PassQueen
a.k.a dumpsqueen.com

Microsoft Azure Security Technologies

Microsoft AZ-500

Version Demo

Total Demo Questions: 122

Total Premium Questions: 1224

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Manage identity and access	460
Topic 2, Secure networking	168
Topic 3, Secure compute, storage, and databases	259
Topic 4, Manage security operations	304
Topic 5, Mix Questions	7
Topic 6, Case Study 1	4
Topic 7, Case Study 2	3
Topic 8, Case Study 3	4
Topic 9, Case Study 4	3
Topic 10, Case Study 5	5
Topic 11, Case Study 6	2
Topic 12, Case Study 7	2
Topic 13, Case Study 8	3
Total	1224

QUESTION NO: 1

You have an Azure subscription named Sub1 which includes the virtual machines listed in the table below.

The table includes the following data:

Your task is to ensure that the Remote Desktop Protocol (RDP) port on the virtual machines within the resource group RG1 remains closed unless access is requested by an authorized user.

What configuration should you apply?

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) VM access is designed to reduce exposure of virtual machine management ports, including Remote Desktop Protocol over TCP port 3389. When JIT access is configured for the VMs in RG1, Microsoft Defender for Cloud ensures that the protected port is not persistently open. The service manages the relevant network controls, such as Network Security Group rules, to deny inbound RDP by default.

An authorized user can request temporary access through Defender for Cloud. The request is evaluated against the user's Azure role-based access control permissions and the configured JIT policy. If approved, JIT creates a narrowly scoped, time-limited inbound rule, typically restricted to the requester's public source IP address and the requested duration. When that duration ends, the temporary rule is removed and RDP returns to its closed state automatically. This directly fulfills the requirement for on-demand access while minimizing the time that RDP is exposed to network scanning and password-based attacks.

For configuration details and supported network controls, see Just-in-time VM access overview and Enable just-in-time access.

QUESTION NO: 2

You are working with an Azure Active Directory (Azure AD) tenant that includes a user named Admin1, who holds the Application Developer role. After purchasing a cloud application named App1 and registering it in Azure AD, Admin1 reports being unable to access the option to enable token encryption for App1. How can you grant Admin1 the ability to enable token encryption for App1 via the Azure portal?

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: D

Explanation:

Assign Admin1 the Cloud application administrator role. Token encryption is an administrative configuration for an enterprise application's service principal. This role grants the directory-level permissions needed to manage enterprise applications, including their SAML single sign-on configuration and token-encryption settings. In the Azure portal, an administrator with

this role can open the enterprise application, navigate to its token-encryption configuration, and manage the encryption certificate used to encrypt SAML assertions issued for that application. The Application Developer role is intended primarily to let users create and manage application registrations they own; it does not provide the broader enterprise-application administration privileges required for this configuration. Microsoft's role-permissions reference identifies Cloud Application Administrator as a role that can manage application registrations and enterprise applications, while the SAML token-encryption guidance describes configuring an encryption certificate in the enterprise application experience. Assign the role in Microsoft Entra ID under Roles and administrators, then have Admin1 reopen App1 in the portal to configure token encryption. See Microsoft Entra built-in roles: Cloud Application Administrator and Configure SAML token encryption.

QUESTION NO: 3

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 Log Analytics

* Azure Table storage

* Azure Queue storage

Which two services data encryption by using the keys stored in the key vault? Each correct answer present a complete solution.

NOTE: Each correct selection is worth one point.

A. Queue storage

B. Table storage

C. Azure Files

D. Blob storage

ANSWER: C D

Explanation:

Azure Files and **Blob storage** are the Azure Storage services whose data can be encrypted at rest with the customer-managed key configured for the storage account. Azure Storage Encryption protects data automatically, and when a customer-managed key is selected, Azure Storage uses the key from Azure Key Vault (or managed HSM) as the key-encryption key for the applicable service encryption hierarchy. This gives the organization control over the key lifecycle, including key rotation, revocation, and access permissions, while Azure Storage performs the underlying data encryption transparently.

