups option is ticked.
5. Configure the How long would you like weekly backups to be retained option to 8 weeks.
6. Click Apply to save the changes.

**Question: 403****CertyIQ****SIMULATION -**

You need to ensure that when administrators deploy resources by using an Azure Resource Manager template, the deployment can access secrets in an Azure key vault named KV12345678.  
To complete this task, sign in to the Azure portal.

**Answer:**

See the explanation below.

**Explanation:**

You need to configure an option in the Advanced Access Policy of the key vault.

1. In the Azure portal, type Azure Key Vault in the search box, select Azure Key Vault from the search results then select the key vault named KV12345678.  
Alternatively, browse to Azure Key Vault in the left navigation pane.
2. In the properties of the key vault, click on Advanced Access Policies.
3. Tick the checkbox labelled Enable access to Azure Resource Manager for template deployment.
4. Click Save to save the changes.

**Question: 404****CertyIQ****HOTSPOT -**

You have an Azure subscription that contains the storage accounts shown in the following table.

Name	Performance	Account kind	Azure Data Lake Storage Gen2
storage1	Standard	BlobStorage	Enabled
storage2	Premium	BlockBlobStorage	Disabled
storage3	Standard	Storage	Disabled
storage4	Premium	FileStorage	Disabled
storage5	Standard	StorageV2	Enabled

You enable Azure Defender for Storage.

Which storage services of storage5 are monitored by Azure Defender for Storage, and which storage accounts are protected by Azure Defender for Storage? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

## Answer Area

Monitored storage5 services:

- File services only
- Data Lake Storage only
- File services and table services only
- File service and Data Lake Storage only
- Data Lake Storage, file services, and table services

Protected storage accounts:

- storage3 and storage5 only
- storage1, storage2, and storage5 only
- storage1, storage4, and storage5 only
- storage1, storage2, storage3, storage4, and storage5

Answer:

### Answer Area

Monitored storage5 services:

- File services only
- Data Lake Storage only
- File services and table services only
- File service and Data Lake Storage only
- Data Lake Storage, file services, and table services

Protected storage accounts:

- storage3 and storage5 only
- storage1, storage2, and storage5 only
- storage1, storage4, and storage5 only
- storage1, storage2, storage3, storage4, and storage5

Explanation:

1st: File service and Data Lake Storage only

2nd: storage1, storage4, and storage5 only

## Question: 405

CertyIQ

You have an Azure subscription that contains an Azure key vault and an Azure Storage account. The key vault contains customer-managed keys. The storage account is configured to use the customer-managed keys stored in the key vault.

You plan to store data in Azure by using the following services:

- Azure Files
- Azure Blob storage
- Azure Table storage
- Azure Queue storage

Which two services support data encryption by using the keys stored in the key vault? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. Table storage
- B. Azure Files
- C. Blob storage
- D. Queue storage



**Answer: BC**

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/azure/storage/common/storage-service-encryption>

### Question: 406

CertyIQ

**SIMULATION -**

You need to ensure that connections through an Azure Application Gateway named Homepage-AGW are inspected for malicious requests.

To complete this task, sign in to the Azure portal.

You do not need to wait for the task to complete.

**Answer:**

See the explanation below.

**Explanation:**

You need to enable the Web Application Firewall on the Application Gateway.

1. In the Azure portal, type Application gateways in the search box, select Application gateways from the search results then select the gateway named Homepage-AGW. Alternatively, browse to Application Gateways in the left navigation pane.
2. In the properties of the application gateway, click on Web application firewall.
3. For the Tier setting, select WAF V2.
4. In the Firewall status section, click the slider to switch to Enabled.
5. In the Firewall mode section, click the slider to switch to Prevention.
6. Click Save to save the changes.

### Question: 407

CertyIQ

**SIMULATION -**

You need to create a web app named Intranet12345678 and enable users to authenticate to the web app by using Azure Active Directory (Azure AD).

To complete this task, sign in to the Azure portal.

**Answer:**

See the explanation below.

**Explanation:**

1. In the Azure portal, type App services in the search box and select App services from the search results.
2. Click the Create app service button to create a new app service.
3. In the Resource Group section, click the Create new link to create a new resource group.
4. Give the resource group a name such as Intranet12345678RG and click OK.
5. In the Instance Details section, enter Intranet12345678 in the Name field.
6. In the Runtime stack field, select any runtime stack such as .NET Core 3.1.
7. Click the Review + create button.
8. Click the Create button to create the web app.
9. Click the Go to resource button to open the properties of the new web app.
10. In the Settings section, click on Authentication / Authorization.
11. Click the App Service Authentication slider to set it to On.
12. In the Action to take when request is not authentication box, select Log in with Azure Active Directory.



**Question: 408**

DRAG DROP -

You have an Azure subscription that contains a Microsoft SQL server named Server1 and an Azure key vault named vault1. Server1 hosts a database named DB1. Vault1 contains an encryption key named key1.

DB1. Vault1 contains an encryption key named key1.

You need to ensure that you can enable Transparent Data Encryption (TDE) on DB1 by using key1.

Which four 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**

Create a managed identity for vault1.

Configure permissions for vault1.

Configure permissions for Server1.

Configure the TDE protector on Server1.

Create a managed identity for Server1.

Add key1 to Server1.

**Answer area****Answer:****Actions**

Create a managed identity for vault1.

Configure permissions for vault1.

**Answer area**

Create a managed identity for Server1.

Configure permissions for Server1.

Add key1 to Server1.

Configure the TDE protector on Server1.

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/azure/azure-sql/database/transparent-data-encryption-byok-configure?tabs=azure-powershell>

### Question: 409



CertyIQ

HOTSPOT -


You have an Azure subscription that contains an Azure key vault named KeyVault1 and the virtual machines shown in the following table.


Name	Private IP address	Public IP address	Connected to
VM1	10.7.0.4	51.144.245.152	VNET1/Default
VM2	10.8.0.4	104.45.9.227	VNET2/Default

You set the Key Vault access policy to Enable access to Azure Disk Encryption for volume encryption. KeyVault1 is configured as shown in the following exhibit.


 Save  Discard

Allow access from: ☐ All networks ☒ Selected networks

 Configure network access control for your key vault. [Learn More](#)

Virtual networks:  [+ Add existing virtual networks](#) [+ Add new virtual network](#)


VIRTUAL NETWORK	SUBNET	RESOURCE GROUP	SUBSCRIPTION
VNET1	default	RG1	...

Firewall: 


IPv4 ADDRESS OR CIDR

IPv4 address or CIDR ...

Exception:

Allow trusted Microsoft services to bypass this firewall? 

☒ Yes ☐ No

 This setting is related to firewall only. In order to access this key vault, the trusted service must also be given explicit permissions in the Access policies section.

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

NOTE: Each correct selection is worth one point.

Hot Area:

#### Answer Area

Statements	Yes	No
From VM1, users can manage the keys and secrets stored in KeyVault1.	<input type="radio"/>	<input type="radio"/>
From VM2, users can manage the keys and secrets stored in KeyVault1.	<input type="radio"/>	<input type="radio"/>
VM2 can use KeyVault1 for Azure Disk Encryption.	<input type="radio"/>	<input type="radio"/>

Answer:

### Answer Area

#### Statements

Yes No

From VM1, users can manage the keys and secrets stored in KeyVault1.

☒ ☐

From VM2, users can manage the keys and secrets stored in KeyVault1.

☐ ☒

VM2 can use KeyVault1 for Azure Disk Encryption.

☒ ☐

#### Explanation:

1. Yes 2. No 3. Yes

Selected Networks for VNET1 and the exemption to allow access to the key vault, VM1 has access, VM2 doesn't. The last option, VM2 should be able to still user the ADE, the exemption only applies to the access to the key vault.

### Question: 410

CertyIQ

You have an Azure subscription that contains an Azure SQL database named DB1 in the East US Azure region. You create the storage accounts shown in the following table.

Name	Location	Performance	Premium account type
storage1	East US	Standard	Not applicable
storage2	East US	Premium	Block blobs
storage3	East US	Premium	File shares
storage4	East US 2	Standard	Not applicable

You plan to enable auditing for DB1.

Which storage accounts can you use as the auditing destination for DB1?

- A. storage1 and storage4 only
- B. storage1 only
- C. storage1, storage2, storage3, and storage4
- D. storage1, storage2, and storage3 only
- E. storage2 and storage3 only

#### Answer: D

#### Explanation:

SQL Azure auditing can use standard accounts

"Premium storage with BlockBlobStorage is supported. Standard storage is supported."

<https://learn.microsoft.com/en-us/azure/azure-sql/database/auditing-overview?view=azuresql#remarks>

Also:

"If you are deploying from the Azure portal, be sure that the storage account is in the same region as your

database and server. If you are deploying through other methods, the storage account can be in any region."

<https://learn.microsoft.com/en-us/azure/azure-sql/database/auditing-overview?view=azuresql#audit-storage-destination>

that means everything in the list except for Azure File shares.

#### Question: 411

CertyIQ

DRAG DROP -

You have an Azure subscription that contains an Azure SQL database named SQLDB1. SQLDB1 contains the columns shown in the following table.

Name	Data type	Sample value
Email	Varchar	admin@contoso.com
Birthday	Date	2010-07-07

For the Email and Birthday columns, you implement dynamic data masking by using the default masking function. Which value will the users see in each column? To answer, drag the appropriate values to the correct columns. Each value may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:

#### Values

1900-01-01

1900-01-01 00:00:00.0000

2010-XX-XX

XXXX

aXXXX@XXXX.com

XXXX@XXXX.com

XXXX@XXXX.XXX

#### Answer Area

Email:

Value

Birthday:

Value

Answer:

**Values****Answer Area**Email: Birthday: **Explanation:**

Box 1: aXXXX @XXXX.com -

The Email masking method, exposes the first letter and replaces the domain with XXX.com using a constant string prefix in the form of an email address.

Example: [email protected] -

Box 2: 1900-01-01 -

Use 01-01-1900 (or 1900-01-01) for date/time data types (date, datetime2, datetime, datetimeoffset, smalldatetime, time).

Reference:

<https://docs.microsoft.com/en-us/azure/azure-sql/database/dynamic-data-masking-overview>**Question: 412****CertyIQ**

HOTSPOT -

You have a hybrid Azure Active Directory (Azure AD) tenant named contoso.com that contains a user named User1 and the servers shown in the following table.

Name	Operating system	Configuration
Server1	Windows Server 2016	Domain-joined
Server2	Windows Server 2022	Domain-joined

The tenant is linked to an Azure subscription that contains a storage account named storage1. The storage1 account contains a file share named share1.

User1 is assigned the Storage File Data SMB Share Contributor role for storage1.

The Security protocol settings for the file shares of storage1 are configured as shown in the following exhibit.



Azure Files exposes settings that let you toggle the SMB protocol to be more compatible or more secure, depending on your organization's requirements. Restricting these settings may prevent some clients from being able to connect. [Learn more](#)

Profile

Custom

SMB protocol versions

- ☐ SMB 2.1
- ☐ SMB 3.0
- ☒ SMB 3.1.1

SMB channel encryption

- ☐ None
- ☐ AES-128-CCM
- ☐ AES-128-GCM
- ☐ AES-256-GCM

Authentication mechanisms

- ☐ NTLM v2
- ☒ Kerberos

Kerberos ticket encryption

- ☒ RC4-HMAC
- ☒ AES-256

**i** For more information on support for protocol settings in SMB clients, see [SMB on Windows](#) and [SMB on Linux](#).

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

Answer Area

Statements	Yes	No
User1 can map share1 to Server1 by using the access key of storage1.	<input type="radio"/>	<input type="radio"/>
User1 can map share1 to Server1 by using the user's credentials.	<input type="radio"/>	<input type="radio"/>
User1 can map share1 to Server2 by using the access key of storage1.	<input type="radio"/>	<input type="radio"/>

Answer:



## Answer Area

Statements	Yes	No
User1 can map share1 to Server1 by using the access key of storage1.	<input type="radio"/>	<input checked="" type="radio"/>
User1 can map share1 to Server1 by using the user's credentials.	<input checked="" type="radio"/>	<input type="radio"/>
User1 can map share1 to Server2 by using the access key of storage1.	<input type="radio"/>	<input checked="" type="radio"/>

### Explanation:

Box 1: No -

Kerberos uses user's credentials, not access keys.

Box 2: Yes -

Kerberos uses user's credentials.

Box 3: No -

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy-configure-single-sign-on-with-kcd>

## Question: 413

CertyIQ

You have an on-premises network and an Azure subscription.

You have the Microsoft SQL Server instances shown in the following table.

Name	Type
sql1	Azure SQL managed instance
sql2	SQL Server 2019 on an Azure virtual machine that runs Windows Server 2019
sql3	SQL Server 2019 on an Azure virtual machine that runs Red Hat Enterprise Linux (RHEL) 8.3
sql4	On-premises physical server that runs Windows Server 2016 and has SQL Server 2016 installed

You plan to implement Microsoft Defender for SQL.

Which SQL Server instances will be protected by Microsoft Defender for SQL?

- A. sql1 and sql2 only
- B. sql1, sql2, and sql3 only
- C. sql1, sql2, and sql4 only
- D. sql1, sql2, sql3, and sql4

### Answer: D

### Explanation:

Microsoft Defender for SQL protected versions:

\* Azure SQL Managed Instance (sql1)

\* SQL on Azure virtual machines

SQL Server on Windows Azure Virtual Machines (sql2)

SQL Server on Linux Azure Virtual Machines including Red Hat Enterprise Linux (RHEL) 8 (sql3)

\* On-premises SQL servers on Windows machines without Azure Arc (sql4)

- \* Azure SQL single databases and elastic pools
- \* SQL Server on Azure Arc-enabled servers
- \* Azure Synapse Analytics (formerly SQL DW) dedicated SQL pool

Reference:

<https://docs.microsoft.com/en-us/azure/defender-for-cloud/defender-for-sql-introduction> <https://docs.microsoft.com/en-us/azure/azure-sql/virtual-machines/windows/sql-server-on-azure-vm-iaas-what-is-overview> <https://docs.microsoft.com/en-us/azure/azure-sql/virtual-machines/linux/sql-server-on-linux-vm-what-is-iaas-overview>

## Question: 414

CertyIQ

HOTSPOT

-

You have a Microsoft Sentinel deployment.

You need to connect a third-party security solution to the deployment. The third-party solution will send Common Event Format (CEF)-formatted messages.

What should you include in the solution? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

### Answer Area

Deploy:

▼

A Linux server and a Syslog forwarder daemon

A Windows server and a Windows Event Forwarding subscription

An Azure event hub that has a dedicated namespace

Forward events to Microsoft Sentinel by using:

▼

A Dependency agent

An Azure Arc enabled servers Connected Machine agent

An Azure Log Analytics agent

Answer:

### Answer Area

Deploy:

▼

A Linux server and a Syslog forwarder daemon

A Windows server and a Windows Event Forwarding subscription

An Azure event hub that has a dedicated namespace

Forward events to Microsoft Sentinel by using:

▼

A Dependency agent

An Azure Arc enabled servers Connected Machine agent

An Azure Log Analytics agent

Explanation:




Deploy: A Linux server and a syslog forwarder deamon

**Question: 415**

CertyIQ

You have an Azure subscription that contains an Azure SQL Database logic server named SQL1 and an Azure virtual machine named VM1. VM1 uses a private IP address only.


The Firewall and virtual networks settings for SQL1 are shown in the following exhibit.

 Save  Discard  Add client IP

---

Deny public network access ⓘ  

Yes No

 Click here to create a new private endpoint.  
[Create Private Endpoint](#)

Minimum TLS Version ⓘ  

1.0 1.1 1.2

Connection Policy ⓘ  

Default Proxy Redirect

Allow Azure services and resources to access this server ⓘ  

Yes No

Client IP address 89.212.25.106

Rule name	Start IP	End IP	
<input type="text"/>	<input type="text"/>	<input type="text"/>	...

No firewall rules configured.

Virtual networks  
[+ Add existing virtual network](#) [+ Create new virtual network](#)

Rule name	Virtual network	Subnet
No vnet rules for this server.		

You need to ensure that VM1 can connect to SQL1. The solution must use the principle of least privilege.

What should you do?

- A. Set Connection Policy to Proxy.
- B. Set Allow Azure services and resources to access this server to Yes.
- C. Add an existing virtual network.
- D. Create a new firewall rule.

**Answer: C**

**Explanation:**

The Azure SQL Database firewall allows you to specify IP address ranges from which communications are accepted into SQL Database. This approach is fine for stable IP addresses that are outside the Azure private network. However, virtual machines (VMs) within the Azure private network are configured with dynamic IP addresses. Dynamic IP addresses can change when your VM is restarted and in turn invalidate the IP-based firewall rule. It would be folly to specify a dynamic IP address in a firewall rule, in a production environment.

You can work around this limitation by obtaining a static IP address for your VM. For details, see [Create a virtual machine with a static public IP address using the Azure portal](#). However, the static IP approach can become difficult to manage, and it's costly when done at scale.

Virtual network rules are easier alternative to establish and to manage access from a specific subnet that contains your VMs.

**Question: 416**

**CertyIQ**

You have an Azure Active Directory (Azure AD) tenant that contains a group named Group1.

You need to ensure that the members of Group1 sign in by using passwordless authentication.

What should you do?

- A. Configure the sign-in risk policy.
- B. Create a Conditional Access policy.
- C. Configure the Microsoft Authenticator authentication method policy.
- D. Configure the certificate-based authentication (CBA) policy.

**Answer: C**

**Explanation:**

Microsoft [...] offer the following three passwordless authentication options that integrate with Azure Active Directory (Azure AD):

\* Windows Hello for Business

\* Microsoft Authenticator

\* FIDO2 security keys

<https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-passwordless>

**Question: 417**

**CertyIQ**

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

Name	Type
storage1	Storage account
KeyVault1	Azure key vault

You need to configure storage1 to regenerate keys automatically every 90 days.

Which cmdlet should you run?

- A. Add-AzKeyVaultManagedStorageAccount
- B. Set-AzStorageAccountManagementPolicy
- C. Set-AzStorageAccount
- D. Add-AzStorageAccountManagementPolicyAction

**Answer: A**

**Explanation:**

Add-AzKeyVaultManagedStorageAccount

#### Question: 418

CertyIQ

HOTSPOT

-

You have an Azure subscription that contains the key vaults shown in the following table.

Name	Days to retain deleted vaults	Purge protection	Permission model
KeyVault1	10	Enabled	Azure role-based access control (Azure RBAC)
KeyVault2	15	Disabled	Azure role-based access control (Azure RBAC)

The subscription contains the users shown in the following table.

Name	Role	Assigned to
Admin1	Key Vault Contributor	KeyVault1
Admin2	Key Vault Secrets Officer	KeyVault2
Admin3	Key Vault Administrator	KeyVault1

On June 1, you perform the following actions:

- Delete a key named key1 from KeyVault1.
- Delete a secret named secret1 from KeyVault2.

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

NOTE: Each correct selection is worth one point.

Statements	Yes	No
Admin1 can recover key1 on June 5.	<input type="radio"/>	<input type="radio"/>
Admin2 can purge secret1 on June 12.	<input type="radio"/>	<input type="radio"/>
Admin3 can recover key1 on June 17.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
Admin1 can recover key1 on June 5.	<input checked="" type="radio"/>	<input type="radio"/>
Admin2 can purge secret1 on June 12.	<input type="radio"/>	<input checked="" type="radio"/>
Admin3 can recover key1 on June 17.	<input type="radio"/>	<input checked="" type="radio"/>

Explanation:

Box1: Yes

Admin1 is Key Vault Contributor on KeyVault1, in which has 10 days to retain deleted vaults, and Key1 from KeyVault1 was deleted on Jun 1st. Hence on Jun 5th, Admin1 can recover Key1

Box2: No

On Jun 1st, secret1 has already been deleted. Hence it cannot be purged again on Jun 12th

Box3: No

KeyVault1 has 10 days to retain deleted vaults, and Key1 from KeyVault1 was deleted on Jun 1st. Hence on Jun 17th it cannot be recovered

### Question: 419

CertyIQ

HOTSPOT

-

You have an Azure Active Directory (Azure AD) tenant that contains two administrative units named AU1 and AU2.

Users are assigned to the administrative units as shown in the following table.



User name	Member of
Admin1	AU1
Admin2	AU1
Admin3	AU2
Admin4	AU2
User1	AU1
User2	AU1
User3	AU2
User4	AU2

Users are assigned the roles shown in the following table.

User	Administrative unit	Role
Admin1	AU1	Helpdesk administrator
Admin2	AU1	Groups administrator
Admin3	AU2	Password administrator
Admin4	AU2	User administrator

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

NOTE: Each correct selection is worth one point

Statements	Yes	No
Admin1 can reset the password of User1.	<input type="radio"/>	<input type="radio"/>
Admin2 can reset the password of User3.	<input type="radio"/>	<input type="radio"/>
Admin3 can reset the password of Admin4.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
Admin1 can reset the password of User1.	<input checked="" type="radio"/>	<input type="radio"/>
Admin2 can reset the password of User3.	<input type="radio"/>	<input checked="" type="radio"/>
Admin3 can reset the password of Admin4.	<input type="radio"/>	<input checked="" type="radio"/>

**Explanation:**

1. yes - Helpdesk Administrator can reset password for non-administrators. 2. no - Group Admin cannot reset password from any user. 3. no - Password Administrator cannot reset password from User Administrator.

Reference:

<https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#who-can-reset-passwords>

**Question: 420****CertyIQ**

You have an Azure subscription that contains an Azure key vault named Vault1 and a virtual machine named VM1. VM1 has the Key Vault VM extension installed.

For Vault1, you rotate the keys, secrets, and certificates.

What will be updated automatically on VM1?

- A. the keys only
- B. the secrets only
- C. the certificates only
- D. the keys and secrets only
- E. the secrets and certificates only
- F. the keys, secrets, and certificates

**Answer: C****Explanation:**

The Key Vault VM extension provides automatic refresh of certificates stored in an Azure key vault. Specifically, the extension monitors a list of observed certificates stored in key vaults, and, upon detecting a change, retrieves, and installs the corresponding certificates."

<https://learn.microsoft.com/en-us/azure/virtual-machines/extensions/key-vault-windows?tabs=version3>

**Question: 421****CertyIQ**

HOTSPOT

-

You have an Azure SQL database named DB1 that contains a table named Table1.

You need to configure DB1 to meet the following requirements:

- Sensitive data in Table1 must be identified automatically.
- Only the first character and last character of the sensitive data must be displayed in query results.

Which two features should you configure? To answer, select the features in the answer area.

NOTE: Each correct selection is worth one point.



# DB1

SQL database



Search (Ctrl+/)



Auditing



Ledger



Data Discovery & Classification



Dynamic Data Masking



Microsoft Defender for Cloud



Transparent data encryption

## Intelligent Performance



Performance overview



Performance recommendations



Query Performance Insight



Automatic tuning

## Monitoring



Alerts



Metrics



Diagnostic settings



Logs

Answer:



# DB1

SQL database



Search (Ctrl+/)



Auditing



Ledger



Data Discovery & Classification



Dynamic Data Masking



Microsoft Defender for Cloud



Transparent data encryption

## Intelligent Performance



Performance overview



Performance recommendations



Query Performance Insight



Automatic tuning

## Monitoring



Alerts



Metrics



Diagnostic settings



Logs

You have an Azure subscription that contains two users named User1 and User2 and the blob containers shown in the following table.

Name	Storage account	Access policy
container1	storage1	Policy1
container2	storage1	None

Policy1 is configured as shown in the following exhibit.

## Edit policy

Identifier \*

Policy1

Permissions

Read

Start time

12/15/2021 12:00:00 AM

(UTC+01:00) Belgrade, Bratisl...

Expiry time

12/31/2021 12:00:00 AM

(UTC+01:00) Belgrade, Bratisl...

OK

Cancel

You assign the roles for storage1 as shown in the following table.

User	Role
User1	Storage Blob Data Reader
User2	Contributor

The storage1 account has the following shared access signature (SAS) named SAS1:

- Allowed services: Blob
- Allowed resource types: Container
- Allowed permissions: Read, Write, List, Add, Create
- Blob versioning permissions: enables deletion of versions
- Allowed blob index permissions: Read/Write
- Start and expiry date/time:
  - o Start: 12/1/2021
  - o End: 12/31/2021

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

NOTE: Each correct selection is worth one point.

Statements	Yes	No
When using SAS1, User1 can write to container2 on December 5, 2021.	<input type="radio"/>	<input type="radio"/>
When using SAS1, User2 can write to container1 on December 20, 2021.	<input type="radio"/>	<input type="radio"/>
When using SAS1, User1 can read from container2 on January 10, 2022.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
When using SAS1, User1 can write to container2 on December 5, 2021.	<input checked="" type="radio"/>	<input type="radio"/>
When using SAS1, User2 can write to container1 on December 20, 2021.	<input checked="" type="radio"/>	<input type="radio"/>
When using SAS1, User1 can read from container2 on January 10, 2022.	<input type="radio"/>	<input checked="" type="radio"/>

**Question: 423**
CertyIQ

HOTSPOT

-

Your on-premises network contains the servers shown in the following table.

Name	Operating system	Description
Server1	Windows Server 2019	Hyper-V host hosting four virtual machines that run Windows Server 2022
Server2	Windows Server 2019	File server that has the Azure Arc agent installed
Server3	SUSE Linux Enterprise Server (SLES)	Database server that has the Azure Arc agent installed

You have an Azure subscription that contains multiple virtual machines that run either Windows Server 2019 or SLES.

You plan to implement adaptive application controls in Microsoft Defender for Cloud.

Which operating systems and platforms can you monitor? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



## Answer Area

Operating systems

▼

Windows Server only  
SLES only  
SLES and Windows Servers

Platforms

▼

Azure virtual machines only  
Azure virtual machines and Hyper-V virtual machines only  
Azure Arc-enabled servers and Azure virtual machines only  
Azure virtual machines, Hyper-V virtual machines, and Azure Arc-enabled servers

Answer:

## Answer Area

Operating systems

▼

Windows Server only  
SLES only  
SLES and Windows Servers

Platforms

▼

Azure virtual machines only  
Azure virtual machines and Hyper-V virtual machines only  
Azure Arc-enabled servers and Azure virtual machines only  
Azure virtual machines, Hyper-V virtual machines, and Azure Arc-enabled servers

## Question: 424

CertyIQ

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

Name	Type
DB1	Azure Cosmos DB account
VM1	Virtual machine
VM2	Virtual machine
VNET1	Virtual network
NSG1	Network security group (NSG)

Both VM1 and VM2 connect to VNET1 and are configured to use NSG1.

You need to ensure that only VM1 and VM2 can access DB1.

What should you do?

- A. For NSG1, configure a rule that has a service tag.
- B. Add the IP address range of VNET1 to the Firewall settings of DB1.
- C. Create an application security group.

D. Configure DB1 to allow access from only VNET1.

**Answer: D**

**Explanation:**

Configure DB1 to allow access from only VNET1.

How would configuring the NSG that VM1 and VM2 are attached to influence who is allowed to access DB1? You have to configure DB1 in a way that I only allows VM1 & VM2, one possible option would be allowing the VNET1 to access DB1

**Question: 425**

**CertyIQ**

You have an Azure AD tenant that contains a user named User1.

You purchase an app named App1.

User1 needs to publish App1 by using Azure AD Application Proxy.

Which role should you assign to User1?

- A. Cloud application administrator
- B. Application administrator
- C. Hybrid identity administrator
- D. Cloud App Security Administrator

**Answer: B**

**Explanation:**

Application administrator is correct.

<https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#cloud-application-administrator>

**Question: 426**

**CertyIQ**

HOTSPOT

-

You have an Azure AD tenant named contoso.com that contains the users shown in the following table.

Name	Role
User1	Application administrator
User2	Application developer
User3	Azure DevOps administrator
User4	Security operator

You add enterprise applications to contoso.com as shown in the following table.

Name	Owner	User and groups
App1	User3	User4
App2	User4	User3

You need to identify which users can grant admin consent for App1 and App2.

Which users should you identify for each application? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

## Answer Area

App1:  ▼

- User1 only
- User1 and User2 only
- User1 and User3 only
- User1, User2 and User3 only
- User1, User2, User3, and User4

App2:  ▼

- User1 only
- User1 and User2 only
- User1 and User4 only
- User1, User2 and User4 only
- User1, User2, User3, and User4

Answer:

### Answer Area

App1:  ▼

- User1 only
- User1 and User2 only
- User1 and User3 only
- User1, User2 and User3 only
- User1, User2, User3, and User4

App2:  ▼

- User1 only
- User1 and User2 only
- User1 and User4 only
- User1, User2 and User4 only
- User1, User2, User3, and User4

**Explanation:**

Box1: User1 only

Box2: User1 only

To grant tenant-wide admin consent, you need: An Azure AD user account with one of the following roles: 1) Global Administrator or Privileged Role Administrator, for granting consent for apps requesting any permission, for any API. 2) Cloud Application Administrator or Application Administrator, for granting consent for apps requesting any permission for any API, except Azure AD Graph or Microsoft Graph app roles (application permissions). 3) A custom directory role that includes the permission to grant permissions to applications, for the permissions required by the application.

<https://learn.microsoft.com/EN-US/azure/active-directory/manage-apps/grant-admin-consent?pivots=portal>

**Question: 427**

**CertyIQ**

DRAG DROP

Your network contains an on-premises Active Directory domain named contoso.com. The domain contains a user named User1.

You have an Azure subscription that is linked to an Azure Active Directory (Azure AD) tenant named contoso.com. The tenant contains an Azure Storage account named storage1. Storage1 contains an Azure file share named share1.

Currently, the domain and the tenant are not integrated.

You need to ensure that User1 can access share1 by using his domain credentials.

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.

**Actions**

**Answer Area**

Create a private link to storage1.

Enable an Active Directory source for Azure File shares

Implement Azure AD Connect.

Create a service endpoint to storage1.

Assign share-level permissions for share1.

**Answer:**

### Answer Area

Implement Azure AD Connect.

Enable an Active Directory source for Azure File shares

Assign share-level permissions for share1.

### Question: 428

CertyIQ

HOTSPOT

-

You have a Microsoft Sentinel deployment.

You need to connect a third-party security solution to the deployment. The third-party solution will send Common Event Format (CEF)-formatted messages.

What should you include in the solution? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

### Answer Area

Deploy:

- A Linux server and a Syslog forwarder daemon
- A Windows server and a Windows Event Forwarding subscription
- An Azure event hub that has a dedicated namespace

Forward events to Microsoft Sentinel by using:

- A Dependency agent
- An Azure Arc enabled servers Connected Machine agent
- An Azure Monitor agent

Answer:

### Answer Area

Deploy:

- A Linux server and a Syslog forwarder daemon
- A Windows server and a Windows Event Forwarding subscription
- An Azure event hub that has a dedicated namespace

Forward events to Microsoft Sentinel by using:

- A Dependency agent
- An Azure Arc enabled servers Connected Machine agent
- An Azure Monitor agent

**Question: 429**

You have an Azure subscription that contains the virtual machines shown in the following table.

Name	Operating system
Computer1	Windows 10
Computer2	Windows Server 2022
Computer3	SUSE Linux Enterprise Server (SLES)

Which computers will support file integrity monitoring?

- A.Computer2 only
- B.Computer1 and Computer2 only
- C.Computer2 and Computer3 only
- D.Computer1, Computer2, and Computer3

**Answer: D**

**Explanation:**

D. Computer1, Computer2, and Computer3

<https://learn.microsoft.com/en-us/azure/defender-for-cloud/file-integrity-monitoring-overview>

**Question: 430**

SIMULATION

-

The developers at your company plan to create a web app named App28681041 and to publish the app to <https://www.contoso.com>.

You need to perform the following tasks:

- Ensure that App28681041 is registered to Azure AD.
- Generate a password for App28681041.

To complete this task, sign in to the Azure portal.

**Answer:**



Register an application with the Microsoft identity platform (Steps 1-8 below)

### Register an application

Registering your application establishes a trust relationship between your app and the Microsoft identity platform. The trust is **unidirectional**: your app trusts the Microsoft identity platform, and not the other way around. Once created, the application object cannot be moved between different tenants.

Follow these steps to create the app registration:

Step 1: Sign in to the Azure portal.

Step 2: If you have access to multiple tenants, use the **Directories + subscriptions** filter in the top menu to switch to the tenant in which you want to register the application.

Step 3: Search for and select **Azure Active Directory**.

Step 4: Under **Manage**, select **App registrations** > **New registration**.

Step 5: Enter a display Name for your application. Users of your application might see the display name when they use the app, for example during sign-in. You can change the display name at any time and multiple app registrations can share the same name. The app registration's automatically generated Application (client) ID, not its display name, uniquely identifies your app within the identity platform.

Step 6: Specify who can use the application, sometimes called its sign-in audience.

\* Details omitted\*

Step 7: Don't enter anything for Redirect URI (optional). You'll configure a redirect URI in the next section.

Step 8: Select **Register** to complete the initial app registration.

Register an application - Microsoft x +

https://portal.azure.com

Microsoft Azure Search resources, services, and docs (G+/)

meganb@contoso.com CONTOSO AD (DEV)

Home > Contoso AD (dev) >

## Register an application

\* Name

The user-facing display name for this application (this can be changed later).

Supported account types

Who can use this application or access this API?

☒ Accounts in this organizational directory only (Contoso AD (dev) only - Single tenant)

☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant)

☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

☐ Personal Microsoft accounts only

[Help me choose...](#)

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web e.g. https://myapp.com/auth

By proceeding, you agree to the Microsoft Platform Policies [?](#)

Register

Now for the password.

Add a client secret

Sometimes called an application password, a client secret is a string value your app can use in place of a certificate to identify itself.

1. In the Azure portal, in **App registrations**, select your application.
2. Select **Certificates & secrets** > **Client secrets** > **New client secret**.
3. Add a description for your client secret.
4. Select an expiration for the secret or specify a custom lifetime. Client secret lifetime is limited to two years (24 months) or less. You can't specify a custom lifetime longer than 24 months. Microsoft recommends that you set an expiration value of less than 12 months.
5. Select **Add**.
6. Record the secret's value for use in your client application code. This secret value is never displayed again after you leave this page.

Reference:

<https://learn.microsoft.com/en-us/azure/active-directory/develop/quickstart-register-app>

**Question: 431****CertyIQ**

You have an Azure AD tenant that contains the users shown in the following table.

Name	Description
User1	Uses app password authentication for the Mail and Calendar app in Windows 10
User2	Uses Outlook on the web

You need to ensure that the users cannot create app passwords. The solution must ensure that User1 can continue to use the Mail and Calendar app.

What should you do?

- A.Assign User1 the Authentication Policy Administrator role.
- B.Enable Azure AD Password Protection.
- C.Configure a multi-factor authentication (MFA) registration policy.
- D.Create a new app registration.
- E.From multi-factor authentication, configure the service settings.

**Answer: E**

**Explanation:**

From multi-factor authentication, configure the service settings.

**Question: 432****CertyIQ**

DRAG DROP

-

You have an Azure subscription named Sub1 that contains the storage accounts shown in the following table.

Name	Resource group
storage1	RG1
storage2	RG1
storage3	RG2

The storage3 storage account is encrypted by using customer-managed keys.

You need to enable Microsoft Defender for Storage to meet the following requirements:

- The storage1 and storage2 accounts must be included in the Defender for Storage protections.
- The storage3 account must be excluded from the Defender for Storage protections.

Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area.

## Actions

## Answer Area

For storage3, disable the customer-managed keys.

Disable Defender for Storage for storage3.

1

Enable the Defender for Storage plan for Sub1.



2



For storage3, assign the AzDefenderPlanAutoEnable tag and set the value to **off**.

3

Enable the Defender for Storage plan for RG1.

Answer:

## Answer Area

1

Enable the Defender for Storage plan for Sub1.

2

For storage3, assign the AzDefenderPlanAutoEnable tag and set the value to **off**.

3

Disable Defender for Storage for storage3.

### Explanation:

Enable the Defender For storage plan for sub 1.

For storage 3,assign the AZ Defender Plan Auto Enable tag and set the value to off.

Disable Defender for storage for Storage 3.

### Question: 433

CertyIQ

You have an Azure subscription that contains the virtual machines shown in the following table.

Name	Operating system
VM1	Windows Server 2019
VM2	Windows Server 2022
VM3	Server Core installation of Windows Server 2022
VM4	Windows Server 2022 configured with an AppLocker policy

You are configuring Microsoft Defender for Servers.

You plan to enable adaptive application controls to create an allowlist of known-safe apps on the virtual machines.

Which virtual machines support the use of adaptive application controls?

- A.VM1 and VM2 only
- B.VM2 and VM4 only
- C.VM2 and VM3 only



**Answer: A****Explanation:**

Answer = A (VM1 and VM2 only)-Adaptive application controls help in defining an allowlist of known-safe applications for virtual machines.-Windows Server Core installations, like VM3, are not supported by this feature.-VM4 is configured with an AppLocker policy, which may conflict with adaptive application controls as they perform similar functions for application whitelisting. Thus, the answer will focus on the virtual machines that are neither Server Core nor use AppLocker. That would be VM1 (Windows Server 2019) and VM2 (Windows Server 2022). The correct answer is A. VM1 and VM2 only.

**Question: 434****CertyIQ**

You have an Azure subscription. The subscription contains a virtual network named VNet1 that contains the subnets shown in the following table.

Name	Associated network security group (NSG)
Subnet1	NSG1
Subnet2	NSG1
Subnet3	NSG1
Subnet4	NSG1

The subscription contains the function apps shown in the following table.

Name	Description
App1	Uses the Azure Functions Premium plan and has virtual network integration with VNet1/Subnet1
App2	Uses an App Service plan in the Basic pricing tier and has virtual network integration with VNet1/Subnet2
App3	Uses an App Service plan in the Premium pricing tier and has virtual network integration with VNet1/Subnet3
App4	Uses an App Service plan in the isolated pricing tier and is deployed to VNet1/Subnet4

The outbound traffic of which app is controlled by using NSG1?

- A.App4 only
- B.App3 and App4 only
- C.App2, App3, and App4 only
- D.App1, App2, App3, and App4

**Answer: D****Explanation:**

App1, App2, App3, and App4.

**Question: 435**

CertyIQ

You have a Microsoft Entra tenant named contoso.com.

You collaborate with a partner organization that has a Microsoft Entra tenant named fabrikam.com.

You need to create an allow list of cloud apps from fabrikam.com that can be used by the users in contoso.com.

What should you do for contoso.com in the Microsoft Entra admin center?

- A.From Inbound access settings in Cross-tenant access settings, configure the B2B direct connect settings.
- B.From External collaboration settings, configure the Collaboration restrictions settings.
- C.From External collaboration settings, configure the Guest invite settings.
- D.From Outbound access settings in Cross-tenant access settings, configure the B2B collaboration settings.

**Answer: A****Explanation:**

From Inbound access settings in Cross-tenant access settings, configure the B2B direct connect settings.

**Question: 436**

CertyIQ

HOTSPOT

-

You have an Azure subscription that contains the virtual networks shown in the following table.

Name	Description
VNet1	Contains two subnets named Subnet1 and Subnet2
VNet2	Contains one subnet named Subnet3 that has an associated network security group (NSG) named NSG1

NSG1 rules restrict access to the internet from Subnet3.

The subscription contains the function apps shown in the following table.

Name	Description
App1	Uses an App Service plan in the Premium pricing tier
App2	Uses an App Service plan in the Premium pricing tier and has virtual network integration with VNet2.

Virtual network integration has the default settings.

You need to configure network access for App1 and App2 to meet the following requirements:

- Deny inbound access to App1 from Subnet1 and allow inbound access from Subnet2.
- Deny outbound access from App2 to the internet.

What should you do for each requirement? To answer, select the appropriate options in the answer area.



NOTE: Each correct selection is worth one point.

Answer Area

Deny inbound access to App1 from Subnet1 and allow inbound access from Subnet2:

Configure a private endpoint for App1  
Configure access restrictions for App1  
Configure virtual network integration with VNet1 for App1

Deny outbound access from App2 to the internet:

Configure access restrictions for App2  
Deploy App2 to an App Service Environment  
Enable Route All for the App2 virtual network integration with VNet2

Answer:

Answer Area

Deny inbound access to App1 from Subnet1 and allow inbound access from Subnet2:

Configure a private endpoint for App1  
**Configure access restrictions for App1**  
Configure virtual network integration with VNet1 for App1

Deny outbound access from App2 to the internet:

Configure access restrictions for App2  
Deploy App2 to an App Service Environment  
**Enable Route All for the App2 virtual network integration with VNet2**

Question: 437

CertyIQ

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

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study. At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

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

Overview -

Litware, Inc. is a digital media company that has 500 employees in the Chicago area and 20 employees in the San Francisco area.

Existing Environment -

Litware has an Azure subscription named Sub1 that has a subscription ID of 43894a43-17c2-4a39-8cfc-3540c2653ef4.

Sub1 is associated to an Azure Active Directory (Azure AD) tenant named litwareinc.com. The tenant contains the

user objects and the device objects of all the Litware employees and their devices. Each user is assigned an Azure AD Premium P2 license. Azure AD Privileged Identity Management (PIM) is activated. The tenant contains the groups shown in the following table.

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.
Group2	Security group	A group that has the Dynamic User membership type and contains the Chicago IT team

The Azure subscription contains the objects shown in the following table.

Name	Type	Description
VNet1	Virtual network	VNet1 is a virtual network that contains security-sensitive IT resources. VNet1 contains three subnets named Subnet0, Subnet1, and AzureFirewallSubnet.
VM0	Virtual machine	VM0 is an Azure virtual machine that runs Windows Server 2016, connects to Subnet0, and has just in time (JIT) VM access configured.
VM1	Virtual machine	VM1 is an Azure virtual machine that runs Windows Server 2016 and connects to Subnet0.
SQLDB1	Azure SQL Database	SQLDB1 is an Azure SQL database on a SQL Database server named LitwareSQLServer1.
WebApp1	Web app	WebApp1 is an Azure web app that is accessible by using <a href="https://www.litwareinc.com">https://www.litwareinc.com</a> and <a href="http://www.litwareinc.com">http://www.litwareinc.com</a> .
RG1	Resource group	RG1 is a resource group that contains VNet1, VM0, and VM1.
RG2	Resource group	RG2 is a resource group that contains shared IT resources.

Azure Security Center is set to the Standard tier.

Requirements -

Planned Changes -

Litware plans to deploy the Azure resources shown in the following table.

Name	Type	Description
Firewall1	Azure Firewall	An Azure firewall on VNet1.
RT1	Route table	A route table that will contain a route pointing to Firewall1 as the default gateway and will be assigned to Subnet0.
AKS1	Azure Kubernetes Service (AKS)	A managed AKS cluster

Identity and Access Requirements

Litware identifies the following identity and access requirements:

- All San Francisco users and their devices must be members of Group1.
- The members of Group2 must be assigned the Contributor role to RG2 by using a permanent eligible assignment.
- Users must be prevented from registering applications in Azure AD and from consenting to applications that

access company information on the users' behalf.

#### Platform Protection Requirements

Litware identifies the following platform protection requirements:

Microsoft Antimalware must be installed on the virtual machines in RG1.