For Azure Files, the customer-managed key applies to file-share data stored by the service. For Blob storage, it applies to blob data, including the supported blob types stored in the account. The storage account must be able to access the key vault key, typically through a managed identity granted the necessary key permissions or an appropriate Key Vault RBAC role. Microsoft documents that customer-managed keys for Azure Storage Encryption are supported for Blob storage and Azure Files. See Customer-managed keys for Azure Storage encryption and Azure Storage service encryption.

QUESTION NO: 4

While troubleshooting a security issue related to an Azure Storage account, you have enabled diagnostic logs for the account. Which tool should you use to retrieve these diagnostic logs?

A. the Security & Compliance admin center

B. SQL query editor in Azure

C. File Explorer in Windows

D. AzCopy

ANSWER: D

Explanation:

AzCopy is the appropriate tool for retrieving Azure Storage diagnostic log files when the logs have been written to a storage account. Storage logging produces log data as blobs, and AzCopy is Microsoft's command-line data-transfer utility for copying blobs between Azure Storage and a local system. During troubleshooting, an administrator can authenticate to the storage account using Microsoft Entra ID or a shared access signature, target the relevant blob container or log prefix, and use `azcopy copy` to download the log files for review. This approach is particularly useful for incident-response and investigation workflows because it supports efficient, scriptable, and repeatable bulk transfer of storage data. AzCopy supports copying data from Azure Blob Storage to a local file system and offers transfer features suitable for large sets of log blobs. The log contents can then be retained, searched, or analyzed with local tools or an organization's investigation platform. See the AzCopy v10 documentation for supported storage transfers and commands, and Microsoft's Storage Analytics logging documentation for details on how storage log data is stored.

QUESTION NO: 5

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: B C

Explanation:

Turn on the HTTPS Only protocol setting and **set the Minimum TLS Version protocol setting to 1.2**. HTTPS Only redirects HTTP requests to HTTPS, helping ensure that requests to the web app use an encrypted transport channel rather than permitting unencrypted HTTP access. This setting is appropriate where the application requirement is to protect traffic in transit for all callers.

The minimum TLS setting controls the oldest TLS protocol version that App Service will accept for inbound connections. Setting it to TLS 1.2 prevents clients from negotiating deprecated, weaker protocol versions while allowing TLS 1.2 and newer versions. Together, these settings enforce encrypted access and a modern minimum cryptographic transport baseline for the application.

Azure App Service documents HTTPS Only as the setting used to redirect HTTP traffic to HTTPS, and documents the minimum inbound TLS setting as the control for enforcing the lowest TLS version accepted by an app. See Enforce HTTPS in Azure App Service and Enforce TLS versions in Azure App Service.

QUESTION NO: 6

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 certificates only will be updated automatically on VM1. The Azure Key Vault VM extension is designed to retrieve certificates from a vault and place them on the virtual machine, such as in the Windows certificate store or at a configured location on Linux. Its configuration identifies the certificates to observe, and the extension periodically polls Key Vault for a newer certificate version. When Key Vault contains a renewed or rotated version, the extension downloads and installs that current certificate material on the VM. This supports workloads that require locally available certificates for TLS, mutual authentication, or similar scenarios without manually copying each renewed certificate to the machine.

Azure Key Vault certificates have versioned lifecycle management: renewal or rotation produces a new version of the certificate, which is the behavior the VM extension monitors. The automatic refresh capability is specifically documented as certificate management by the extension, enabling a VM to remain synchronized with the latest configured certificate versions. See Azure Key Vault virtual machine extension for Windows and About Azure Key Vault certificates.

QUESTION NO: 7

You are tasked with gathering events from Azure virtual machines into an Azure Log Analytics workspace, intending to create alerts based on these collected events. It is crucial to determine which Azure services are capable of creating these alerts. Which two Azure services should you choose? Each correct answer contributes to the complete solution.

Note: Each accurate selection grants one point.

A. Azure Monitor

B. Azure Security Center

C. Azure Analysis Services

D. Azure Sentinel

E. Azure Advisor

ANSWER: A D

Explanation:

Azure Monitor is correct because a Log Analytics workspace stores Azure Monitor Logs, including virtual-machine event data collected through supported agents and data collection rules. Azure Monitor can create log search alert rules from Kusto Query Language queries against that workspace. When a query result meets a configured threshold or condition, the alert rule can trigger an action group for notification, automation, or remediation. This supports operational monitoring scenarios based directly on collected Windows Event Log or Syslog records.