The members of Group2 must be assigned the Azure Kubernetes Service Cluster Admin Role.

Azure AD users must be able to authenticate to AKS1 by using their Azure AD credentials.

Following the implementation of the planned changes, the IT team must be able to connect to VM0 by using JIT VM access.

A new custom RBAC role named Role1 must be used to delegate the administration of the managed disks in RG1.

Role1 must be available only for RG1.

#### Security Operations Requirements

Litware must be able to customize the operating system security configurations in Azure Security Center.

#### Data and Application Requirements

Litware identifies the following data and applications requirements:

The users in Group2 must be able to authenticate to SQLDB1 by using their Azure AD credentials.

WebApp1 must enforce mutual authentication.

#### General Requirements -

Litware identifies the following general requirements:

Whenever possible, administrative effort must be minimized.

Whenever possible, use of automation must be maximized.

- Question 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 group type of Microsoft 365. Add users and devices to the group.

C. Modify the membership rule of Group1.

D. Change the membership type of Group1 to Assigned. Create two groups that have dynamic memberships. Add the new groups to Group1.

**Answer: D**

#### Explanation:

When you create dynamic groups, they can either contain users or devices. Hence here we need to create two separate dynamic groups and assign those groups to an Assigned group.

Incorrect Answers:

A, C: You can create a dynamic group for devices or users, but you can't create a rule that contains both users and devices.

Scenario:

Litware identifies the following identity and access requirements: All San Francisco users and their devices must be members of Group1.

The tenant currently contains 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.

Reference:

<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>



You need to ensure that the Azure AD application registration and consent configurations meet the identity and access requirements.  
What should you use in the Azure portal? To answer, select the appropriate options in the answer area.  
NOTE: Each correct selection is worth one point.  
Hot Area:

Answer Area

To configure the registration settings:

	▼
Azure AD – User settings	
Azure AD – App registrations settings	
Enterprise Applications – User settings	

To configure the consent settings:

	▼
Azure AD – User settings	
Azure AD – App registrations settings	
Enterprise Applications – User settings	

Answer:

Answer Area

To configure the registration settings:

	▼
Azure AD – User settings	
Azure AD – App registrations settings	
Enterprise Applications – User settings	

To configure the consent settings:

	▼
Azure AD – User settings	
Azure AD – App registrations settings	
Enterprise Applications – User settings	

Explanation:

Reference:  
<https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/configure-user-consent>

Question: 439

CertyIQ

HOTSPOT  
-

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

Name	Type	Location	In resource group
RG1	Resource group	East US	<i>Not applicable</i>
RG2	Resource group	West US	<i>Not applicable</i>
RG3	Resource group	Central US	<i>Not applicable</i>
VNet1	Virtual network	Central US	RG2

VNet1 contains the subnets shown in the following table.

Name	Description
AzureFirewall	Contains no resources
AzureFirewallSubnet	Contains no resources
Subnet1	Contains a virtual machine
Subnet2	Contains no resources

You plan to use the Azure portal to deploy an Azure firewall named AzFW1 to VNet1.

Which resource group and subnet can you use to deploy AzFW1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Resource group:

RG1  
RG2  
RG3

Subnet:

AzureFirewall only  
AzureFirewallSubnet only  
AzureFirewall or AzureFirewallSubnet only  
AzureFirewall, AzureFirewallSubnet, or Subnet2 only  
AzureFirewall, AzureFirewallSubnet, Subnet1, or Subnet2

Answer:

## Answer Area

Resource group:

▼

RG1

RG2

RG3

Subnet:

▼

AzureFirewall only

AzureFirewallSubnet only

AzureFirewall or AzureFirewallSubnet only

AzureFirewall, AzureFirewallSubnet, or Subnet2 only

AzureFirewall, AzureFirewallSubnet, Subnet1, or Subnet2

### Explanation:

Box 1: RG2

The firewall, VNet, and the public IP address all must be in the same resource group.

<https://learn.microsoft.com/en-us/azure/firewall/firewall-faq>

Box 2: AzureFirewallSubnet only

The subnet name must be AzureFirewallSubnet.

<https://learn.microsoft.com/en-us/azure/firewall/tutorial-firewall-deploy-portal>

### Question: 440

CertyIQ

You have an Azure subscription that contains a storage account named storage1 and a virtual machine named VM1.

VM1 is connected to a virtual network named VNet1 that contains one subnet and uses Azure DNS.

You need to ensure that VM1 connects to storage1 by using a private IP address. The solution must minimize administrative effort.

What should you do?

- A.For storage1, disable public network access.
- B.On VNet1, create a new subnet.
- C.For storage1, create a new private endpoint.
- D.Create an Azure Private DNS zone.

**Answer: C**

### Explanation:

C. For storage1, create a new private endpoint



**Question: 441**

You have an Azure subscription that contains a web app named App1. App1 provides users with product images and videos. Users access App1 by using a URL of HTTPS://app1.contoso.com.

You deploy two server pools named Pool1 and Pool2. Pool1 hosts product images. Pool2 hosts product videos.

You need to optimize the performance of App1. The solution must meet the following requirements:

- Minimize the performance impact of TLS connections on Pool1 and Pool2.
- Route user requests to the server pools based on the requested URL path.

What should you include in the solution?

- A.Azure Bastion
- B.Azure Front Door
- C.Azure Traffic Manager
- D.Azure Application Gateway

**Answer: B**

**Explanation:**

B. Azure Front Door

By using Azure Front Door, you can configure routing rules to direct requests for product images to Pool1 and requests for product videos to Pool2. This ensures that user requests are directed to the appropriate server pool based on the requested URL path.

**Question: 442**

HOTSPOT

-

You have an Azure subscription that is linked to an Azure AD tenant and contains the virtual machines shown in the following table.

Name	Connected to	Private IP address	Public IP address
VM1	VNet1/Subnet1	10.1.1.5	20.224.219.170
VM2	VNet1/Subnet2	10.1.2.5	20.224.219.230
VM3	VNet2/Subnet1	10.11.1.5	40.122.155.212

The subnets of the virtual networks have the service endpoints shown in the following table.

Subnet	Service endpoint
VNET1/Subnet1	Microsoft.Storage
VNET1/Subnet2	Microsoft.KeyVault
VNET2/Subnet1	Microsoft.Storage, Microsoft.KeyVault

You create the resources shown in the following table.

Name	Type
storage1	Azure Storage account
Vault1	Azure Key Vault

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

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
Connections from VM1 to storage1 always use IP address 10.1.1.5.	<input type="radio"/>	<input type="radio"/>
Connections from VM2 to Vault1 always use IP address 20.224.219.230.	<input type="radio"/>	<input type="radio"/>
Authentication from VM3 to the tenant uses either IP address 10.11.1.5 or 40.122.155.212.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
Connections from VM1 to storage1 always use IP address 10.1.1.5.	<input checked="" type="radio"/>	<input type="radio"/>
Connections from VM2 to Vault1 always use IP address 20.224.219.230.	<input type="radio"/>	<input checked="" type="radio"/>
Authentication from VM3 to the tenant uses either IP address 10.11.1.5 or 40.122.155.212.	<input type="radio"/>	<input checked="" type="radio"/>

Explanation:

- yes
- no
- no

You need to identify whether you can use the following features with AzFW1:

- TLS inspection
- Threat intelligence
- The network intrusion detection and prevention systems (IDPS)

What can you use?

- A.TLS inspection only
- B.threat intelligence only
- C.TLS inspection and the IDPS only
- D.threat intelligence and the IDPS only
- E.TLS inspection, threat intelligence, and the IDPS

**Answer: B**

**Explanation:**

Azure Firewall Standard includes the following features: Built-in high availability Availability Zones Unrestricted cloud scalability Application FQDN filtering rules Network traffic filtering rules FQDN tags Service tags Threat intelligence DNS proxy Custom DNS FQDN in network rules Deployment without public IP address in Forced Tunnel Mode Outbound SNAT support Inbound DNAT support Multiple public IP addresses Azure Monitor logging Forced tunneling Web categories Certifications

## Question: 444

CertyIQ

SIMULATION

-

Use the following login credentials as needed:

To enter your username, place your cursor in the Sign in box and click on the username below.

To enter your password, place your cursor in the Enter password box and click on the password below.

Azure Username: [email protected]

Azure Password: Gp0Ae4@!Dg

-

If the Azure portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.

The following information is for technical support purposes only:

Lab Instance: 28681041

-

You need to configure Azure to allow RDP connections from the Internet to a virtual machine named VM1. The solution must minimize the attack surface of VM1.

To complete this task, sign in to the Azure portal.

**Answer:**

Cannot connect remotely to a VM because RDP port is not enabled in NSG

#### Symptom

You cannot make an RDP connection to a VM in Azure because the RDP port is not opened in the network security group.

#### Solution

When you create a new VM, all traffic from the Internet is blocked by default.

To enable the RDP port in an NSG, follow these steps:

Step 1: Sign in to the Azure portal.

Step 2: In Virtual Machines, select the VM that has the problem.

Step 3: In Settings, select Networking.

Step 4: In Inbound port rules, check whether the port for RDP is set correctly. The following is an example of the configuration:

Priority: 300

Name: Port\_3389

Port(Destination): 3389

Protocol: TCP

Source: Any

Destinations: Any

Action: Allow

If you specify the source IP address, this setting allows traffic only from a specific IP address or range of IP addresses to connect to the VM. Make sure that the computer you are using to start the RDP session is within the range.

Incorrect:

\* Create an RDP connection to a Windows VM using Azure Bastion.

Need to allow an RDP connection, not try to create a RDP connection.

Reference:

<https://learn.microsoft.com/en-us/azure/bastion/bastion-connect-vm-rdp-windows>

## Question: 445

CertyIQ

### SIMULATION

-

You need to ensure that only devices connected to a 131.107.0.0/16 subnet can access data in the rg1lod28681041 Azure Storage account.

To complete this task, sign in to the Azure portal.

### Answer:

Grant access from a virtual network.

You can configure storage accounts to allow access only from specific subnets. The allowed subnets can belong to a virtual network in the same subscription or a different subscription, including those that belong to a different Azure AD tenant.

You can enable a service endpoint for Azure Storage within the virtual network. The service endpoint routes traffic from the virtual network through an optimal path to the Azure Storage service. The identities of the subnet and the virtual network are also transmitted with each request. Administrators can then configure network rules for the storage account that allow requests to be received from specific subnets in a virtual network. Clients granted access via these network rules must continue to meet the authorization requirements of the storage account to access the data.

Step 1: Go to the storage account that you want to secure.

Step 2: Select Networking.

Step 3: Check that you've chosen to allow access from Selected networks.

Step 4: To grant access to a virtual network by using a new network rule, under Virtual networks, select Add existing virtual network. Select the Virtual networks and Subnets options, and then select Add.

In our case specify the 131.107.0.0/16 subnet.

If a service endpoint for Azure Storage wasn't previously configured for the selected virtual network and subnets, you can configure it as part of this operation.

Create a service endpoint policy

1. Select + Create a resource on the upper, left corner of the Azure portal.
2. In search pane, type "service endpoint policy" and select Service endpoint policy and then select Create.

[Dashboard](#) > [New](#) > Service endpoint policy

## Service endpoint policy

Microsoft

[Save for later](#)

[Create](#)

[Overview](#) [Plans](#)

Virtual Network (VNet) service endpoints extend your virtual network private address space and the identity of your VNet to the Azure services, over a direct connection. Endpoints allow you to secure your critical Azure service resources to only your virtual networks. Traffic from your VNet to the Azure service always remains on the Microsoft Azure backbone network. VNet service endpoint policies provide granular access control to specific service resources over the direct connection of service endpoints. Combined with NSG service tags, this capability provides an additional layer of security for virtual networks, allowing you to connect your VNets securely to access only specific service resources. Currently, you can restrict access to specific Azure storage accounts. Create a service endpoint policy and define the storage accounts that the policy should allow. You can then associate the policy to one or more subnets that have service endpoints associated with Azure Storage.

Useful Links  
[Documentation](#)

3. Enter, or select, the following information in Basics

\* Details omitted\*

4. Select + Add under Resources and enter or select the following information in Add a resource pane

Service: Only Microsoft.Storage is available with Service Endpoint Policies

Scope: Select one out of Single Account, All accounts in subscription and All accounts in resource group

Subscription: Select your subscription for storage account. Policy and storage accounts can be in different subscriptions.

Resource group: Select your resource group. Required, if scope is set as, "All accounts in resource group" or "Single account".

Resource: Select your Azure Storage resource under the selected Subscription or Resource Group

Click on Add button at bottom to finish adding the resource

[Home](#) > [Resource groups](#) > [MySEP-RG](#) > [New](#) > Service endpoint policy

### Create a service endpoint policy

[Basics](#) [Policy definitions](#) [Tags](#) [Review + create](#)

This policy will allow access only to the azure service resources listed

**Resources**  
[+ Add a resource](#)

Service	Allowed Resources	Resource Group
Add a resource to get started		

#### Add a resource

Service \*  
Microsoft.Storage

Scope \*  
Single account

Subscription \*

Resource group \*  
MySEP-RG

Resource \*  
myteststgacc123

[Review + create](#) [< Previous](#) [Next : Tags >](#) [Do not save](#) [Add](#)

5. Select Associated subnets to view the subnets the policy is associated. If no subnet is associated yet, follow the instructions in the next step.

[Home](#) > [MySEP-RG](#) > MySEP - Policy definitions

### MySEP - Policy definitions

[Service endpoint policy](#)

[Save](#) [Discard](#) [+ Add](#) [Refresh](#)

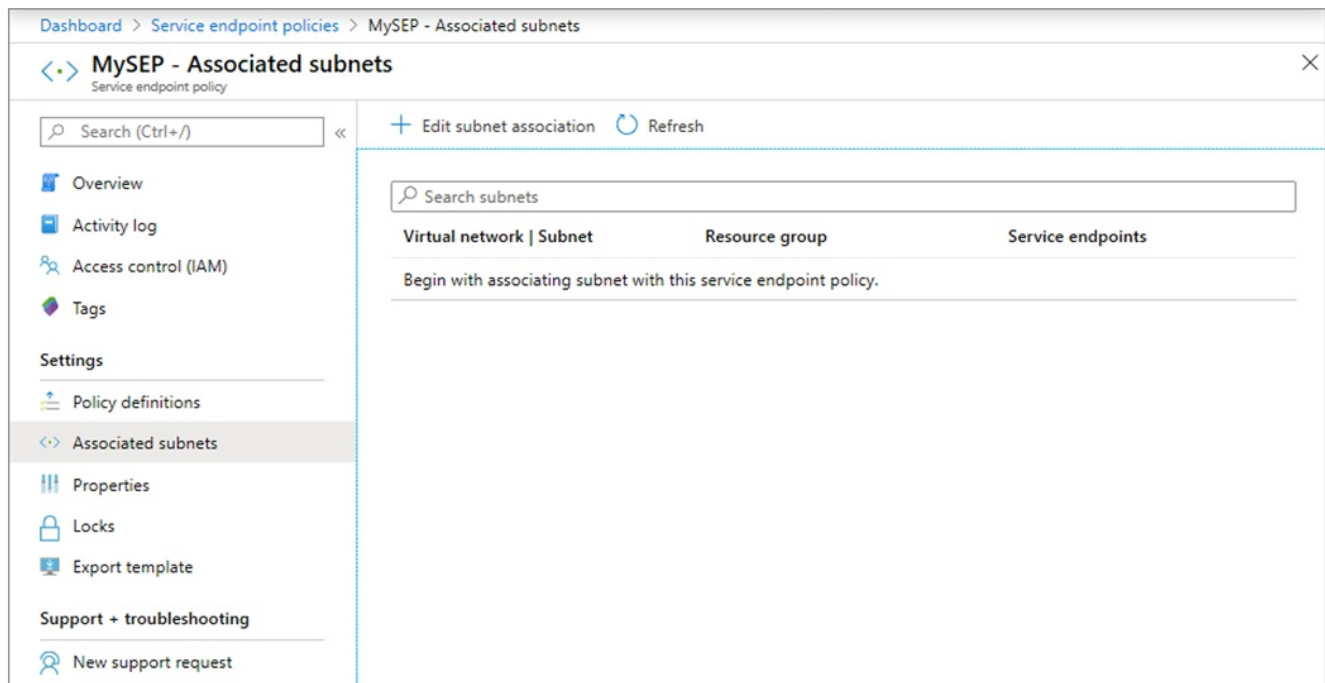
[Overview](#)  
[Activity log](#)  
[Access control \(IAM\)](#)  
[Tags](#)  
[Settings](#)

Service	Allowed Resources	Resource Group	Subscription name	Subscription ID
Microsoft.Storage				
Microsoft.Storage	myteststgacc123 (Sto...	MySEP-RG		

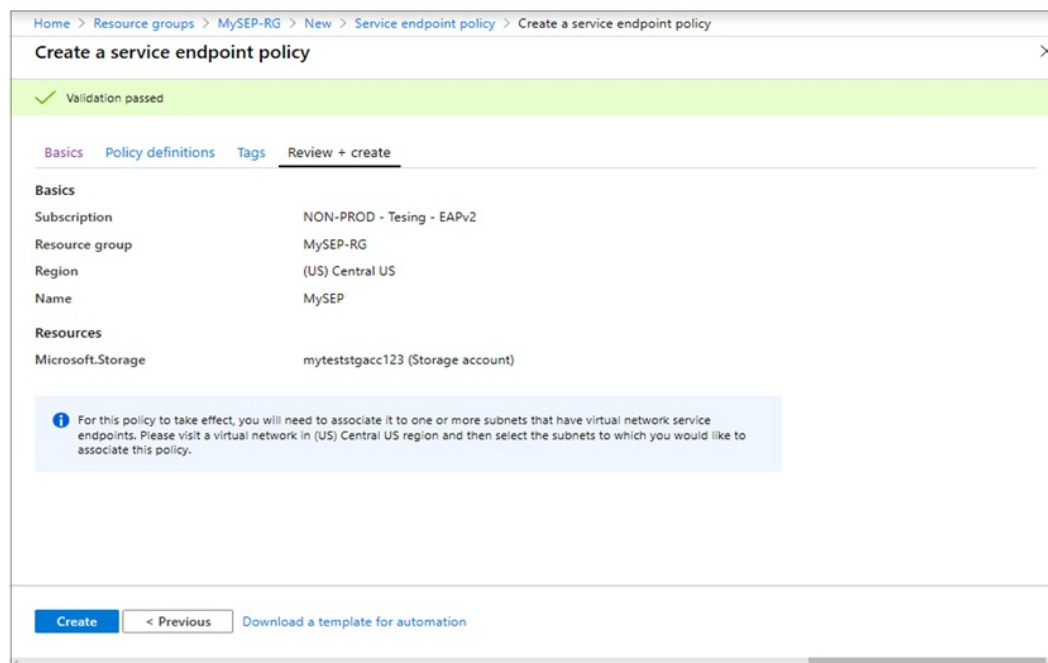




6. Select Associated subnets to view the subnets the policy is associated. If no subnet is associated yet, follow the instructions in the next step.
7. Associate a policy to a subnet



8. Select Review + Create. Validate the information and Click Create. To make further edits, click Previous.





in the following table.

Name	Description
storage1	A storage account
storage2	A storage account
KeyVault1	An Azure key vault
VNet1	A virtual network containing a single subnet that has five virtual machines connected
VNet2	A virtual network containing a single subnet that has three virtual machines connected

You need to configure virtual network service endpoints for VNet1 and VNet2. The solution must meet the following requirements:

- The virtual machines that connect to the subnet of VNet1 must access storage1, storage2, and Azure AD by using the Microsoft backbone network.
- The virtual machines that connect to the subnet of VNet2 must access storage1 and KeyVault1 by using the Microsoft backbone network.
- The virtual machines must use the Microsoft backbone network to communicate between VNet1 and VNet2.

How many service endpoints should you configure for each virtual network? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

VNet1: 

▼

1

2

3

5

VNet2: 

▼

1

2

3

5

Answer:

## Answer Area

VNet1:

VNet2:

### Explanation:

VNet1: 1 VNet2: 2

### Question: 447

CertyIQ

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

Name	Type
LB1	Azure Standard Load Balancer
VM1	Virtual machine
SQL1	Azure SQL Database
VMSS1	Virtual machine scale set

You plan to deploy an Azure Private Link service named APL1.

Which resource should you reference during the creation of APL1.

- A.LB1
- B.SQL1
- C.VMSS1
- D.VM1

### Answer: A

### Explanation:

The correct answer is A: LB1. Create a Private Link service behind the load balancer you created in the previous section.<https://learn.microsoft.com/en-us/azure/private-link/create-private-link-service-portal?tabs=dynamic-ip>

## Question: 448

DRAG DROP

-

You have an on-premises datacenter.

You have an Azure subscription that contains a virtual machine named VM1. VM1 is connected to a virtual network named VNet1. VNet1 is connected to the on-premises datacenter by using a Site-to-Site (S2S) VPN.

You plan to create an Azure storage account named storage1 and deploy an Azure web app named App1.

You need to ensure that network communication to each resource meets the following requirements:

- Connections to App1 must be allowed only from corporate network NAT addresses.
- Connections from VNet1 to storage1 must use the Microsoft backbone network.
- The solution must minimize costs.

What should you configure for each resource? To answer, drag the appropriate components to the correct resources. Each component may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

### Components

A private endpoint

A service endpoint

An access restriction rule

Azure Private Link

### Answer Area

storage1:

Component

App1:

Component

Answer:

### Answer Area

storage1:

A private endpoint

App1:

Azure Private Link

Explanation:

storage1: Private endpoint App1: Private link

<https://learn.microsoft.com/en-us/azure/storage/common/storage-private-endpoints>

**Question: 449**

You have an Azure subscription that contains the subnets shown in the following table.

Name	Virtual network	Location
Subnet11	VNet1	West US
Subnet12	VNet1	West US
Subnet21	VNet2	West US

The subscription contains an Azure web app named WebApp1 that has the following configurations:

- Region: West US
- Virtual network: VNet1
- VNet integration: Enabled
- Outbound subnet: Subnet11
- Windows plan (West US): ASP1

You plan to deploy an Azure web app named WebApp2 that will have the following settings:

- Region: West US
- VNet integration: Enabled
- Windows plan (West US): ASP1

To which subnets can you integrate WebApp2?

- A.Subnet11 only
- B.Subnet12 only
- C.Subnet11 or Subnet12 only
- D.Subnet12 or Subnet21 only
- E.Subnet11, Subnet12, or Subnet21

**Answer: D**

**Explanation:**

Correct answer is D. Subnet12 or Subnet21 only.

<https://learn.microsoft.com/en-us/azure/app-service/overview-vnet-integration>

**Question: 450**

You have an Azure subscription.

You need to deploy an Azure virtual WAN to meet the following requirements:

- Create three secured virtual hubs located in the East US, West US, and North Europe Azure regions.
- Ensure that security rules sync between the regions.

What should you use?

- A.Azure Virtual Network Manager
- B.Azure Front Door

- C.Azure Network Function Manager
- D.Azure Firewall Manager

Answer: A

Explanation:

1. <https://azure.microsoft.com/en-us/products/virtual-network-manager>

Question: 451

CertyIQ

HOTSPOT

-

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

Name	Description
storage1	General-purpose v2 storage account
SQL1	Azure SQL Managed Instance
VNet1	Virtual network
VM1	Virtual machine on VNet1

VNet1 connects to a remote site by using a Site-to-Site (S2S) VPN that uses forced tunneling.

VNet1 contains the subnets shown in the following table.

Name	CIDR	Network security group (NSG)
Default	10.1.0.0/24	None
GatewaySubnet	10.1.1.0/27	None
SQL	10.1.1.32/26	NSG1

The SQL subnet contains SQL1.

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

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
To restrict inbound traffic to SQL1, you must modify an access rule in NSG1.	<input type="radio"/>	<input type="radio"/>
To enable VM1 to access storage1 by using the Microsoft backbone network, you must enable a service endpoint on the Default subnet.	<input type="radio"/>	<input type="radio"/>
You can deploy an App Service Environment to the Default subnet.	<input type="radio"/>	<input type="radio"/>

Answer:

### Answer Area

#### Statements

To restrict inbound traffic to SQL1, you must modify an access rule in NSG1.

Yes

☒

No

☐

To enable VM1 to access storage1 by using the Microsoft backbone network, you must enable a service endpoint on the Default subnet.

☐

☒

You can deploy an App Service Environment to the Default subnet.

☒☐

#### Explanation:

YES

NO

YES

### Question: 452

CertyIQ

You have an Azure subscription that contains an Azure web app named App1 and a virtual machine named VM1. VM1 runs Microsoft SQL Server and is connected to a virtual network named VNet1. App1, VM1, and VNet1 are in the US Central Azure region.

You need to ensure that App1 can connect to VM1. The solution must minimize costs.

What should you include in the solution?

- A.regional virtual network integration
- B.gateway-required virtual network integration
- C.Azure Front Door
- D.Azure Application Gateway integration
- E.NAT gateway integration

#### Answer: A

#### Explanation:

Correct answer: A. regional virtual network integration  
<https://connectedcircuits.blog/2020/04/23/connecting-an-azure-webapp-to-a-sql-server-vm-inside-a-vnet/>

### Question: 453

CertyIQ

HOTSPOT

-

You have an Azure subscription that contains the virtual networks shown in the following table.



Name	Location	Peered with
VNet1	East US	VNet2
VNet2	West US	VNet1

The subscription contains the subnets shown in the following table.

Name	IP address space	Virtual network	Description
Subnet11	10.1.1.0/24	VNet1	Contains a virtual machine named VM1
Subnet12	172.16.1.0/27	VNet1	Contains no resources
Subnet21	192.168.10.0/24	VNet2	Contains an integrated Azure web app named WebApp1

You plan to create an Azure web app named WebApp2 that will have the following configurations:

- Region: East US
- VNet integration: Enabled
- Scale out: Autoscale to up to 10 instances

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

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
WebApp2 can be integrated with Subnet11.	<input type="radio"/>	<input type="radio"/>
WebApp2 can be integrated with Subnet12.	<input type="radio"/>	<input type="radio"/>
WebApp2 can be integrated with Subnet21.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
WebApp2 can be integrated with Subnet11.	<input type="radio"/>	<input checked="" type="radio"/>
WebApp2 can be integrated with Subnet12.	<input checked="" type="radio"/>	<input type="radio"/>
WebApp2 can be integrated with Subnet21.	<input type="radio"/>	<input checked="" type="radio"/>

### Question: 454

CertyIQ

DRAG DROP

You have an Azure subscription.

You plan to implement Azure DDoS Protection. The solution must meet the following requirements:

- Provide access to DDoS rapid response support during active attacks.
- Protect Basic SKU public IP addresses.

You need to recommend which type of DDoS Protection to use for each requirement.

What should you recommend? To answer, drag the appropriate DDoS Protection types to the correct requirements. Each DDoS Protection type may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

#### DDoS Protection types

DDoS infrastructure protection

DDoS IP Protection

DDoS Network Protection

#### Answer Area

Provide access to DDoS rapid response support during active attacks:

DDoS Protection type

Protect Basic SKU public IP addresses:

DDoS Protection type

#### Answer:

##### DDoS Protection types

DDoS infrastructure protection

DDoS IP Protection

DDoS Network Protection

##### Answer Area

Provide access to DDoS rapid response support during active attacks:

DDoS Network Protection

Protect Basic SKU public IP addresses:

DDoS Network Protection

#### Explanation:

1 DDOS network protection2: DDOS network protection

<https://learn.microsoft.com/en-us/azure/ddos-protection/ddos-protection-sku-comparison>

### Question: 455

CertyIQ

You have an Azure subscription that contains a virtual network named VNet1. VNet1 contains a single subnet. The subscription contains a virtual machine named VM1 that is connected to VNet1.

You plan to deploy an Azure SQL managed instance named SQL1.

You need to ensure that VM1 can access SQL1.

Which three components should you create? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A.a subnet
- B.a network security perimeter
- C.a virtual network gateway
- D.a network security group (NSG)
- E.a route table

**Answer: ADE**

**Explanation:**

A. a subnet.

D.a network security group (NSG).

E.a route table.

### Question: 456

CertyIQ

HOTSPOT

-

You are implementing an Azure Application Gateway web application firewall (WAF) named WAF1.

You have the following Bicep code snippet.

```

resource AppGW_AppFW_Pol
'Microsoft.Network/ApplicationGatewayWebApplicationFirewallPolicies@2021-08-01' = {
    name: AppGW_AppFW_Pol_name
    location: location
    properties: {
        customRules: [
            {
                name: 'CustRule01'
                priority: 100
                ruleType: 'MatchRule'
                action: 'Block'
                matchConditions: [
                    {
                        matchVariables: [
                            {
                                variableName: 'RemoteAddr'
                            }
                        ]
                        operator: 'IPMatch'
                        negationCondition: true
                        matchValues: [
                            '10.10.10.0/24'
                        ]
                    }
                ]
            }
        ]
    }
}

policySettings: {
    requestBodyCheck: true
    maxRequestBodySizeInKb: 128
    state: 'Enabaled'
    mode: 'Detection'
}
managedRules: {
    managedRuleSets: [
        {
            ruleSetType: 'OWASP'
            ruleSetVersion: '3.2'
        }
    ]
}
}

```

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

NOTE: Each correct selection is worth one point.

## Answer Area

Statements	Yes	No
A request to the backend pool from IP address 10.1.1.5 is allowed.	<input type="radio"/>	<input type="radio"/>
Incoming requests attempting file path attacks are blocked.	<input type="radio"/>	<input type="radio"/>
WAF1 allows a 50-MB file to be uploaded.	<input type="radio"/>	<input type="radio"/>

Answer:

### Answer Area

Statements	Yes	No
A request to the backend pool from IP address 10.1.1.5 is allowed.	<input checked="" type="radio"/>	<input type="radio"/>
Incoming requests attempting file path attacks are blocked.	<input type="radio"/>	<input checked="" type="radio"/>
WAF1 allows a 50-MB file to be uploaded.	<input checked="" type="radio"/>	<input type="radio"/>

Explanation:

YNY .WAF is in Detection mode, which means it won't take any action. <https://learn.microsoft.com/en-us/azure/web-application-firewall/cdn/cdn-overview#waf-modes>As far as the file upload limit, I only found 1 article indicating the limit is 2GB. <https://learn.microsoft.com/en-us/azure/web-application-firewall/ag/waf-engine>

### Question: 457

CertyIQ

HOTSPOT

-

You have an Azure subscription that contains the virtual networks shown in the following table.

Name	Subnet	Subnet-associated network security group (NSG)	Peered with
VNet1	Subnet1	NSG1	VNet2
VNet2	Subnet2	NSG2	VNet1

NSG1 and NSG2 both have default rules only.

The subscription contains the virtual machines shown in the following table.

Name	Connected to
VM1	Subnet1
VM2	Subnet2

The subscription contains the web apps shown in the following table.

Name	Description
WebApp1	Uses an App Service plan in the Premium pricing tier and has virtual network integration with VNet1.
WebApp2	Uses an App Service plan in the isolated pricing tier and is deployed to Subnet2.

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

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
WebApp1 can connect to VM2.	<input type="radio"/>	<input type="radio"/>
NSG1 controls inbound traffic to WebApp1.	<input type="radio"/>	<input type="radio"/>
WebApp2 can connect to VM1.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
WebApp1 can connect to VM2.	<input checked="" type="radio"/>	<input type="radio"/>
NSG1 controls inbound traffic to WebApp1.	<input type="radio"/>	<input checked="" type="radio"/>
WebApp2 can connect to VM1.	<input type="radio"/>	<input checked="" type="radio"/>

Explanation:



YNN.

VNET integration is for outbound traffic only, thus NSG won't apply here, at least not for inbound traffic.

"Virtual network integration gives your app access to resources in your virtual network, but it doesn't grant inbound private access to your app from the virtual network. "

<https://learn.microsoft.com/en-us/azure/azure-functions/functions-networking-options?tabs=azure-cli#virtual-network-integration>

### Question: 458

CertyIQ

DRAG DROP

You have an Azure subscription.





You create an Azure Firewall policy that has the rules shown in the following table.

Name	Type	Priority
Rule1	Application rule collection	100
Rule2	NAT rule collection	200
Rule3	Network rule collection	300
Rule4	NAT rule collection	400
Rule5	Network rule collection	500

In which order should the rules be processed? To answer, move all rules from the list of rules to the answer area and arrange them in the correct order.

#### Rules

#### Answer Area

Rule1		1	
Rule2		2	
Rule3		3	
Rule4		4	
Rule5		5	

Answer:

## Answer Area

1	Rule2
2	Rule4
3	Rule3
4	Rule5
5	Rule1

### Explanation:

Rule 2

Rule 4

Rule 3

Rule 5

Rule 1

### Question: 459

CertyIQ

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

Name	Type	Location
VNet1	Virtual network	West US
VNet2	Virtual network	East US
WebApp1	Web app	West US

You create an Azure DDoS Protection plan named DDoS1 in the West US Azure region.

Which resources can you add to DDoS1?

- A.VNet1only
- B.WebApp1 only
- C.VNet1 and VNet2 only
- D.VNet1 and WebApp1 only
- E.VNet1, VNet2, and WebApp1

**Answer: C**

**Explanation:**

Correct answer is C:VNet1 and VNet2 only.

### Question: 460

CertyIQ

DRAG DROP

-

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

Name	Type	Location
VM1	Virtual machine	East US
VNet1	Virtual network	East US
NSG1	Network security group (NSG)	East US
storage1	Storage account	West US

You need to configure network connectivity to meet the following requirements:

- Communication from VM1 to storage1 must traverse an optimized Microsoft backbone network.
- All the outbound traffic from VM1 to the internet must be denied.
- The solution must minimize costs and administrative effort.

What should you configure for VNet1 and NSG1? To answer, drag the appropriate components to the correct resources. Each component may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

## Components      Answer Area

A private endpoint

A route table

A service endpoint

A service tag

VNet1:

NSG1:

Answer:

## Components

## Answer Area

A private endpoint

A route table

A service endpoint

A service tag

VNet1:

A service endpoint

NSG1:

A service tag

### Explanation:

A Service endpoint.

A Service tag.

### Question: 461

CertyIQ

HOTSPOT

-

You have an Azure subscription that contains an Azure firewall named AzFW1. AzFW1 has a firewall policy named FWPolicy1.

You need to add rule collections to FWPolicy1 to meet the following requirements:

- Allow traffic based on the FQDN of the destination.
- Allow TCP traffic.

Which types of rule collections should you add for each requirement? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

## Answer Area

Allow traffic based on the destination FQDN:

Network only  
Application only  
Network or DNAT only  
Application or DNAT only  
Network or application only  
Network, application, or DNAT

Allow TCP traffic:

Network only  
Application only  
Network or DNAT only  
Application or DNAT only  
Network or application only  
Network, application, or DNAT

Answer:

## Answer Area

Allow traffic based on the destination FQDN:

Network only  
**Application only**  
Network or DNAT only  
Application or DNAT only  
Network or application only  
Network, application, or DNAT

Allow TCP traffic:

Network only  
Application only  
**Network or DNAT only**  
Application or DNAT only  
Network or application only  
Network, application, or DNAT

Explanation:

1. Application only.
2. Network or DNAT only.

**Question: 462**

HOTSPOT

-

You have an Azure subscription that contains the virtual networks shown in the following table.

Name	Location	Peered with
VNet1	East US	VNet2
VNet2	East US	VNet1, VNet3
VNet3	West US	VNet2

The subscription contains the virtual machines shown in the following table.

Name	Operating system	Connected to
VM1	Windows Server	VNet1
VM2	Linux	VNet2
VM3	Windows Server	VNet3

All the virtual machines have only private IP addresses.

You deploy Azure Bastion to VNet1 as shown in the following exhibit.



# Create a Bastion



Basics   Tags   Advanced   Review + create

Bastion allows web based RDP access to your vnet VM. [Learn more.](#)

## Project details

Subscription *	Azure subscription 1
Resource group *	RG1

[Create new](#)

## Instance details

Name *	Bastion1
Region *	East US
Tier * ⓘ	Basic
Instance count ⓘ	<input type="radio"/> 1 <input checked="" type="radio"/> 2

## Configure virtual networks

Virtual network * ⓘ	VNet1
Subnet *	AzureBastionSubnet (10.0.2.0/24)

[Create new](#)  
[Manage subnet configuration](#)

## Public IP address

Public IP address * ⓘ	<input checked="" type="radio"/> Create new <input type="radio"/> Use existing
Public IP address name *	VNet1-ip
Public IP address SKU	Standard
Assignment	<input type="radio"/> Dynamic <input checked="" type="radio"/> Static

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

NOTE: Each correct selection is worth one point.

Answer Area

Statements

- You can connect to VM1 through Bastion1 by using the Remote Desktop Connection client.
- You can connect to VM2 through Bastion1 by using SSH.
- You can connect to VM3 through Bastion1 by using the Azure portal.

Yes	No
<input type="radio"/>	<input type="radio"/>
<input type="radio"/>	<input type="radio"/>
<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements

- You can connect to VM1 through Bastion1 by using the Remote Desktop Connection client.
- You can connect to VM2 through Bastion1 by using SSH.
- You can connect to VM3 through Bastion1 by using the Azure portal.

Yes	No
<input checked="" type="radio"/>	<input type="radio"/>
<input checked="" type="radio"/>	<input type="radio"/>
<input checked="" type="radio"/>	<input type="radio"/>

Explanation:

- Yes
- Yes
- Yes

Question: 463

CertyIQ

HOTSPOT

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

Name	Type	Resource provider
VM1	Virtual machine	Microsoft.Compute
storage1	Storage account	Microsoft.Storage
WebApp1	Azure App Service web app	Microsoft.Web

You plan to use service endpoints and service endpoint policies.

Which resources can be accessed by using a service endpoint, and which resources support service endpoint policies? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

## Answer Area

Can be accessed by using a service endpoint:

storage1 and WebApp1 only  
VM1 and storage1 only  
VM1 and WebApp1 only  
VM1, storage1, and WebApp1 only

Support service endpoint policies:

storage1 only  
VM1 only  
WebApp1 only  
VM1 and storage1 only  
Storage1 and WebApp1 only

Answer:

### Answer Area

Can be accessed by using a service endpoint:

storage1 and WebApp1 only  
VM1 and storage1 only  
VM1 and WebApp1 only  
VM1, storage1, and WebApp1 only

Support service endpoint policies:

storage1 only  
VM1 only  
WebApp1 only  
VM1 and storage1 only  
Storage1 and WebApp1 only

## Question: 464

CertyIQ

HOTSPOT

-

You have an Azure App Service web app named App1 as shown in the following exhibit.



# Virtual Network Integration

ASP-demoapp8789577567336group-84d2

...

App Service Plan	ASP-demoapp8789577567336group-84d2
App Service Plan Location	East US
Regional VNet integrations	1/2
Gateway required VNet integrations	0/5
VNet NAME ↑↓	GATEWAY STATUS ↑↓
vnet1/subnet2	N/A

Subnet 2 contains a virtual machine named VM1.

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

NOTE: Each correct selection is worth one point.

## Answer Area

To deny outbound access, configure **[answer choice]** on Subnet2.

- a network security group (NSG)
- a service endpoint
- an application security group

To connect to a virtual network in a different region, configure **[answer choice]**.

- an Azure NAT Gateway integration
- Gateway-required VNet integrations
- Regional VNet integrations

Answer:

## Answer Area

To deny outbound access, configure **[answer choice]** on Subnet2.

- a network security group (NSG)
- a service endpoint
- an application security group

To connect to a virtual network in a different region, configure **[answer choice]**.

- an Azure NAT Gateway integration
- Gateway-required VNet integrations
- Regional VNet integrations









Question: 465

HOTSPOT

CertyIQ

You have an Azure subscription that contains a virtual machine named VM1.

You have a network security group (NSG) named NSG1 that is associated to the network interface of VM1 and is configured as shown in the following exhibit.

Priority <span>↑↓</span>	Name <span>↑↓</span>	Port <span>↑↓</span>	Protocol <span>↑↓</span>	Source <span>↑↓</span>	Destination <span>↑↓</span>	Action <span>↑↓</span>
Inbound Security Rules						
300	 RDP	3389	TCP	Any	Any	 Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	 Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	 Allow
65500	DenyAllInBound	Any	Any	Any	Any	 Deny
Outbound Security Rules						
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	 Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	 Allow
65500	DenyAllOutBound	Any	Any	Any	Any	 Deny

Just-in-time (JIT) VM access is enabled on VM1 and has the following configurations:

- Management ports: 3389, 22
- Maximum time range: 3 hours
- Allowed source IP addresses: Any

You activate the JIT rule and connect to VM1 by using SSH.

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

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
The RDP rule has priority over the NSG rule created by JIT.	<input type="radio"/>	<input type="radio"/>
If you disconnect from VM1 within the three-hour time range, you must reactivate the JIT rule to reconnect to VM1.	<input type="radio"/>	<input type="radio"/>
The SSH connection to VM1 disconnects automatically after three hours.	<input type="radio"/>	<input type="radio"/>

Answer:



## Answer Area

### Statements

Yes

No

The RDP rule has priority over the NSG rule created by JIT.

☒☐

If you disconnect from VM1 within the three-hour time range, you must reactivate the JIT rule to reconnect to VM1.

☐☒

The SSH connection to VM1 disconnects automatically after three hours.

☒☐

### Question: 466

CertyIQ

You have an on-premises network.

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

Name	Description
VNet1	Virtual network
ER1	ExpressRoute circuit that links the on-premises network to VNet1

You plan to deploy a Site-to-Site (S2S) VPN between the on-premises network and VNet1.

You need to recommend an Azure VPN Gateway SKU that meets the following requirements:

- Supports 1-Gbps throughput
- Minimizes costs

What should you recommend?

- A.VpnGw1
- B.VpnGw2
- C.VpnGw1AZ
- D.VpnGw2AZ

**Answer: B**

**Explanation:**

Correct answer is B: VpnGw2.

### Question: 467

CertyIQ

HOTSPOT

-

You have an Azure subscription that contains a virtual network named VNet1. VNet1 contains the subnets shown in the following table.



Name	IP address space
Subnet1	10.10.0.0/24
Subnet2	172.16.0.0/24
Subnet3	192.168.10.0/24

The subscription contains the virtual machines shown in the following table.

Name	Connected to
VM1	Subnet1
VM2	Subnet2
VM3	Subnet3

VM3 contains a service that listens for connections on port 8080.

For VM1, you configure just-in-time (JIT) VM access as shown in the following exhibit.

Home > Just-in-time VM access >

# JIT VM access configuration

VM1

+

 Add 

Save 

X

 Discard

Configure the ports for which the just-in-time VM access will be applicable

Port	Protocol	Allowed source IPs	IP range	Time range (hours)
3389	Any	CIDR	10.10.0.0/24,192.168.10.0/24	3 hours
8080	Any	Per request	N/A	5 hours

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

NOTE: Each correct selection is worth one point.