Azure Sentinel is also correct. Now called Microsoft Sentinel, it is a cloud-native SIEM solution that uses a Log Analytics workspace as its data store and query foundation. Sentinel analytics rules run scheduled or near-real-time detections against ingested workspace data and create security alerts and incidents when matching events are found. This makes it suitable for security-focused detections based on events from Azure virtual machines, while Azure Monitor provides the broader platform monitoring and alerting capability. See the Azure Monitor alerts overview and Microsoft Sentinel overview.

QUESTION NO: 8

You have initiated a new Azure subscription.

To enable the creation of custom alert rules within Azure Security Center, what are the two necessary steps you must undertake? Each correct choice is a component of the complete solution.

Note: Each accurate selection will earn you a 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: D E

Explanation:

Create an Azure Log Analytics workspace. and **Upgrade the pricing tier of Security Center to Standard.** are the required actions in the Security Center terminology used by this question. A Log Analytics workspace provides the data store and query platform used to collect security telemetry and evaluate the log queries that underpin custom detections. It is therefore the foundational workspace resource for creating and operating alert logic based on collected Azure security data.

The Standard tier was the paid Azure Security Center tier that enabled the enhanced security capabilities needed for advanced detection and alerting. In current product terminology, Azure Security Center is Microsoft Defender for Cloud, and the equivalent configuration is to enable the relevant Defender plans. After the workspace is available and enhanced security is enabled, security data can be collected and analyzed to support custom alerting workflows. Microsoft Sentinel can also use the Log Analytics workspace for analytics rules and incident management when it is deployed as part of the broader security-operations solution.

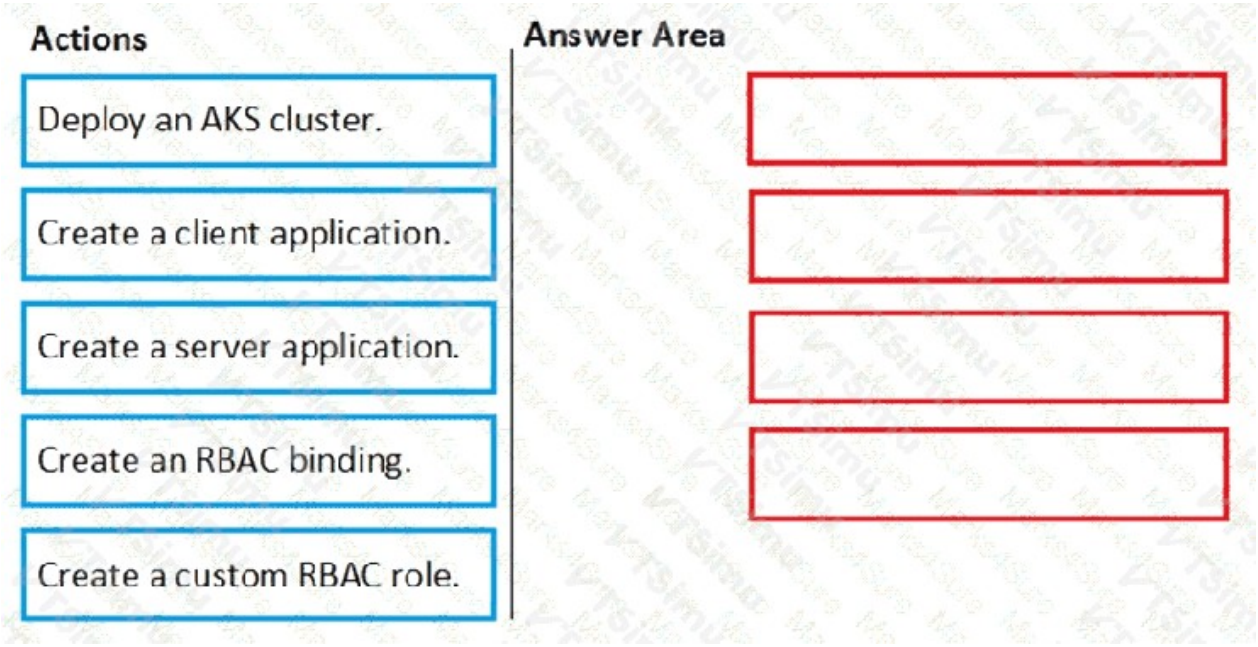
For current guidance on enabling enhanced Defender for Cloud protections, see Microsoft Defender for Cloud enhanced security. For details about onboarding a Log Analytics workspace to Microsoft Sentinel, see Microsoft Sentinel onboarding quickstart.

QUESTION NO: 9 - (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.



ANSWER:

Explanation:

The sequence begins by creating a server application because it establishes the application identity that represents the protected Kubernetes API resource. During Azure Active Directory integration, this application supplies the resource or audience for which users obtain tokens. Its configuration, including the required permissions and exposed API details, needs to be available before the interactive application can be configured to request tokens for it.

Next, create a client application. This identity is used by the sign-in workflow to obtain a user token from Azure Active Directory and request access to the server application. With both application identities prepared, the AKS cluster can be deployed using the corresponding Azure Active Directory integration settings. At cluster creation, AKS uses these application details to configure authentication for access to the Kubernetes control plane. Microsoft's AKS identity and access guidance is available at Identity and access management for Azure Kubernetes Service.

After AKS is deployed, create an RBAC binding. Authentication establishes who the signed-in user is, while Kubernetes role-based access control applies permissions to that authenticated identity. The binding connects the user or group to the appropriate Kubernetes role or cluster role, enabling the required access scope in the cluster. This completes the platform protection flow: define the authentication resource, configure the interactive sign-in identity, deploy AKS with those identities, and then authorize the resulting authenticated principals. Kubernetes authorization concepts and role bindings are documented at Using RBAC Authorization.

QUESTION NO: 10

You have an Azure Container Registry named **Registry1**. You have enabled vulnerability scanning of images in **Registry1** through Azure Security Center. You then perform the following actions:

- Upload a Windows image named **Image1** to **Registry1**.
- Upload a Linux image named **Image2** to **Registry1**.
- Upload a Windows image named **Image3** to **Registry1**.
- Modify **Image1** and upload it as **Image4** to **Registry1**.
- Modify **Image2** and upload it as **Image5** to **Registry1**.

Which two images will be analyzed for vulnerabilities? Each correct answer provides a complete solution.

NOTE: Each correct selection is worth one point.

A. Image4

B. Image2

C. Image1

D. Image3

E. Image5

ANSWER: B E

Explanation:

Image2 and **Image5** will be analyzed because the Azure Security Center container-image vulnerability assessment described in this question supports Linux container images in Azure Container Registry. When a supported image is pushed to a protected registry, the service assesses the image layers and installed packages for known vulnerabilities and reports the findings through the security service. Therefore, pushing the Linux-based Image2 creates a supported image for assessment.

Image5 is also analyzed because it is a modified version of the Linux image that is pushed to the registry as a new image. A modification results in a distinct image artifact or digest, so it is eligible for assessment when uploaded. Vulnerability assessment is associated with the image content rather than merely the original image name; a newly pushed, changed Linux image must be assessed independently so that findings reflect its current packages and layers. Microsoft documentation for the service explains container image vulnerability assessment and its registry integration in Vulnerability assessment for container images. Additional feature and protection context is available in the Microsoft Defender for Containers overview.