## Answer Area

Statements	Yes	No
You can establish a Remote Desktop connection from VM1 to VM3 for a maximum of three hours.	<input type="radio"/>	<input type="radio"/>
You can establish a Remote Desktop connection from VM2 to VM1 after requesting access.	<input type="radio"/>	<input type="radio"/>
You can establish a Remote Desktop connection from VM3 to VM1 without requesting access.	<input type="radio"/>	<input type="radio"/>

Answer:

## Answer Area

Statements	Yes	No
You can establish a Remote Desktop connection from VM1 to VM3 for a maximum of three hours.	<input type="radio"/>	<input checked="" type="radio"/>
You can establish a Remote Desktop connection from VM2 to VM1 after requesting access.	<input checked="" type="radio"/>	<input type="radio"/>
You can establish a Remote Desktop connection from VM3 to VM1 without requesting access.	<input checked="" type="radio"/>	<input type="radio"/>

### Question: 468

CertyIQ

You need to recommend which virtual machines to use to host App1. The solution must meet the technical requirements for KeyVault1.

Which virtual machines should you use?

- A. VM1 only
- B. VM1, VM2, VM3, and VM4
- C. VM1 and VM2 only
- D. VM1, VM2, and VM4 only

**Answer: B**

**Explanation:**

All VMs can access KV1 through private endpoint in VNET1/Subnet1. All VNETs are peered, so all the traffic traverse Microsoft backbone network without any exposure to public Internet.

The private endpoint can be reached from the same virtual network, regionally peered VNets, globally peered VNets and on premises using private VPN or ExpressRoute connections.

<https://docs.microsoft.com/en-us/azure/private-link/private-link-service-overview>

The traffic between virtual machines in peered virtual networks uses the Microsoft backbone infrastructure. Like traffic between virtual machines in the same network, traffic is routed through Microsoft's private network only.

<https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-peering-overview>

### Question: 469

CertyIQ

SIMULATION

-

You need to prevent HTTP connections to the rg1lod28681041n1 Azure Storage account.

To complete this task, sign in to the Azure portal.

## Answer:

Require secure transfer to ensure secure connections

You can configure your storage account to accept requests from secure connections only by setting the Secure transfer required property for the storage account. When you require secure transfer, any requests originating from an insecure connection are rejected. Microsoft recommends that you always require secure transfer for all of your storage accounts.

When secure transfer is required, a call to an Azure Storage REST API operation must be made over HTTPS. Any request made over HTTP is rejected.

Require secure transfer in the Azure portal

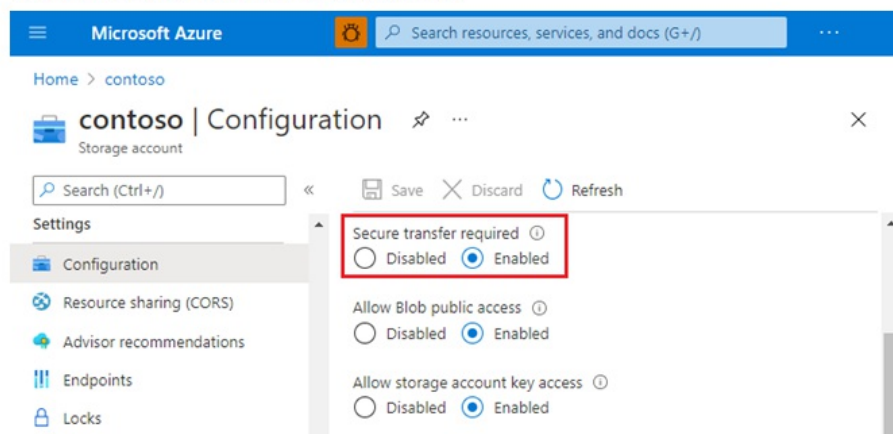
You can turn on the Secure transfer required property when you create a storage account in the Azure portal. You can also enable it for existing storage accounts.

Require secure transfer for an existing storage account

Step 1: Select an existing storage account (here: rg1lod28681041n1) in the Azure portal.

Step 2: In the storage account menu pane, under Settings, select Configuration.

Step 3: Under Secure transfer required, select Enabled.



Reference:

<https://learn.microsoft.com/en-us/azure/storage/common/storage-require-secure-transfer>

## Question: 470

CertyIQ

### SIMULATION

You need to ensure that the rg1lod28681041n1 Azure Storage account is encrypted by using a key stored in the KeyVault28681041 Azure key vault.

To complete this task, sign in to the Azure portal.

## Answer:

Configure customer-managed keys in the same tenant for an existing storage account

Azure Storage encrypts all data in a storage account at rest. By default, data is encrypted with Microsoft-managed keys. For additional control over encryption keys, you can manage your own keys. Customer-managed keys must be stored in Azure Key Vault or Key Vault Managed Hardware Security Model (HSM).

Configure encryption for manual updating of key versions

Step 1: In the Azure portal, navigate to the Storage accounts page, and select rg1lod28681041n1

Step 2: On the Encryption tab, indicate for which services you want to enable support for customer-managed keys in the Enable support for customer-managed keys field.

Step 3: In the Encryption type field, select Customer-managed keys (CMK).

Step 4: To locate the key URI in the Azure portal, navigate to your key vault, and select the Keys setting. Select the desired key, then select the key to view its versions. Select a key version to view the settings for that version.

Step 5: Copy the value of the Key Identifier field, which provides the URI.

413b17f8e2e14085950de59c584e32bc

## Properties

Key type	RSA
RSA key size	2048
Created	8/25/2022, 4:53:37 PM
Updated	8/25/2022, 4:53:37 PM
Key Identifier	<key-uri>
Settings	
Set activation date ⓘ	<input type="checkbox"/>
Set expiration date ⓘ	<input type="checkbox"/>
Enabled	<input checked="" type="radio"/> Yes <input type="radio"/> No
Tags	0 tags

## Permitted operations

- ☒ Encrypt
- ☒ Decrypt
- ☒ Sign
- ☒ Verify
- ☒ Wrap Key
- ☒ Unwrap Key

Step 6: In the Encryption key settings for your storage account, choose the Enter key URI option.

Step 7: Paste the URI that you copied into the Key URI field. Include the key version on the URI to configure manual updating of the key version.

Step 8: Specify a user-assigned managed identity by choosing the Select an identity link.

[Home](#) > [Storage accounts](#) >

## Create a storage account ...

Basics Advanced Networking Data protection Encryption Tags Review

Encryption type ⓘ \*

☐ Microsoft-managed keys (MMK)

☒ Customer-managed keys (CMK)

**i** This storage account will be granted access to the selected key vault. Both soft delete and purge protection will be enabled on the key vault and cannot be disabled.

Enable support for customer-managed keys ⓘ

☒ Blobs and files only

☐ All service types (blobs, files, tables, and queues)

**w** This option cannot be changed after this storage account is created.

**i** In order to use customer-managed keys, the following resources will need to have been created beforehand. If they have not been created, you will need to leave this experience to go do so.

- A user-assigned identity that has Get, Wrap key, and Unwrap key permissions on the same key vault. [Learn more](#)

Encryption key \*

☐ Select a key vault and key

☒ Enter key from URI

Key URI \*

<key-uri>

User-assigned identity ⓘ \*

sample-user-assigned-identity  
[Change](#)

Enable infrastructure encryption ⓘ

☐

[Review](#)

[< Previous](#)

[Next : Tags >](#)

Step 9: Select the Review button to validate

Reference:

<https://learn.microsoft.com/en-us/azure/storage/common/customer-managed-keys-configure-existing-account>



**Question: 471**

## HOTSPOT

You have an Azure subscription that contains the virtual machines shown in the following table.

Name	Connected to	Private IP address	Public IP address
VM1	VNET1/Subnet1	10.1.1.5	20.224.219.170
VM2	VNET1/Subnet2	10.1.2.5	20.224.219.230
VM3	VNET2/Subnet1	10.11.1.5	40.122.155.212

You have an Azure Cosmos DB account named cosmos1 configured as shown in the following exhibit.

Allow access from

☐ All networks ☒ Selected networks

Configure network security for your Azure Cosmos DB account. [Learn more.](#)

Virtual networks

Secure your Azure Cosmos DB account with virtual networks. [+ Add existing virtual network](#)  
[+ Add new virtual network](#)

Virtual Network	Subnet	Address range	Endpoint Status	Resource Group	Subscription
▼ vnet1	2	10.1.0.0/16		rg1	Azure Pass - Spons
	vnet1/subnet1	10.1.1.0/24	✓ Enabled	rg1	Azure Pass - Spons
	vnet1/subnet2	10.1.2.0/24	⚠ Disabled	rg1	Azure Pass - Spons

Firewall

Add IP ranges to allow access from the internet or your on-premises networks.

[+ Add my current IP \(20.224.219.170\)](#) ⓘ

IP (Single IPv4 or CIDR range)

<input type="text"/>	...
20.224.219.0/24	...
40.122.155.0/24	...

Exceptions

- ☐ Accept connections from within public Azure datacenters ⓘ  
☒ Allow access from Azure Portal ⓘ

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

NOTE: Each correct selection is worth one point.

## Answer Area

Statements	Yes	No
VM1 can access cosmos1 over the internet.	<input type="radio"/>	<input type="radio"/>
VM2 can access cosmos1 over the internet.	<input type="radio"/>	<input type="radio"/>
VM3 can access cosmos1 over the internet.	<input type="radio"/>	<input type="radio"/>

Answer:

## Answer Area

Statements	Yes	No
VM1 can access cosmos1 over the internet.	<input checked="" type="radio"/>	<input type="radio"/>
VM2 can access cosmos1 over the internet.	<input type="radio"/>	<input checked="" type="radio"/>
VM3 can access cosmos1 over the internet.	<input checked="" type="radio"/>	<input type="radio"/>

### Question: 472

CertyIQ

You are troubleshooting a security issue for an Azure Storage account.

You enable Azure Storage Analytics logs and archive it to a storage account.

What should you use to retrieve the diagnostics logs?

- A.Azure Cosmos DB explorer
- B.Azure Monitor
- C.AzCopy
- D.Microsoft Defender for Cloud

**Answer: C**

**Explanation:**

It's either Az-copy or Azure Storage Explorer. AzCopy is a command-line utility that you can use to copy blobs or files to or from a storage account

### Question: 473

CertyIQ



You have an Azure subscription that contains an Azure Blob storage account named blob1.

You need to configure attribute-based access control (ABAC) for blob1.

Which attributes can you use in access conditions?

- A.blob index tags only
- B.blob index tags and container names only
- C.file extensions and container names only
- D.blob index tags, file extensions, and container names

**Answer: B**

**Explanation:**

Correct answer: B. blob index tags and container names only

<https://learn.microsoft.com/en-us/azure/role-based-access-control/conditions-overview>

#### Question: 474

CertyIQ

You have an Azure subscription that contains a storage account and an Azure web app named App1.

App1 connects to an Azure Cosmos DB database named Cosmos1 that uses a private endpoint named Endpoint1. Endpoint1 has the default settings.

You need to validate the name resolution to Cosmos1.

Which DNS zone should you use?

- A.endpoint1.privatelink.documents.azure.com
- B.endpoint1.privatelink.blob.core.windows.net
- C.endpoint1.privatelink.azurewebsites.net
- D.endpoint1.privatelink.database.azure.com

**Answer: A**

**Explanation:**

Correct Answer: A. endpoint1.privatelink.documents.azure.com <https://learn.microsoft.com/en-us/azure/cosmos-db/how-to-configure-private-endpoints>

#### Question: 475

CertyIQ

HOTSPOT

-

You have an Azure subscription that contains the virtual networks shown in the following table.

Name	Subnet	Peered with
VNet1	Subnet11	VNet2
VNet2	Subnet21, Subnet22	VNet1

The subscription contains the virtual machines shown in the following table.

Name	Connected to
VM1	Subnet11
VM2	Subnet22

You have a storage account named contoso2024 that contains the following resources:

- A container named Container1 that contains a file named File1
- A file share named Share1 that contains a file named File2

You create a private endpoint for contoso2024 as shown in the following exhibit.

# Create a private endpoint ...

 Validation passed

- ✓ Basics
- ✓ Resource
- ✓ Virtual Network
- ✓ DNS
- ✓ Tags
- 6** Review + create

## Basics

Subscription	Azure Pass - Sponsorship
Resource group	RG1
Region	East US
Name	PE1
Network Interface Name	PE1-nic

## Resource

Subscription ID	-4700-afeb-80f3df1585fd (Azure Pass - Sponsorship)
Subscription	Azure Pass - Sponsorship
Resource group	RG1
Resource	contoso2024
Target sub-resource	blob

## Virtual Network

Virtual network resource group	RG1
Virtual network	VNet2
Subnet	Subnet21
Network Policies	Disabled
Application security groups	None

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

NOTE: Each correct selection is worth one point.

## Answer Area

Statements	Yes	No
From VM1, you can access File1 by using a private IP address.	<input type="radio"/>	<input type="radio"/>
From VM2, you can access File1 by using a private IP address.	<input type="radio"/>	<input type="radio"/>
From VM2, you can access File2 by using a private IP address.	<input type="radio"/>	<input type="radio"/>

**Answer:**

**Answer Area**

**Statements**

**Yes**

**No**

From VM1, you can access File1 by using a private IP address.

☒☐

From VM2, you can access File1 by using a private IP address.

☒☐

From VM2, you can access File2 by using a private IP address.

☐☒

**Explanation:**

Yes

Yes

No

**Question: 476**

**CertyIQ**

You have an Azure subscription that contains an Azure Kubernetes Service (AKS) cluster named AKS1.

You have an Azure container registry that stores container images that were deployed by using Azure DevOps Microsoft-hosted agents.

You need to ensure that administrators can access AKS1 only from specific networks. The solution must minimize administrative effort.

What should you configure for AKS1?

- A. authorized IP address ranges
- B. an Application Gateway Ingress Controller (AGIC)
- C. a private endpoint
- D. a private cluster

**Answer: A**

**Explanation:**

authorized IP address ranges.

**Question: 477**

**CertyIQ**

You have an Azure subscription that uses Microsoft Defender for Cloud. The subscription contains an instance of Azure Database for PostgreSQL.

You need to ensure that an email alert is triggered when a suspected brute force attack on the database is detected. The solution must minimize administrative effort.

What should you configure?

- A.the Azure Monitor activity log
- B.an Azure Monitor alert rule
- C.Microsoft Defender for open-source relational databases
- D.the PostgreSQL Audit extension (pgAudit)

**Answer: C**

**Explanation:**

Microsoft Defender for open-source relational databases.

### Question: 478

CertyIQ

HOTSPOT

-

Your company uses cloud-based resources from the following platforms:

- Azure
- Amazon Web Services (AWS)
- Google Cloud Platform (GCP)

You plan to implement Microsoft Defender for Cloud.

On which platforms can you use Defender for Cloud to protect containers and storage? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

## Answer Area

Containers:

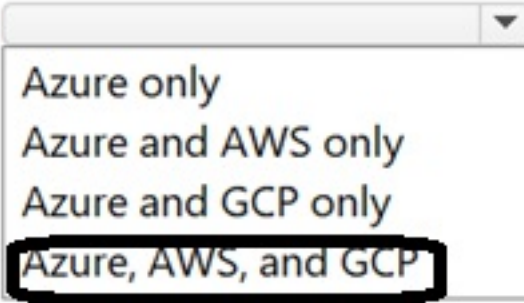
- Azure only
- Azure and AWS only
- Azure and GCP only
- Azure, AWS, and GCP

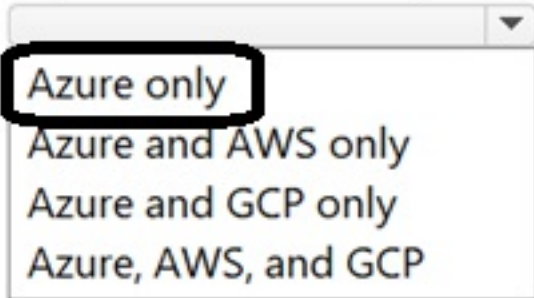
Storage:

- Azure only
- Azure and AWS only
- Azure and GCP only
- Azure, AWS, and GCP

**Answer:**

## Answer Area

Containers: 

Storage: 

### Explanation:

Containers: Azure, AWS, GCP <https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-containers-introduction> Microsoft Defender for Containers is a cloud-native solution to improve, monitor, and maintain the security of your containerized assets (Kubernetes clusters, Kubernetes nodes, Kubernetes workloads, container registries, container images and more), and their applications, across multicloud and on-premises environments.

Storage: Azure only <https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-storage-introduction>

### Question: 479

CertyIQ

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

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study. At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

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

Overview -

Litware, Inc. is a digital media company that has 500 employees in the Chicago area and 20 employees in the San Francisco area.

Existing Environment -

Litware has an Azure subscription named Sub1 that has a subscription ID of 43894a43-17c2-4a39-8cfc-3540c2653ef4.



Sub1 is associated to an Azure Active Directory (Azure AD) tenant named litwareinc.com. The tenant contains the user objects and the device objects of all the Litware employees and their devices. Each user is assigned an Azure AD Premium P2 license. Azure AD Privileged Identity Management (PIM) is activated. The tenant contains the groups shown in the following table.

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.
Group2	Security group	A group that has the Dynamic User membership type and contains the Chicago IT team

The Azure subscription contains the objects shown in the following table.

Name	Type	Description
VNet1	Virtual network	VNet1 is a virtual network that contains security-sensitive IT resources. VNet1 contains three subnets named Subnet0, Subnet1, and AzureFirewallSubnet.
VM0	Virtual machine	VM0 is an Azure virtual machine that runs Windows Server 2016, connects to Subnet0, and has just in time (JIT) VM access configured.
VM1	Virtual machine	VM1 is an Azure virtual machine that runs Windows Server 2016 and connects to Subnet0.
SQLDB1	Azure SQL Database	SQLDB1 is an Azure SQL database on a SQL Database server named LitwareSQLServer1.
WebApp1	Web app	WebApp1 is an Azure web app that is accessible by using https://www.litwareinc.com and http://www.litwareinc.com.
RG1	Resource group	RG1 is a resource group that contains VNet1, VM0, and VM1.
RG2	Resource group	RG2 is a resource group that contains shared IT resources.

Azure Security Center is set to the Standard tier.

Requirements -

Planned Changes -

Litware plans to deploy the Azure resources shown in the following table.

Name	Type	Description
Firewall1	Azure Firewall	An Azure firewall on VNet1.
RT1	Route table	A route table that will contain a route pointing to Firewall1 as the default gateway and will be assigned to Subnet0.
AKS1	Azure Kubernetes Service (AKS)	A managed AKS cluster

Identity and Access Requirements  
Litware identifies the following identity and access requirements:  
All San Francisco users and their devices must be members of Group1.  
The members of Group2 must be assigned the Contributor role to RG2 by using a permanent eligible assignment.

Users must be prevented from registering applications in Azure AD and from consenting to applications that access company information on the users' behalf.

#### Platform Protection Requirements

Litware identifies the following platform protection requirements:

- Microsoft Antimalware must be installed on the virtual machines in RG1.

The members of Group2 must be assigned the Azure Kubernetes Service Cluster Admin Role.

Azure AD users must be able to authenticate to AKS1 by using their Azure AD credentials.

Following the implementation of the planned changes, the IT team must be able to connect to VM0 by using JIT VM access.

A new custom RBAC role named Role1 must be used to delegate the administration of the managed disks in RG1.

Role1 must be available only for RG1.

#### Security Operations Requirements

Litware must be able to customize the operating system security configurations in Azure Security Center.

#### Data and Application Requirements

Litware identifies the following data and applications requirements:

The users in Group2 must be able to authenticate to SQLDB1 by using their Azure AD credentials.

WebApp1 must enforce mutual authentication.

#### General Requirements -

Litware identifies the following general requirements:

Whenever possible, administrative effort must be minimized.

Whenever possible, use of automation must be maximized.