QUESTION NO: 11

You have an Azure subscription with 100 virtual machines and Azure Security Center Standard tier enabled. You plan to conduct a vulnerability scan on each virtual machine. What are the two values you need to include in your Azure Resource Manager template to automate the deployment of the vulnerability scanner extension onto the virtual machines? Select the correct options from the following choices. Each option you select is a part of the solution and 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: B F

Explanation:

The required values are **the workspace ID** and **the primary shared key**. In this scenario, the Resource Manager template deploys and configures the Microsoft Monitoring Agent extension on the virtual machines so that Security Center can collect the data needed for its vulnerability-assessment workflow. The extension configuration identifies the target Log Analytics workspace by using its workspace ID, also called the customer ID. It authenticates the machine to that workspace by using the workspace primary shared key. Together, these values are supplied as the extension settings and protected settings in an ARM deployment, enabling the virtual machines to connect and report telemetry at scale without configuring each machine manually. The shared key should be handled as a protected value, such as by retrieving it securely during deployment rather than exposing it in plain-text template parameters. Microsoft's ARM-template guidance for the Log Analytics agent shows the use of the workspace ID in settings and the workspace key in protected settings. Microsoft also documents vulnerability-assessment deployment and management for Azure virtual machines through Defender for Cloud. See Install the Log Analytics agent by using Azure Resource Manager templates and Deploy a vulnerability assessment solution on Azure VMs.

QUESTION NO: 12

You have an Azure Active Directory (Azure AD) tenant that includes a user named Admin1, who is assigned the Application developer role.

You purchase and register a cloud application named App1 in Azure AD. Admin1 reports that the option to enable token encryption for App1 is not available.

What action should you take to ensure Admin1 can enable token encryption for App1 in the Azure portal?

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: D

Explanation:

Assign Admin1 the Cloud Application Administrator role. Token encryption is configured for the application's service principal, which is represented in the Microsoft Entra admin center as an enterprise application. This configuration is an enterprise-application management task and requires an appropriate directory role, such as Cloud Application Administrator, Application Administrator, Global Administrator, or ownership of the relevant service principal. The Cloud Application Administrator role is designed to manage application registrations and enterprise applications, including their single sign-on configuration and credentials. It therefore gives Admin1 the necessary permissions to access and configure the token-encryption settings for App1 in the portal. The Application Developer role is intentionally more limited: it supports application development and management of applications created by the user, but it does not provide the broad enterprise-application administration permissions required for this tenant-level configuration. After the role assignment takes effect, Admin1 can open App1 under Enterprise applications, access its SAML-based single sign-on configuration where applicable, upload or select the required encryption certificate, and enable encrypted tokens or assertions. Microsoft documents the Cloud Application Administrator permissions in its Microsoft Entra built-in roles reference and describes the configuration process in Configure SAML token encryption.

QUESTION NO: 13

You are planning to deploy Azure Container Instances and have an application consisting of two containers: an application container and a validation container. The validation container monitors the application container by performing security checks via requests and waiting for responses post every transaction. It is essential to ensure that these two containers are scheduled for deployment together and that they communicate exclusively over ports which are not accessible from outside. What should you include in the deployment to achieve this?

A. application security groups

B. network security groups (NSGs)

C. management groups

D. container groups

ANSWER: D

Explanation:

A container group is the correct deployment construct for this scenario. In Azure Container Instances, a container group is a collection of containers scheduled onto the same host as a single unit. The containers share a lifecycle, local storage volumes where configured, and a network namespace. This supports the sidecar pattern: the validation container can be deployed alongside the application container and remain available whenever the application container runs.

Because containers in the same container group share a network namespace, they communicate through localhost using any required internal ports. The deployment need only expose ports intended for external access. Ports used by the validation container to submit checks to, and receive responses from, the application container can remain unexposed, so

they cannot be reached from outside the container group. This provides the required co-scheduling and private container-to-container communication without requiring separate network resources for the two tightly coupled containers.

Microsoft documents container groups as ACI's fundamental resource and scheduling unit, and specifically notes that containers in a group share a network namespace and can reach one another over localhost. See Container groups in Azure Container Instances and ACI container group networking.

QUESTION NO: 14

You have an Azure subscription that includes the resources outlined in the table below:

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 the 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 adhere to the principle of least privilege.

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

Explanation:

Assign **the Virtual Machine Contributor role for RG1** so that ServerAdmins can create and manage virtual machines within the resource group that is designated for VMs. This built-in role grants the permissions needed to manage Microsoft.Compute virtual-machine resources while keeping the assignment scope limited to RG1. Consequently, the group does not receive VM-management permissions in other resource groups.