- Question 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: BE**

#### Explanation:

B. Turn on the HTTPS Only protocol setting. (x) > To force 'mutual auth' you must turn off HTTP E. Turn on the Incoming client certificates protocol setting. (X) > must set it to 'Require'

### Question: 480

CertyIQ

#### 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" : [  

```

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

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

```
    ],  

```

```
  "NotActions": [  
    ],  
  "AssignableScopes": [  

```

	▼
"/	
"/subscriptions/43894a43-17c2-4a39-8cfc-3540c2653ef4/resourceGroups/RG1"	
"/subscriptions/43894a43-17c2-4a39-8cfc-3540c2653ef4	

```
    ]  

```

```
}
```

Answer:

## Answer Area

```
{  
  "Name": "Role1",  
  "Id": "11111111-1111-1111-1111-111111111111",  
  "IsCustom" : true,  
  "Description": "VM storage operator"  
  "Actions" : [  

```

	▼
Microsoft.Compute/	
Microsoft.Resources/	
Microsoft.Storage/	

	▼
disks/**,	
storageAccounts/**,	
virtualMachines/disks/**,	

],

```
  "NotActions": [  
    ],
```

```
  "AssignableScopes": [  

```

	▼
/*	
*/subscriptions/43894a43-17c2-4a39-8cfc-3540c2653ef4/resourceGroups/rg1*	
*/subscriptions/43894a43-17c2-4a39-8cfc-3540c2653ef4	

]

### Explanation:

1) Microsoft.Compute/

2) disks

3) /subscription/ subscriptionId /resourceGroups/ Resource Group Id

### Question: 481

CertyIQ

DRAG DROP -

You need to configure SQLDB1 to meet the data and application requirements.

Which three actions should you recommend be performed 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

## Answer Area

From the Azure portal, create a managed identity.

Connect to SQLDB1 by using Microsoft SQL Server Management Studio (SSMS).

In Azure AD, enable authentication method policy.

In SQLDB1, create contained database users.

From the Azure portal, create an Azure AD administrator for LitwareSQLServer1.



### Answer:

#### Actions

From the Azure portal, create a managed identity.

Connect to SQLDB1 by using Microsoft SQL Server Management Studio (SSMS).

In Azure AD, enable authentication method policy.

In SQLDB1, create contained database users.

From the Azure portal, create an Azure AD administrator for LitwareSQLServer1.

#### Answer Area

From the Azure portal, create an Azure AD administrator for LitwareSQLServer1.

In SQLDB1, create contained database users.

Connect to SQLDB1 by using Microsoft SQL Server Management Studio (SSMS).



### Explanation:

- 1) From the Azure Portal, create an Azure AD administrator for LitwareSQLServer1.
- 2) In SQLDB1, create contained database users.
- 3) Connect to SQLDB1 by using Microsoft SQL Server Management Studio.

## Question: 482

CertyIQ

### Introductory Info Case Study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided. To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

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

To start the case study -

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

Overview -

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.

Existing Environment -

Azure AD -

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
User9	Sydney	Owner

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.

User9 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	networkSecurityGroups	RG5
Not allowed resource types	virtualNetworks/virtualNetworkPeerings	RG6

Sub2 -

Sub2 contains the virtual networks shown in the following table.

Name	Subnet
VNetwork1	Subnet11, Subnet12, and Subnet13
VNetwork2	Subnet21

Sub2 contains the virtual machines shown in the following table.

Name	Network interface	Application security group	Connected to
VM1	NIC1	ASG1	Subnet11
VM2	NIC2	ASG2	Subnet11
VM3	NIC3	None	Subnet12
VM4	NIC4	ASG1	Subnet13
VM5	NIC5	None	Subnet21

All virtual machines have 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	Subnet11
NSG3	Subnet13
NSG4	Subnet21

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

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. Question You need to ensure that User2 can implement PIM.

What should you do first?

- A. Assign User2 the Global administrator role.
- B. Configure authentication methods for contoso.com.
- C. Configure the identity secure score for contoso.com.
- D. Enable multi-factor authentication (MFA) for User2.

**Answer: A**

**Explanation:**

To start using PIM in your directory, you must first enable PIM.

1. Sign in to the Azure portal as a Global Administrator of your directory.

You must be a Global Administrator with an organizational account (for example, @yourdomain.com), not a Microsoft account (for example, @outlook.com), to enable PIM for a directory.

Scenario: Technical requirements include: Enable Azure AD Privileged Identity Management (PIM) for

Reference:

<https://docs.microsoft.com/bs-latn-ba/azure/active-directory/privileged-identity-management/pim-getting-started>

**Question: 483**

**CertyIQ**

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

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study. At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

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

**General Overview -**

Fabrikam, Inc. is a consulting company that has a main office in Montreal and branch offices in Seattle and New York. Fabrikam has IT, human resources (HR), and finance departments.

**Existing Environment -**

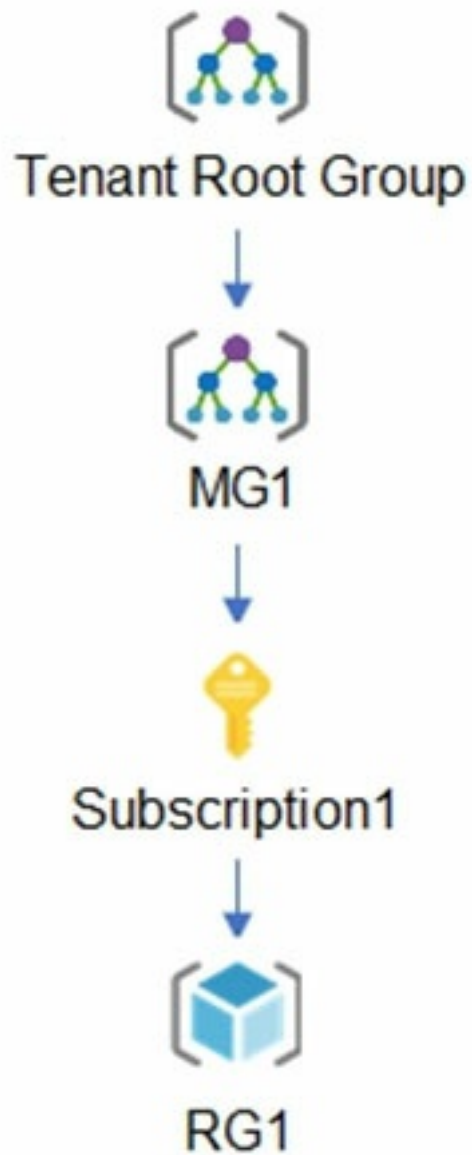
**Network Environment -**

Fabrikam has a Microsoft 365 subscription and an Azure subscription named subscription1.

The network contains an on-premises Active Directory domain named Fabrikam.com. The domain contains two organizational units (OUs) named OU1 and OU2.

Azure AD Connect cloud sync syncs only OU1.

The Azure resources hierarchy is shown in the following exhibit.



The Azure Active Directory (Azure AD) tenant contains the users shown in the following table.

Name	Type	Directory-synced	Role	Delegated to
User1	User	Yes	User	<b>None</b>
Admin1	User	No	User Access Administrator	Tenant Root Group
Admin2	User	No	Security administrator	MG1
Admin3	User	No	Contributor	Subscription1
Admin4	User	No	Owner	RG1
Group1	Group	No	<b>Not applicable</b>	<b>None</b>

Azure AD contains the resources shown in the following table.



Name	Type	Setting
CAPolicy1	Conditional access policy	Users in the finance department must use multi-factor authentication (MFA) when accessing Microsoft SharePoint Online
Sentinel1	Azure Sentinel workspace	<b>Not applicable</b>
SecPol1	Azure Policy definition	Security configuration for virtual machines

Subscription1 Resources -  
Subscription1 contains the virtual networks shown in the following table.

Name	Subnet	Location	Peer
VNET1	Subnet1, Subnet2	West US	VNET2, VNET3
VNET2	Subnet1	Central US	VNET1, VNET3
VNET3	Subnet1	West US	VNET1, VNET2

Subscription1 contains the network security groups (NSGs) shown in the following table.

Name	Location
NSG2	West US
NSG3	Central US
NSG4	West US

Subscription1 contains the virtual machines shown in the following table.

Name	Operating system	Location	Connected to	Associated NSG
VM1	Windows Server 2019	West US	VNET1/Subnet1	<b>None</b>
VM2	CentOS-based 8.2	West US	VNET1/Subnet2	NSG2
VM3	Windows Server 2016	Central US	VNET2/Subnet1	NSG3
VM4	Ubuntu Server 18.04 LTS	West US	VNET3/Subnet1	NSG4

Subscription1 contains the Azure key vaults shown in the following table.

Name	Location	Pricing tier	Private endpoint
KeyVault1	West US	Standard	VNET1/Subnet1
KeyVault2	Central US	Premium	<b>None</b>
KeyVault3	East US	Premium	VNET1/Subnet1, VNET2/Subnet1, VNET3/Subnet1

Subscription1 contains a storage account named storage1 in the West US Azure region.  
Planned Changes and Requirements

Planned Changes -  
Fabrikam plans to implement the following changes:  
Create two application security groups as shown in the following table.

Name	Location
ASG1	West US
ASG2	Central US

Associate the network interface of VM1 to ASG1.  
Deploy SecPol1 by using Microsoft Defender for Cloud.

Deploy a third-party app named App1. A version of App1 exists for all available operating systems.  
Create a resource group named RG2.  
Sync OU2 to Azure AD.  
Add User1 to Group1.

Technical Requirements -  
Fabrikam identifies the following technical requirements:  
The finance department users must reauthenticate after three hours when they access SharePoint Online.  
Storage1 must be encrypted by using customer-managed keys and automatic key rotation.  
From Sentinel1, you must ensure that the following notebooks can be launched:  
- Entity Explorer "" Account  
- Entity Explorer "" Windows Host  
- Guided Investigation Process Alerts  
VM1, VM2, and VM3 must be encrypted by using Azure Disk Encryption.  
Just in time (JIT) VM access for VM1, VM2, and VM3 must be enabled.  
App1 must use a secure connection string stored in KeyVault1.  
KeyVault1 traffic must NOT travel over the internet. Question DRAG DROP -  
You need to perform the planned changes for OU2 and User1.  
Which tools should you use? To answer, drag the appropriate tools to the correct resources. Each tool may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.  
NOTE: Each correct selection is worth one point.  
Select and Place:

**Tools**

The Azure portal

Azure AD Connect

The Active Directory admin center

Active Directory Sites and Services

Active Directory Users and Computers

**Answer Area**

OU2:

Tool

User1:

Tool

**Answer:**

**Tools**

The Active Directory admin center

Active Directory Sites and Services

Active Directory Users and Computers

**Answer Area**

OU2:

Azure AD Connect

User1:

The Azure portal

**Explanation:**

Azure ad connect

the azure portal



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

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study. At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

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

**General Overview -**

Fabrikam, Inc. is a consulting company that has a main office in Montreal and branch offices in Seattle and New York. Fabrikam has IT, human resources (HR), and finance departments.

**Existing Environment -**

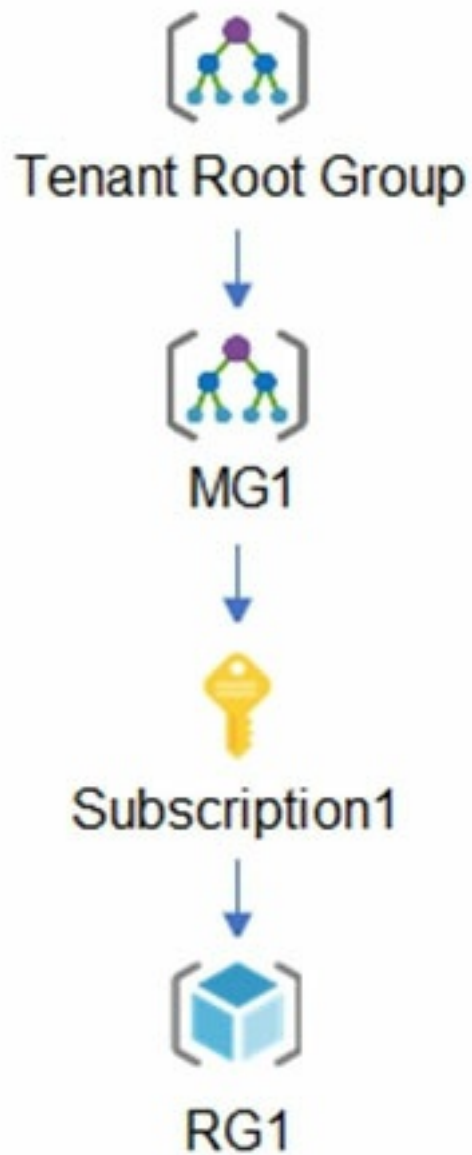
**Network Environment -**

Fabrikam has a Microsoft 365 subscription and an Azure subscription named subscription1.

The network contains an on-premises Active Directory domain named Fabrikam.com. The domain contains two organizational units (OUs) named OU1 and OU2.

Azure AD Connect cloud sync syncs only OU1.

The Azure resources hierarchy is shown in the following exhibit.



The Azure Active Directory (Azure AD) tenant contains the users shown in the following table.

Name	Type	Directory-synced	Role	Delegated to
User1	User	Yes	User	<b>None</b>
Admin1	User	No	User Access Administrator	Tenant Root Group
Admin2	User	No	Security administrator	MG1
Admin3	User	No	Contributor	Subscription1
Admin4	User	No	Owner	RG1
Group1	Group	No	<b>Not applicable</b>	<b>None</b>

Azure AD contains the resources shown in the following table.

Name	Type	Setting
CAPolicy1	Conditional access policy	Users in the finance department must use multi-factor authentication (MFA) when accessing Microsoft SharePoint Online
Sentinel1	Azure Sentinel workspace	<b>Not applicable</b>
SecPol1	Azure Policy definition	Security configuration for virtual machines

Subscription1 Resources -  
Subscription1 contains the virtual networks shown in the following table.

Name	Subnet	Location	Peer
VNET1	Subnet1, Subnet2	West US	VNET2, VNET3
VNET2	Subnet1	Central US	VNET1, VNET3
VNET3	Subnet1	West US	VNET1, VNET2

Subscription1 contains the network security groups (NSGs) shown in the following table.

Name	Location
NSG2	West US
NSG3	Central US
NSG4	West US

Subscription1 contains the virtual machines shown in the following table.

Name	Operating system	Location	Connected to	Associated NSG
VM1	Windows Server 2019	West US	VNET1/Subnet1	<b>None</b>
VM2	CentOS-based 8.2	West US	VNET1/Subnet2	NSG2
VM3	Windows Server 2016	Central US	VNET2/Subnet1	NSG3
VM4	Ubuntu Server 18.04 LTS	West US	VNET3/Subnet1	NSG4

Subscription1 contains the Azure key vaults shown in the following table.

Name	Location	Pricing tier	Private endpoint
KeyVault1	West US	Standard	VNET1/Subnet1
KeyVault2	Central US	Premium	<b>None</b>
KeyVault3	East US	Premium	VNET1/Subnet1, VNET2/Subnet1, VNET3/Subnet1

Subscription1 contains a storage account named storage1 in the West US Azure region.  
Planned Changes and Requirements

Planned Changes -  
Fabrikam plans to implement the following changes:  
Create two application security groups as shown in the following table.

Name	Location
ASG1	West US
ASG2	Central US

Associate the network interface of VM1 to ASG1.  
Deploy SecPol1 by using Microsoft Defender for Cloud.

Deploy a third-party app named App1. A version of App1 exists for all available operating systems.  
Create a resource group named RG2.  
Sync OU2 to Azure AD.  
Add User1 to Group1.

Technical Requirements -

Fabrikam identifies the following technical requirements:

The finance department users must reauthenticate after three hours when they access SharePoint Online.

Storage1 must be encrypted by using customer-managed keys and automatic key rotation.

From Sentinel1, you must ensure that the following notebooks can be launched:

- Entity Explorer "" Account
- Entity Explorer "" Windows Host
- Guided Investigation Process Alerts

VM1, VM2, and VM3 must be encrypted by using Azure Disk Encryption.

Just in time (JIT) VM access for VM1, VM2, and VM3 must be enabled.

App1 must use a secure connection string stored in KeyVault1.

KeyVault1 traffic must NOT travel over the internet. Question You need to meet the technical requirements for the finance department users.

Which CAPolicy1 settings should you modify?

- A. Cloud apps or actions
- B. Conditions
- C. Grant
- D. Session

**Answer: D**

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-session-lifetime>

## Question: 485

CertyIQ

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

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study. At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

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

General Overview -

Fabrikam, Inc. is a consulting company that has a main office in Montreal and branch offices in Seattle and New York. Fabrikam has IT, human resources (HR), and finance departments.

Existing Environment -

Network Environment -

Fabrikam has a Microsoft 365 subscription and an Azure subscription named subscription1.

The network contains an on-premises Active Directory domain named Fabrikam.com. The domain contains two organizational units (OUs) named OU1 and OU2. Azure AD Connect cloud sync syncs only OU1. The Azure resources hierarchy is shown in the following exhibit.



The Azure Active Directory (Azure AD) tenant contains the users shown in the following table.

Name	Type	Directory-synced	Role	Delegated to
User1	User	Yes	User	None
Admin1	User	No	User Access Administrator	Tenant Root Group
Admin2	User	No	Security administrator	MG1
Admin3	User	No	Contributor	Subscription1
Admin4	User	No	Owner	RG1
Group1	Group	No	Not applicable	None

Azure AD contains the resources shown in the following table.

Name	Type	Setting
CAPolicy1	Conditional access policy	Users in the finance department must use multi-factor authentication (MFA) when accessing Microsoft SharePoint Online
Sentinel1	Azure Sentinel workspace	<b>Not applicable</b>
SecPol1	Azure Policy definition	Security configuration for virtual machines

Subscription1 Resources -  
Subscription1 contains the virtual networks shown in the following table.

Name	Subnet	Location	Peer
VNET1	Subnet1, Subnet2	West US	VNET2, VNET3
VNET2	Subnet1	Central US	VNET1, VNET3
VNET3	Subnet1	West US	VNET1, VNET2

Subscription1 contains the network security groups (NSGs) shown in the following table.

Name	Location
NSG2	West US
NSG3	Central US
NSG4	West US

Subscription1 contains the virtual machines shown in the following table.

Name	Operating system	Location	Connected to	Associated NSG
VM1	Windows Server 2019	West US	VNET1/Subnet1	<b>None</b>
VM2	CentOS-based 8.2	West US	VNET1/Subnet2	NSG2
VM3	Windows Server 2016	Central US	VNET2/Subnet1	NSG3
VM4	Ubuntu Server 18.04 LTS	West US	VNET3/Subnet1	NSG4

Subscription1 contains the Azure key vaults shown in the following table.

Name	Location	Pricing tier	Private endpoint
KeyVault1	West US	Standard	VNET1/Subnet1
KeyVault2	Central US	Premium	<b>None</b>
KeyVault3	East US	Premium	VNET1/Subnet1, VNET2/Subnet1, VNET3/Subnet1

Subscription1 contains a storage account named storage1 in the West US Azure region.  
Planned Changes and Requirements

Planned Changes -  
Fabrikam plans to implement the following changes:  
Create two application security groups as shown in the following table.

Name	Location
ASG1	West US
ASG2	Central US

Associate the network interface of VM1 to ASG1.  
Deploy SecPol1 by using Microsoft Defender for Cloud.



Deploy a third-party app named App1. A version of App1 exists for all available operating systems.  
Create a resource group named RG2.  
Sync OU2 to Azure AD.  
Add User1 to Group1.

#### Technical Requirements -

Fabrikam identifies the following technical requirements:

The finance department users must reauthenticate after three hours when they access SharePoint Online.

Storage1 must be encrypted by using customer-managed keys and automatic key rotation.

From Sentinel1, you must ensure that the following notebooks can be launched:

- Entity Explorer "" Account
- Entity Explorer "" Windows Host
- Guided Investigation Process Alerts

VM1, VM2, and VM3 must be encrypted by using Azure Disk Encryption.

Just in time (JIT) VM access for VM1, VM2, and VM3 must be enabled.

App1 must use a secure connection string stored in KeyVault1.

KeyVault1 traffic must NOT travel over the internet.QuestionHOTSPOT -

You need to delegate the creation of RG2 and the management of permissions for RG1.

Which users can perform each task? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

#### Answer Area

Create RG2:

	▼
Admin3 only	
Admin2 and Admin3 only	
Admin3 and Admin4 only	
Admin2, Admin3, and Admin4 only	
Admin1, Admin2, Admin3, and Admin4	

Manage RG1 permissions:

	▼
Admin4 only	
Admin1 and Admin4 only	
Admin3 and Admin4 only	
Admin1, Admin2, and Admin4 only	
Admin1, Admin2, Admin3, and Admin4	

Answer:

#### Answer Area

Create RG2:

	▼
Admin3 only	
Admin2 and Admin3 only	
Admin3 and Admin4 only	
Admin2, Admin3, and Admin4 only	
Admin1, Admin2, Admin3, and Admin4	

Manage RG1 permissions:

	▼
Admin4 only	
Admin1 and Admin4 only	
Admin3 and Admin4 only	
Admin1, Admin2, and Admin4 only	
Admin1, Admin2, Admin3, and Admin4	

Explanation:

Box 1: Admin3 only -

The Contributor role has the necessary write permissions to create the resource group.

## Question: 486

CertyIQ

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

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study. At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

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

General Overview -

Fabrikam, Inc. is a consulting company that has a main office in Montreal and branch offices in Seattle and New York. Fabrikam has IT, human resources (HR), and finance departments.

Existing Environment -

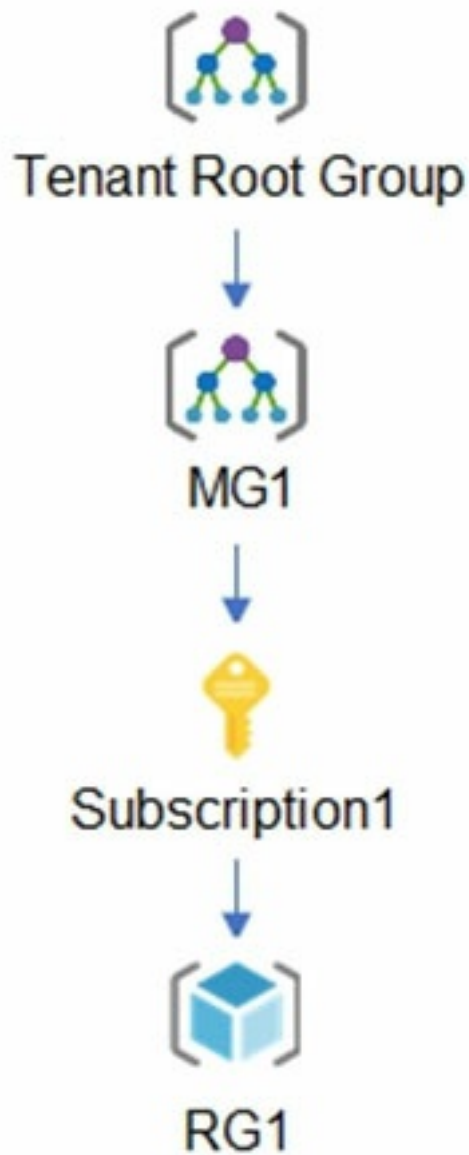
Network Environment -

Fabrikam has a Microsoft 365 subscription and an Azure subscription named subscription1.

The network contains an on-premises Active Directory domain named Fabrikam.com. The domain contains two organizational units (OUs) named OU1 and OU2.

Azure AD Connect cloud sync syncs only OU1.

The Azure resources hierarchy is shown in the following exhibit.



The Azure Active Directory (Azure AD) tenant contains the users shown in the following table.

Name	Type	Directory-synced	Role	Delegated to
User1	User	Yes	User	<b>None</b>
Admin1	User	No	User Access Administrator	Tenant Root Group
Admin2	User	No	Security administrator	MG1
Admin3	User	No	Contributor	Subscription1
Admin4	User	No	Owner	RG1
Group1	Group	No	<b>Not applicable</b>	<b>None</b>

Azure AD contains the resources shown in the following table.

Name	Type	Setting
CAPolicy1	Conditional access policy	Users in the finance department must use multi-factor authentication (MFA) when accessing Microsoft SharePoint Online
Sentinel1	Azure Sentinel workspace	<b>Not applicable</b>
SecPol1	Azure Policy definition	Security configuration for virtual machines

Subscription1 Resources -  
Subscription1 contains the virtual networks shown in the following table.

Name	Subnet	Location	Peer
VNET1	Subnet1, Subnet2	West US	VNET2, VNET3
VNET2	Subnet1	Central US	VNET1, VNET3
VNET3	Subnet1	West US	VNET1, VNET2

Subscription1 contains the network security groups (NSGs) shown in the following table.

Name	Location
NSG2	West US
NSG3	Central US
NSG4	West US

Subscription1 contains the virtual machines shown in the following table.

Name	Operating system	Location	Connected to	Associated NSG
VM1	Windows Server 2019	West US	VNET1/Subnet1	<b>None</b>
VM2	CentOS-based 8.2	West US	VNET1/Subnet2	NSG2
VM3	Windows Server 2016	Central US	VNET2/Subnet1	NSG3
VM4	Ubuntu Server 18.04 LTS	West US	VNET3/Subnet1	NSG4

Subscription1 contains the Azure key vaults shown in the following table.

Name	Location	Pricing tier	Private endpoint
KeyVault1	West US	Standard	VNET1/Subnet1
KeyVault2	Central US	Premium	<b>None</b>
KeyVault3	East US	Premium	VNET1/Subnet1, VNET2/Subnet1, VNET3/Subnet1

Subscription1 contains a storage account named storage1 in the West US Azure region.  
Planned Changes and Requirements

Planned Changes -  
Fabrikam plans to implement the following changes:  
Create two application security groups as shown in the following table.

Name	Location
ASG1	West US
ASG2	Central US

Associate the network interface of VM1 to ASG1.  
Deploy SecPol1 by using Microsoft Defender for Cloud.

Deploy a third-party app named App1. A version of App1 exists for all available operating systems.  
Create a resource group named RG2.  
Sync OU2 to Azure AD.  
Add User1 to Group1.

Technical Requirements -

Fabrikam identifies the following technical requirements:

The finance department users must reauthenticate after three hours when they access SharePoint Online.

Storage1 must be encrypted by using customer-managed keys and automatic key rotation.

From Sentinel1, you must ensure that the following notebooks can be launched:

- Entity Explorer "" Account
- Entity Explorer "" Windows Host
- Guided Investigation Process Alerts

VM1, VM2, and VM3 must be encrypted by using Azure Disk Encryption.

Just in time (JIT) VM access for VM1, VM2, and VM3 must be enabled.

App1 must use a secure connection string stored in KeyVault1.

KeyVault1 traffic must NOT travel over the internet. Question You plan to configure Azure Disk Encryption for VM4.

Which key vault can you use to store the encryption key?

- A.KeyVault1
- B.KeyVault2
- C.KeyVault3

**Answer: A**

**Explanation:**

The key vault needs to be in the same subscription and same region as the VM.

VM4 is in West US. KeyVault1 is the only key vault in the same region as the VM.

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-machines/windows/disk-encryption-key-vault>

## Question: 487

CertyIQ

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

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study. At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

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

General Overview -

Fabrikam, Inc. is a consulting company that has a main office in Montreal and branch offices in Seattle and New York. Fabrikam has IT, human resources (HR), and finance departments.

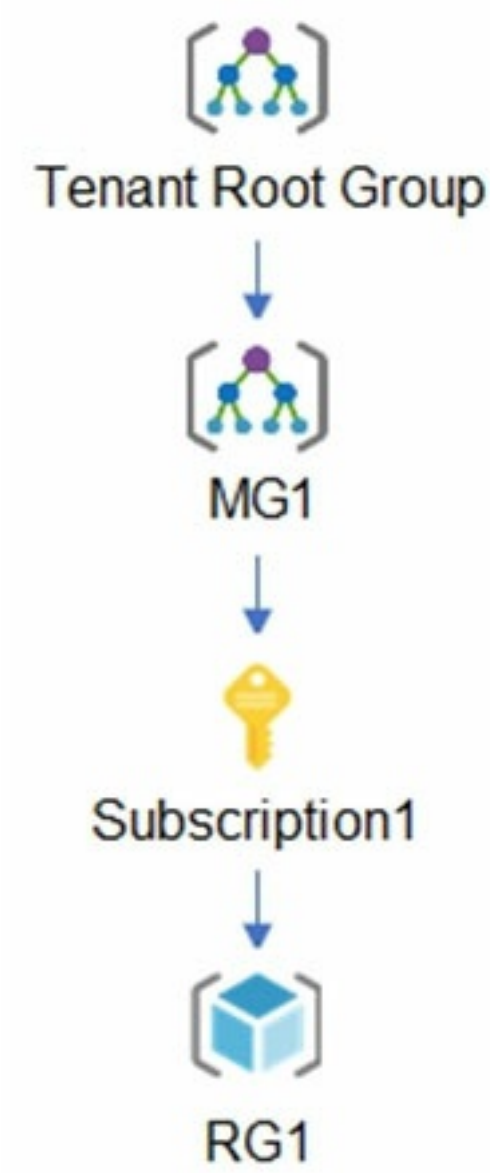
Existing Environment -

Network Environment -

Fabrikam has a Microsoft 365 subscription and an Azure subscription named subscription1.

The network contains an on-premises Active Directory domain named Fabrikam.com. The domain contains two

organizational units (OUs) named OU1 and OU2.  
Azure AD Connect cloud sync syncs only OU1.  
The Azure resources hierarchy is shown in the following exhibit.



The Azure Active Directory (Azure AD) tenant contains the users shown in the following table.

Name	Type	Directory-synced	Role	Delegated to
User1	User	Yes	User	None
Admin1	User	No	User Access Administrator	Tenant Root Group
Admin2	User	No	Security administrator	MG1
Admin3	User	No	Contributor	Subscription1
Admin4	User	No	Owner	RG1
Group1	Group	No	Not applicable	None

Azure AD contains the resources shown in the following table.



Name	Type	Setting
CAPolicy1	Conditional access policy	Users in the finance department must use multi-factor authentication (MFA) when accessing Microsoft SharePoint Online
Sentinel1	Azure Sentinel workspace	<b>Not applicable</b>
SecPol1	Azure Policy definition	Security configuration for virtual machines

Subscription1 Resources -  
Subscription1 contains the virtual networks shown in the following table.

Name	Subnet	Location	Peer
VNET1	Subnet1, Subnet2	West US	VNET2, VNET3
VNET2	Subnet1	Central US	VNET1, VNET3
VNET3	Subnet1	West US	VNET1, VNET2

Subscription1 contains the network security groups (NSGs) shown in the following table.

Name	Location
NSG2	West US
NSG3	Central US
NSG4	West US

Subscription1 contains the virtual machines shown in the following table.

Name	Operating system	Location	Connected to	Associated NSG
VM1	Windows Server 2019	West US	VNET1/Subnet1	<b>None</b>
VM2	CentOS-based 8.2	West US	VNET1/Subnet2	NSG2
VM3	Windows Server 2016	Central US	VNET2/Subnet1	NSG3
VM4	Ubuntu Server 18.04 LTS	West US	VNET3/Subnet1	NSG4

Subscription1 contains the Azure key vaults shown in the following table.

Name	Location	Pricing tier	Private endpoint
KeyVault1	West US	Standard	VNET1/Subnet1
KeyVault2	Central US	Premium	<b>None</b>
KeyVault3	East US	Premium	VNET1/Subnet1, VNET2/Subnet1, VNET3/Subnet1

Subscription1 contains a storage account named storage1 in the West US Azure region.  
Planned Changes and Requirements

Planned Changes -  
Fabrikam plans to implement the following changes:  
Create two application security groups as shown in the following table.

Name	Location
ASG1	West US
ASG2	Central US

Associate the network interface of VM1 to ASG1.  
Deploy SecPol1 by using Microsoft Defender for Cloud.

Deploy a third-party app named App1. A version of App1 exists for all available operating systems.  
Create a resource group named RG2.  
Sync OU2 to Azure AD.  
Add User1 to Group1.

Technical Requirements -

Fabrikam identifies the following technical requirements:

The finance department users must reauthenticate after three hours when they access SharePoint Online.

Storage1 must be encrypted by using customer-managed keys and automatic key rotation.

From Sentinel1, you must ensure that the following notebooks can be launched:

- Entity Explorer "" Account
- Entity Explorer "" Windows Host
- Guided Investigation Process Alerts

VM1, VM2, and VM3 must be encrypted by using Azure Disk Encryption.

Just in time (JIT) VM access for VM1, VM2, and VM3 must be enabled.

App1 must use a secure connection string stored in KeyVault1.

KeyVault1 traffic must NOT travel over the internet. Question You need to encrypt storage1 to meet the technical requirements.

Which key vaults can you use?

- A.KeyVault2 and KeyVault3 only
- B.KeyVault1 only
- C.KeyVault1 and KeyVault3 only
- D.KeyVault1, KeyVault2, and KeyVault3

**Answer: D**

**Explanation:**

Things have changed. Now KeyVault can be in a different region or sub, but in the same tenant:

[https://learn.microsoft.com/en-us/azure/storage/common/customer-managed-keys-configure-existing-account?WT.mc\\_id=Portal-Microsoft\\_Azure\\_Storage&tabs=azure-portal](https://learn.microsoft.com/en-us/azure/storage/common/customer-managed-keys-configure-existing-account?WT.mc_id=Portal-Microsoft_Azure_Storage&tabs=azure-portal)

On reference link: The storage account and the key vault or managed HSM can be different Azure Active Directory (Azure AD) tenants, regions, and subscriptions.

**Question: 488**

**CertyIQ**

HOTSPOT -

You implement the planned changes for ASG1 and ASG2.

In which NSGs can you use ASG1, and the network interfaces of which virtual machines can you assign to ASG2?

Hot Area:

## Answer Area

NSGs:

	▼
NSG2 only	
NSG2 and NSG4 only	
NSG2, NSG3, and NSG4	

Virtual machines:

	▼
VM3 only	
VM2 and VM4 only	
VM1, VM2, and VM4 only	
VM2, VM3, and VM4 only	
VM1, VM2, VM3, and VM4	

Answer:

### Answer Area

NSGs:

	▼
NSG2 only	
NSG2 and NSG4 only	
NSG2, NSG3, and NSG4	

Virtual machines:

	▼
VM3 only	
VM2 and VM4 only	
VM1, VM2, and VM4 only	
VM2, VM3, and VM4 only	
VM1, VM2, VM3, and VM4	

Explanation:

ASG constraint : All network interfaces assigned to an application security group have to exist in the same virtual network that the first network interface assigned to the application security group is in. (Not a regional constraint)

1) NSG2 only

2) VM3 only

**Question: 489**

CertyIQ

You plan to implement JIT VM access.  
Which virtual machines will be supported?

- A. VM2, VM3, and VM4 only
- B. VM1, VM2, VM3, and VM4
- C. VM1 and VM3 only
- D. VM1 only

**Answer: A**

**Explanation:**

NSG is a requirement for JIT, So A makes more sense. VM2, VM3, and VM4 all have NSGs.

**Question: 490**

CertyIQ

DRAG DROP -  
You need to deploy AKS1 to meet the platform protection requirements.  
Which four 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.  
NOTE: More than one order of answer choices is correct. You will receive credit for any of the correct orders you select.  
Select and Place:

**Actions**

**Answer Area**

- Deploy an AKS cluster.
- Create a client application.
- Create a server application.
- Create an RBAC binding.
- Create a custom RBAC role.

Answer:

### Actions

Create a custom RBAC role.

### Answer Area

Create a server application.

Create a client application.

Deploy an AKS cluster.

Create an RBAC binding.

#### Explanation:

Scenario: Azure AD users must be able to authenticate to AKS1 by using their Azure AD credentials.

Litware plans to deploy AKS1, which is a managed AKS (Azure Kubernetes Services) cluster.

Step 1: Create a server application

To provide Azure AD authentication for an AKS cluster, two Azure AD applications are created. The first application is a server component that provides user authentication.

Step 2: Create a client application

The second application is a client component that's used when you're prompted by the CLI for authentication. This client application uses the server application for the actual authentication of the credentials provided by the client.

Step 3: Deploy an AKS cluster.

Use the `az group create` command to create a resource group for the AKS cluster.

Use the `az aks create` command to deploy the AKS cluster.

Step 4: Create an RBAC binding.

Before you use an Azure Active Directory account with an AKS cluster, you must create role-binding or cluster role-binding. Roles define the permissions to grant, and bindings apply them to desired users. These assignments can be applied to a given namespace, or across the entire cluster.

Reference:

<https://docs.microsoft.com/en-us/azure/aks/azure-ad-integration>

#### Question: 491

CertyIQ

You need to ensure that users can access VM0. The solution must meet the platform protection requirements. What should you do?

- A. Move VM0 to Subnet1.
- B. On Firewall, configure a network traffic filtering rule.
- C. Assign RT1 to AzureFirewallSubnet.
- D. On Firewall, configure a DNAT rule.

Answer: A



**Explanation:**

Azure Firewall has the following known issue:

Conflict with Azure Security Center (ASC) Just-in-Time (JIT) feature.

If a virtual machine is accessed using JIT, and is in a subnet with a user-defined route that points to Azure Firewall as a default gateway, ASC JIT doesn't work.

This is a result of asymmetric routing " a packet comes in via the virtual machine public IP (JIT opened the access), but the return path is via the firewall, which drops the packet because there is no established session on the firewall.

Solution: To work around this issue, place the JIT virtual machines on a separate subnet that doesn't have a user-defined route to the firewall.

Scenario:

VM0	Virtual machine	VM0 is an Azure virtual machine that runs Windows Server 2016, connects to Subnet0, and has just in time (JIT) VM access configured.
-----	-----------------	--

Following the implementation of the planned changes, the IT team must be able to connect to VM0 by using JIT VM access.

Name	Type	Description
Firewall1	Azure Firewall	An Azure firewall on VNet1.
RT1	Route table	A route table that will contain a route pointing to Firewall1 as the default gateway and will be assigned to Subnet0.

Reference:

<https://docs.microsoft.com/en-us/azure/firewall/overview>

**Question: 492****CertyIQ**

HOTSPOT -

You need to deploy Microsoft Antimalware to meet the platform protection requirements.

What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

**Answer Area**

Create a custom policy definition that has effect set to:

Append

Deny

DeployIfNotExists

Create a policy assignment and modify:

The Create a Managed Identity setting

The exclusion settings

The scope

**Answer:**



## Answer Area

Create a custom policy definition that has effect set to:

▼

Append

Deny

DeployIfNotExists

Create a policy assignment and modify:

▼

The Create a Managed Identity setting

The exclusion settings

The scope

### Explanation:

Scenario: Microsoft Antimalware must be installed on the virtual machines in RG1.

RG1 is a resource group that contains Vnet1, VM0, and VM1.

Box 1: DeployIfNotExists -

DeployIfNotExists executes a template deployment when the condition is met.

Azure policy definition Antimalware

Incorrect Answers:

Append:

Append is used to add additional fields to the requested resource during creation or update. A common example is adding tags on resources such as costCenter or specifying allowed IPs for a storage resource.

Deny:

Deny is used to prevent a resource request that doesn't match defined standards through a policy definition and fails the request.

Box 2: THE SCOPE

scope as generally it will be applied on Sub but you need to change it to RG as per requirements

## Question: 493

CertyIQ

You have an Azure Kubernetes Service (AKS) cluster that will connect to an Azure Container Registry. You need to use automatically generated service principal for the AKS cluster to authenticate to the Azure Container Registry.

What should you create?

- A. a secret in Azure Key Vault
- B. a role assignment
- C. an Azure Active Directory (Azure AD) user
- D. an Azure Active Directory (Azure AD) group

**Answer: B**

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/azure/aks/kubernetes-service-principal>

### Question: 494

CertyIQ

You are troubleshooting a security issue for an Azure Storage account. You enable the diagnostic logs for the storage account. What should you use to retrieve the diagnostics logs?

- A. the Security & Compliance admin center
- B. SQL query editor in Azure
- C. File Explorer in Windows
- D. AzCopy

**Answer: D**

#### Explanation:

To view and analyze your log data, you should download the blobs that contain the log data you are interested in to a local machine. Many storage-browsing tools enable you to download blobs from your storage account; you can also use the Azure Storage team provided command-line Azure Copy Tool AzCopy to download your log data.

So AzCopy is the most appropriate answer. AzCopy.

References:

<https://docs.microsoft.com/en-us/azure/storage/common/storage-analytics-logging?toc=%2fazure%2fstorage%2fblobs%2ftoc.json>

### Question: 495

CertyIQ

Introductory InfoCase Study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided. To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study. At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

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

Overview -

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.

Existing Environment -

Azure AD -

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
User9	Sydney	Owner

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.

User9 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	networkSecurityGroups	RG5
Not allowed resource types	virtualNetworks/virtualNetworkPeerings	RG6



Sub2 -  
Sub2 contains the virtual networks shown in the following table.

Name	Subnet
VNetwork1	Subnet11, Subnet12, and Subnet13
VNetwork2	Subnet21

Sub2 contains the virtual machines shown in the following table.

Name	Network interface	Application security group	Connected to
VM1	NIC1	ASG1	Subnet11
VM2	NIC2	ASG2	Subnet11
VM3	NIC3	None	Subnet12
VM4	NIC4	ASG1	Subnet13
VM5	NIC5	None	Subnet21

All virtual machines have 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	Subnet11
NSG3	Subnet13
NSG4	Subnet21

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

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.

What is the membership of Group1 and Group2? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

## Answer Area

Group1:

	▼
No members	
Only User2	
Only User2 and User4	
User1, User2, User3, and User4	

Group2:

	▼
No members	
Only User3	
Only User1 and User3	
User1, User2, User3, and User4	

Answer:



# Answer Area

Group1:

▼

No members
Only User2
Only User2 and User4
User1, User2, User3, and User4

Group2:

▼

No members
Only User3
Only User1 and User3
User1, User2, User3, and User4

## Explanation:

Box 1: User1, User2, User3, User4

Contains "ON" is true for Montreal (User1), MONTREAL (User2), London (User 3), and Ontario (User4) as string and regex operations are not case sensitive.

Box 2: Only User3 -

Match "\*"on" is only true for London (User3) as 'London' is the only word that ends with 'on'.

Scenario:

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"

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/groups-dynamic-membership>

## Question: 496

CertyIQ

### Introductory InfoCase Study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided. To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study. At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

### To start the case study -

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

### Overview -

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.

### Existing Environment -

#### Azure AD -

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
User9	Sydney	Owner

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.  
User9 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	networkSecurityGroups	RG5
Not allowed resource types	virtualNetworks/virtualNetworkPeerings	RG6

Sub2 -  
Sub2 contains the virtual networks shown in the following table.

Name	Subnet
VNetwork1	Subnet11, Subnet12, and Subnet13
VNetwork2	Subnet21

Sub2 contains the virtual machines shown in the following table.



Name	Network interface	Application security group	Connected to
VM1	NIC1	ASG1	Subnet11
VM2	NIC2	ASG2	Subnet11
VM3	NIC3	None	Subnet12
VM4	NIC4	ASG1	Subnet13
VM5	NIC5	None	Subnet21

All virtual machines have 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	Subnet11
NSG3	Subnet13
NSG4	Subnet21

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

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.  
 You are evaluating the security of the network communication between the virtual machines in Sub2.  
 For each of the following statements, select Yes if the statement is true. Otherwise, select No.  
 NOTE: Each correct selection is worth one point.

Hot Area:

### Answer Area

Statements	Yes	No
From VM1, you can successfully ping the public IP address of VM2.	<input type="radio"/>	<input type="radio"/>
From VM1, you can successfully ping the private IP address of VM3.	<input type="radio"/>	<input type="radio"/>
From VM1, you can successfully ping the private IP address of VM5.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
From VM1, you can successfully ping the public IP address of VM2.	<input type="radio"/>	<input checked="" type="radio"/>
From VM1, you can successfully ping the private IP address of VM3.	<input checked="" type="radio"/>	<input type="radio"/>
From VM1, you can successfully ping the private IP address of VM5.	<input type="radio"/>	<input checked="" type="radio"/>

Explanation:

1 -- No, as traffic would be sourced from internet since it is destined to the public IP address of VM2.2 -- Yes, as VM3 has no NSGs interfering and traffic is contained within the same vnet.3 -- No, as VM5 is in a separate vnet and there is no mention of any peering going on.

### Question: 497

CertyIQ

#### HOTSPOT -

You are evaluating the effect of the application security groups on the network communication between the virtual machines in Sub2.

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

NOTE: Each correct selection is worth one point.

Hot Area:

#### Answer area

Statements	Yes	No
From VM1, you can successfully ping the private IP address of VM4.	<input type="radio"/>	<input type="radio"/>
From VM2, you can successfully ping the private IP address of VM4.	<input type="radio"/>	<input type="radio"/>
From VM1, you can connect to the web server on VM4.	<input type="radio"/>	<input type="radio"/>

#### Answer:

#### Answer area

Statements	Yes	No
From VM1, you can successfully ping the private IP address of VM4.	<input type="radio"/>	<input checked="" type="radio"/>
From VM2, you can successfully ping the private IP address of VM4.	<input checked="" type="radio"/>	<input type="radio"/>
From VM1, you can connect to the web server on VM4.	<input checked="" type="radio"/>	<input type="radio"/>

#### Explanation:

Box 1: No. VM4 is in Subnet13 which has NSG3 attached to it.

VM1 is in ASG1. NSG3 would only allow ICMP pings from ASG2 but not ASG1. Only TCP traffic is allowed from ASG1.

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

Box 2: Yes.

VM2 is in ASG2. Any protocol is allowed from ASG2 so ICMP ping would be allowed.

Box3. VM1 is in ASG1. TCP traffic is allowed from ASG1 so VM1 could connect to the web server as connections to the web server would be on ports TCP 80 or



**Question: 498****Introductory Info Case Study -**

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided. To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study. At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

**To start the case study -**

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

**Overview -**

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.

**Existing Environment -****Azure AD -**

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
User9	Sydney	Owner

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.

User9 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	networkSecurityGroups	RG5
Not allowed resource types	virtualNetworks/virtualNetworkPeerings	RG6

Sub2 -

Sub2 contains the virtual networks shown in the following table.

Name	Subnet
VNetwork1	Subnet11, Subnet12, and Subnet13
VNetwork2	Subnet21

Sub2 contains the virtual machines shown in the following table.

Name	Network interface	Application security group	Connected to
VM1	NIC1	ASG1	Subnet11
VM2	NIC2	ASG2	Subnet11
VM3	NIC3	None	Subnet12
VM4	NIC4	ASG1	Subnet13
VM5	NIC5	None	Subnet21

All virtual machines have 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	Subnet11
NSG3	Subnet13
NSG4	Subnet21

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

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. Question You need to meet the technical requirements for VNetwork1.

What should you do first?

- A. Create a new subnet on VNetwork1.
- B. Remove the NSGs from Subnet11 and Subnet13.
- C. Associate an NSG to Subnet12.
- D. Configure DDoS protection for VNetwork1.

**Answer: A**

**Explanation:**

From scenario: Deploy Azure Firewall to VNetwork1 in Sub2.

Azure firewall needs a dedicated subnet named AzureFirewallSubnet.

Reference:

<https://docs.microsoft.com/en-us/azure/firewall/tutorial-firewall-deploy-portal>

**Question: 499**

**CertyIQ**

Introductory Info Case Study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided. To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study. At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

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

Overview -

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.

Existing Environment -

Azure AD -

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
User9	Sydney	Owner

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.

User9 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	networkSecurityGroups	RG5
Not allowed resource types	virtualNetworks/virtualNetworkPeerings	RG6

Sub2 -

Sub2 contains the virtual networks shown in the following table.



Name	Subnet
VNetwork1	Subnet11, Subnet12, and Subnet13
VNetwork2	Subnet21

Sub2 contains the virtual machines shown in the following table.

Name	Network interface	Application security group	Connected to
VM1	NIC1	ASG1	Subnet11
VM2	NIC2	ASG2	Subnet11
VM3	NIC3	None	Subnet12
VM4	NIC4	ASG1	Subnet13
VM5	NIC5	None	Subnet21

All virtual machines have 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	Subnet11
NSG3	Subnet13
NSG4	Subnet21

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

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. Question HOTSPOT -

You are evaluating the security of VM1, VM2, and VM3 in Sub2.

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

NOTE: Each correct selection is worth one point.

Hot Area:

**Answer area**

	Yes	No
From the Internet, you can connect to the web server on VM1 by using HTTP.	<input type="radio"/>	<input type="radio"/>
From the Internet, you can connect to the web server on VM2 by using HTTP.	<input type="radio"/>	<input type="radio"/>
From the Internet, you can connect to the web server on VM3 by using HTTP.	<input type="radio"/>	<input type="radio"/>

**Answer:**

**Answer area**

	Yes	No
From the Internet, you can connect to the web server on VM1 by using HTTP.	<input checked="" type="radio"/>	<input type="radio"/>
From the Internet, you can connect to the web server on VM2 by using HTTP.	<input type="radio"/>	<input checked="" type="radio"/>
From the Internet, you can connect to the web server on VM3 by using HTTP.	<input checked="" type="radio"/>	<input type="radio"/>

**Explanation:**

VM1: Yes. NSG2 applies to VM1 and this allows inbound traffic on port 80.

VM2: No. NSG2 and NSG1 apply to VM2. NSG2 allows the inbound traffic on port 80 but NSG1 does not allow it.

VM3: Yes. There are no NSGs applying to VM3 so all ports will be open.

## Question: 500

CertyIQ

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

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study. At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

**To start the case study -**

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

**General Overview -**

Fabrikam, Inc. is a consulting company that has a main office in Montreal and branch offices in Seattle and New York. Fabrikam has IT, human resources (HR), and finance departments.

**Existing Environment -**

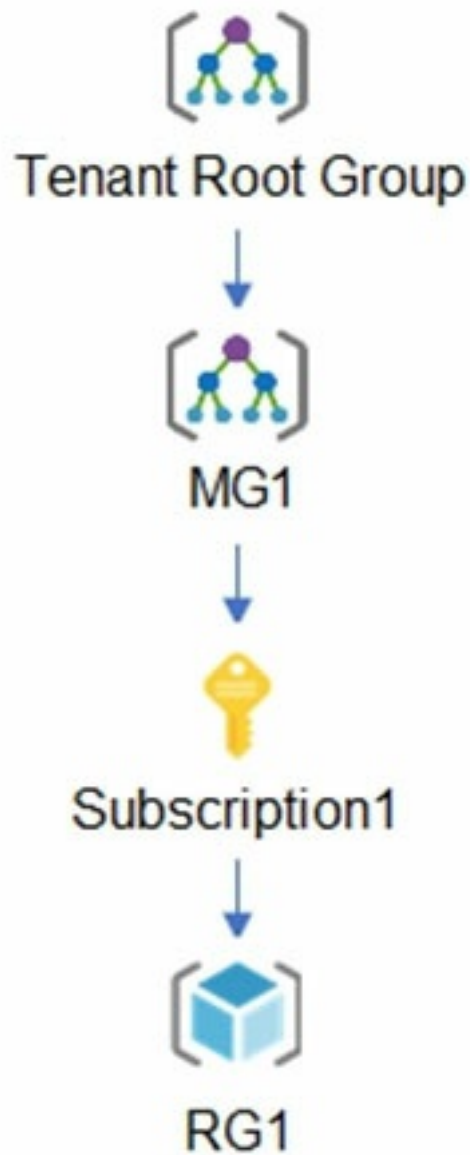
**Network Environment -**

Fabrikam has a Microsoft 365 subscription and an Azure subscription named subscription1.

The network contains an on-premises Active Directory domain named Fabrikam.com. The domain contains two organizational units (OUs) named OU1 and OU2.

Azure AD Connect cloud sync syncs only OU1.

The Azure resources hierarchy is shown in the following exhibit.



The Azure Active Directory (Azure AD) tenant contains the users shown in the following table.

Name	Type	Directory-synced	Role	Delegated to
User1	User	Yes	User	<b>None</b>
Admin1	User	No	User Access Administrator	Tenant Root Group
Admin2	User	No	Security administrator	MG1
Admin3	User	No	Contributor	Subscription1
Admin4	User	No	Owner	RG1
Group1	Group	No	<b>Not applicable</b>	<b>None</b>

Azure AD contains the resources shown in the following table.

Name	Type	Setting
CAPolicy1	Conditional access policy	Users in the finance department must use multi-factor authentication (MFA) when accessing Microsoft SharePoint Online
Sentinel1	Azure Sentinel workspace	<b>Not applicable</b>
SecPol1	Azure Policy definition	Security configuration for virtual machines

Subscription1 Resources -  
Subscription1 contains the virtual networks shown in the following table.

Name	Subnet	Location	Peer
VNET1	Subnet1, Subnet2	West US	VNET2, VNET3
VNET2	Subnet1	Central US	VNET1, VNET3
VNET3	Subnet1	West US	VNET1, VNET2

Subscription1 contains the network security groups (NSGs) shown in the following table.

Name	Location
NSG2	West US
NSG3	Central US
NSG4	West US

Subscription1 contains the virtual machines shown in the following table.

Name	Operating system	Location	Connected to	Associated NSG
VM1	Windows Server 2019	West US	VNET1/Subnet1	<b>None</b>
VM2	CentOS-based 8.2	West US	VNET1/Subnet2	NSG2
VM3	Windows Server 2016	Central US	VNET2/Subnet1	NSG3
VM4	Ubuntu Server 18.04 LTS	West US	VNET3/Subnet1	NSG4

Subscription1 contains the Azure key vaults shown in the following table.

Name	Location	Pricing tier	Private endpoint
KeyVault1	West US	Standard	VNET1/Subnet1
KeyVault2	Central US	Premium	<b>None</b>
KeyVault3	East US	Premium	VNET1/Subnet1, VNET2/Subnet1, VNET3/Subnet1

Subscription1 contains a storage account named storage1 in the West US Azure region.  
Planned Changes and Requirements

Planned Changes -  
Fabrikam plans to implement the following changes:  
Create two application security groups as shown in the following table.

Name	Location
ASG1	West US
ASG2	Central US

Associate the network interface of VM1 to ASG1.  
Deploy SecPol1 by using Microsoft Defender for Cloud.

Deploy a third-party app named App1. A version of App1 exists for all available operating systems.  
Create a resource group named RG2.  
Sync OU2 to Azure AD.  
Add User1 to Group1.

Technical Requirements -  
Fabrikam identifies the following technical requirements:  
The finance department users must reauthenticate after three hours when they access SharePoint Online.  
Storage1 must be encrypted by using customer-managed keys and automatic key rotation.  
From Sentinel1, you must ensure that the following notebooks can be launched:  
- Entity Explorer "" Account  
- Entity Explorer "" Windows Host  
- Guided Investigation Process Alerts  
VM1, VM2, and VM3 must be encrypted by using Azure Disk Encryption.  
Just in time (JIT) VM access for VM1, VM2, and VM3 must be enabled.  
App1 must use a secure connection string stored in KeyVault1.  
KeyVault1 traffic must NOT travel over the internet. Question HOTSPOT -  
You need to configure support for Microsoft Sentinel notebooks to meet the technical requirements.  
What is the minimum number of Azure container registries and Azure Machine Learning workspaces required?  
Hot Area:

Answer Area

Container registries:

	▼
0	
1	
2	
3	

Workspaces:

	▼
0	
1	
2	
3	

Answer:



## Answer Area

Container registries:

	▼
0	
1	
2	
3	

Workspaces:

	▼
0	
1	
2	
3	

### Explanation:

Has nothing to do with container registries, so 0 needed,

you need 1 Az ML Workspace

("In Microsoft Sentinel, notebooks are run on an Azure Machine Learning (Azure ML) platform")

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/notebooks>

### Question: 501

CertyIQ

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

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study. At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

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



General Overview -  
Fabrikam, Inc. is a consulting company that has a main office in Montreal and branch offices in Seattle and New York. Fabrikam has IT, human resources (HR), and finance departments.

Existing Environment -

Network Environment -  
Fabrikam has a Microsoft 365 subscription and an Azure subscription named subscription1.  
The network contains an on-premises Active Directory domain named Fabrikam.com. The domain contains two organizational units (OUs) named OU1 and OU2.  
Azure AD Connect cloud sync syncs only OU1.  
The Azure resources hierarchy is shown in the following exhibit.



The Azure Active Directory (Azure AD) tenant contains the users shown in the following table.

Name	Type	Directory-synced	Role	Delegated to
User1	User	Yes	User	None
Admin1	User	No	User Access Administrator	Tenant Root Group
Admin2	User	No	Security administrator	MG1
Admin3	User	No	Contributor	Subscription1
Admin4	User	No	Owner	RG1
Group1	Group	No	Not applicable	None

Azure AD contains the resources shown in the following table.

Name	Type	Setting
CAPolicy1	Conditional access policy	Users in the finance department must use multi-factor authentication (MFA) when accessing Microsoft SharePoint Online
Sentinel1	Azure Sentinel workspace	<b>Not applicable</b>
SecPol1	Azure Policy definition	Security configuration for virtual machines

Subscription1 Resources -  
Subscription1 contains the virtual networks shown in the following table.

Name	Subnet	Location	Peer
VNET1	Subnet1, Subnet2	West US	VNET2, VNET3
VNET2	Subnet1	Central US	VNET1, VNET3
VNET3	Subnet1	West US	VNET1, VNET2

Subscription1 contains the network security groups (NSGs) shown in the following table.

Name	Location
NSG2	West US
NSG3	Central US
NSG4	West US

Subscription1 contains the virtual machines shown in the following table.

Name	Operating system	Location	Connected to	Associated NSG
VM1	Windows Server 2019	West US	VNET1/Subnet1	<b>None</b>
VM2	CentOS-based 8.2	West US	VNET1/Subnet2	NSG2
VM3	Windows Server 2016	Central US	VNET2/Subnet1	NSG3
VM4	Ubuntu Server 18.04 LTS	West US	VNET3/Subnet1	NSG4

Subscription1 contains the Azure key vaults shown in the following table.

Name	Location	Pricing tier	Private endpoint
KeyVault1	West US	Standard	VNET1/Subnet1
KeyVault2	Central US	Premium	<b>None</b>
KeyVault3	East US	Premium	VNET1/Subnet1, VNET2/Subnet1, VNET3/Subnet1

Subscription1 contains a storage account named storage1 in the West US Azure region.  
Planned Changes and Requirements

Planned Changes -  
Fabrikam plans to implement the following changes:  
Create two application security groups as shown in the following table.

Name	Location
ASG1	West US
ASG2	Central US

Associate the network interface of VM1 to ASG1.

Deploy SecPol1 by using Microsoft Defender for Cloud.  
Deploy a third-party app named App1. A version of App1 exists for all available operating systems.  
Create a resource group named RG2.  
Sync OU2 to Azure AD.  
Add User1 to Group1.

Technical Requirements -

Fabrikam identifies the following technical requirements:

The finance department users must reauthenticate after three hours when they access SharePoint Online.

Storage1 must be encrypted by using customer-managed keys and automatic key rotation.

From Sentinel1, you must ensure that the following notebooks can be launched:

- Entity Explorer "" Account
- Entity Explorer "" Windows Host
- Guided Investigation Process Alerts

VM1, VM2, and VM3 must be encrypted by using Azure Disk Encryption.

Just in time (JIT) VM access for VM1, VM2, and VM3 must be enabled.

App1 must use a secure connection string stored in KeyVault1.

KeyVault1 traffic must NOT travel over the internet. Question From Microsoft Defender for Cloud, you need to deploy SecPol1.

What should you do first?

- A. Enable Microsoft Defender for Cloud.
- B. Create an Azure Management group.
- C. Create an initiative.
- D. Configure continuous export.

**Answer: A**

**Explanation:**

First enable Microsoft Defender for Cloud for your subscriptions, see URL

<https://learn.microsoft.com/en-us/azure/defender-for-cloud/onboard-management-group>

## Question: 502

CertyIQ

HOTSPOT -

You assign User8 the Owner role for RG4, RG5, and RG6.

In which resource groups can User8 create virtual networks and NSGs by using the Azure portal? 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

RG5 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

Answer:

## Answer Area

User8 can create virtual networks in:

▼

RG4 only

RG6 only

RG4 and RG6 only

RG5 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

**Explanation:**

Box 1: RG6 only -

The policy does not allow the creation of virtual networks/subnets in RG5. Only NSGs can be created in RG4.

Box 2: The policy does not allow the creation of NSGs in RG5.

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

Reference:

<https://docs.microsoft.com/en-us/azure/governance/policy/overview>

**Question: 503**

HOTSPOT -

Which virtual networks in Sub1 can User9 modify and delete in their current state? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

**Answer Area**

Virtual networks that User9 can modify:

	▼
VNET4 only	
VNET4 and VNET1 only	
VNET4, VNET3, and VNET1 only	
VNET4, VNET3, VNET2, and VNET1	

Virtual networks that User9 can delete:

	▼
VNET4 only	
VNET4 and VNET1 only	
VNET4, VNET3, and VNET1 only	
VNET4, VNET3, VNET2, and VNET1	

Answer:

**Answer Area**

Virtual networks that User9 can modify:

	▼
VNET4 only	
VNET4 and VNET1 only	
VNET4, VNET3, and VNET1 only	
VNET4, VNET3, VNET2, and VNET1	

Virtual networks that User9 can delete:

	▼
VNET4 only	
VNET4 and VNET1 only	
VNET4, VNET3, and VNET1 only	
VNET4, VNET3, VNET2, and VNET1	

**Explanation:**

Box 1: VNET4 and VNET1 only -

RG1 has only Delete lock, while there are no locks on RG4.

RG2 and RG3 both have Read-only locks.

Box 2: VNET4 only -



There are no locks on RG4, while the other resource groups have either Delete or Read-only locks.

Note: As an administrator, you may need to lock a subscription, resource group, or resource to prevent other users in your organization from accidentally deleting or modifying critical resources. You can set the lock level to CanNotDelete or ReadOnly. In the portal, the locks are called Delete and Read-only respectively.

⇒ CanNotDelete means authorized users can still read and modify a resource, but they can't delete the resource.

⇒ ReadOnly means authorized users can read a resource, but they can't delete or update the resource.

Applying this lock is similar to restricting all authorized users to the permissions granted by the Reader role.

Scenario:

Sub1 contains six resource groups named RG1, RG2, RG3, RG4, RG5, and RG6.

User9 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

Reference:

<https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-lock-resources>

## Question: 504

CertyIQ

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

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study. At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

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

Overview -

Litware, Inc. is a digital media company that has 500 employees in the Chicago area and 20 employees in the San Francisco area.

Existing Environment -



Litware has an Azure subscription named Sub1 that has a subscription ID of 43894a43-17c2-4a39-8cfc-3540c2653ef4.

Sub1 is associated to an Azure Active Directory (Azure AD) tenant named litwareinc.com. The tenant contains the user objects and the device objects of all the Litware employees and their devices. Each user is assigned an Azure AD Premium P2 license. Azure AD Privileged Identity Management (PIM) is activated.

The tenant contains the groups shown in the following table.

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.
Group2	Security group	A group that has the Dynamic User membership type and contains the Chicago IT team

The Azure subscription contains the objects shown in the following table.

Name	Type	Description
VNet1	Virtual network	VNet1 is a virtual network that contains security-sensitive IT resources. VNet1 contains three subnets named Subnet0, Subnet1, and AzureFirewallSubnet.
VM0	Virtual machine	VM0 is an Azure virtual machine that runs Windows Server 2016, connects to Subnet0, and has just in time (JIT) VM access configured.
VM1	Virtual machine	VM1 is an Azure virtual machine that runs Windows Server 2016 and connects to Subnet0.
SQLDB1	Azure SQL Database	SQLDB1 is an Azure SQL database on a SQL Database server named LitwareSQLServer1.
WebApp1	Web app	WebApp1 is an Azure web app that is accessible by using https://www.litwareinc.com and http://www.litwareinc.com.
RG1	Resource group	RG1 is a resource group that contains VNet1, VM0, and VM1.
RG2	Resource group	RG2 is a resource group that contains shared IT resources.

Azure Security Center is set to the Standard tier.

Requirements -

Planned Changes -

Litware plans to deploy the Azure resources shown in the following table.

Name	Type	Description
Firewall1	Azure Firewall	An Azure firewall on VNet1.
RT1	Route table	A route table that will contain a route pointing to Firewall1 as the default gateway and will be assigned to Subnet0.
AKS1	Azure Kubernetes Service (AKS)	A managed AKS cluster

Identity and Access Requirements

Litware identifies the following identity and access requirements:

All San Francisco users and their devices must be members of Group1.  
The members of Group2 must be assigned the Contributor role to RG2 by using a permanent eligible assignment.  
Users must be prevented from registering applications in Azure AD and from consenting to applications that access company information on the users' behalf.

**Platform Protection Requirements**  
Litware identifies the following platform protection requirements:  
Microsoft Antimalware must be installed on the virtual machines in RG1.  
The members of Group2 must be assigned the Azure Kubernetes Service Cluster Admin Role.  
Azure AD users must be able to authenticate to AKS1 by using their Azure AD credentials.  
Following the implementation of the planned changes, the IT team must be able to connect to VM0 by using JIT VM access.  
A new custom RBAC role named Role1 must be used to delegate the administration of the managed disks in RG1.  
Role1 must be available only for RG1.

**Security Operations Requirements**  
Litware must be able to customize the operating system security configurations in Azure Security Center.

**Data and Application Requirements**  
Litware identifies the following data and applications requirements:  
The users in Group2 must be able to authenticate to SQLDB1 by using their Azure AD credentials.  
WebApp1 must enforce mutual authentication.

**General Requirements -**

Litware identifies the following general requirements:  
Whenever possible, administrative effort must be minimized.  
Whenever possible, use of automation must be maximized. Question 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-days 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.

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/security-center-pricing>

# Thank you

Thank you for being so interested in the premium exam material.  
I'm glad to hear that you found it informative and helpful.

If you have any feedback or thoughts on the bumps, I would love to hear them.  
Your insights can help me improve our writing and better understand our readers.

## Best of Luck

You have worked hard to get to this point, and you are well-prepared for the exam  
Keep your head up, stay positive, and go show that exam what you're made of!

Feedback

More Papers



Future is Secured  
100% Pass Guarantee



24/7 Customer Support  
Mail us - [certyiqofficial@gmail.com](mailto:certyiqofficial@gmail.com)



Free Updates  
Lifetime Free Updates!

Total: **504 Questions**

Link: <https://certyiq.com/papers/microsoft/az-500>