Because the target virtual networks and subnets are in RG2, ServerAdmins also need permissions at that separate scope to associate a VM network interface with an existing subnet. **A custom RBAC role for RG2** supports least privilege by including only the required network read and subnet join permissions, such as `Microsoft.Network/virtualNetworks/subnets/read` and `Microsoft.Network/virtualNetworks/subnets/join/action`. Scope this custom role to RG2, ensuring that the group can use the existing RG2 network resources for VM deployment without receiving broad authority to create, modify, or delete network resources.

This separation of assignments follows Azure RBAC's scope model: VM administration is granted where VMs reside, while the narrowly tailored network-access permission is granted where the virtual network resides. See Virtual Machine Contributor and Azure custom roles.

QUESTION NO: 15

You are responsible for gathering logs from a substantial number of Windows Server 2016 computers using Azure Log Analytics.

Currently, you are configuring an Azure Resource Manager template to deploy the Microsoft Monitoring Agent across all servers automatically.

Which of the following elements should be incorporated into the template for successful deployment? (Choose all that apply.)

A. WorkspaceID

B. AzureADApplicationID

C. WorkspaceKey

D. StorageAccountKey

ANSWER: A C

Explanation:

Successful automated deployment of the Microsoft Monitoring Agent through an Azure Resource Manager template requires both *WorkspaceID* and *WorkspaceKey*. The workspace ID, also called the customer ID, identifies the specific Log Analytics workspace to which the installed agent must connect and send collected telemetry. In an ARM deployment of the Microsoft.EnterpriseCloud.Monitoring/MicrosoftMonitoringAgent extension, this value is supplied in the extension's public settings as `workspaceId`.

The workspace key is the shared authentication secret used when the agent is onboarded to that workspace. It is supplied as `workspaceKey` in the extension's protected settings, rather than ordinary public template settings, because it is sensitive credential material. A primary or secondary workspace shared key can be used. Together, these settings let every deployed agent identify its destination workspace and authenticate its registration, allowing centrally configured Windows event, performance, and other Log Analytics data collection to begin.

Microsoft documents the Windows Log Analytics agent VM extension settings, including `workspaceId` and protected `workspaceKey`, at Log Analytics virtual machine extension for Windows. Workspace IDs and shared keys are available as documented in Manage access to a Log Analytics workspace.

QUESTION NO: 16

Note: This question is part of a series of questions that share the same setup, but each question has a unique result. Determine whether the solution meets the requirements.

Your organization's Azure subscription includes a virtual network configured with a single subnet.

You have configured a service endpoint on this subnet, which hosts an Azure virtual machine running Ubuntu Server 18.04.

You plan to deploy Docker containers to this virtual machine. You must ensure that these containers can access Azure Storage resources and Azure SQL databases using the service endpoint.

Before deploying the containers, you need to perform a specific task on the virtual machine.

Solution: Install the container network interface (CNI) plug-in on the virtual machine.

Does this solution meet the intended goal?

A. Yes

B. No

ANSWER: A

Explanation:

Installing the container network interface (CNI) plug-in on the virtual machine meets the goal. Azure Virtual Network container networking enables Docker containers to receive IP addresses from the virtual network subnet rather than relying solely on the host virtual machine's default Docker bridge/NAT network. Consequently, the containers are connected to the subnet on which the Azure service endpoint is enabled.

Service endpoints extend the identity of a virtual network and subnet to supported Azure platform services, including Azure Storage and Azure SQL Database. Traffic from container IP addresses allocated from the endpoint-enabled subnet can therefore reach those services through the service endpoint path. This also permits the applicable Storage account and Azure SQL network rules to authorize the designated virtual network/subnet, rather than requiring public-source IP allowlisting. Installing the plug-in before container deployment is necessary because it configures the container networking capability used when the containers are created.

Microsoft documents Azure Virtual Network container networking and its use of subnet IP addresses at Azure container networking overview. The behavior and supported services for service endpoints are documented at Virtual Network service endpoints overview.

QUESTION NO: 17 - (DRAG DROP)

DRAG DROP (Drag and Drop is not supported) (Drag and Drop is not supported) You have an Azure subscription that contains an Azure web app named App1.

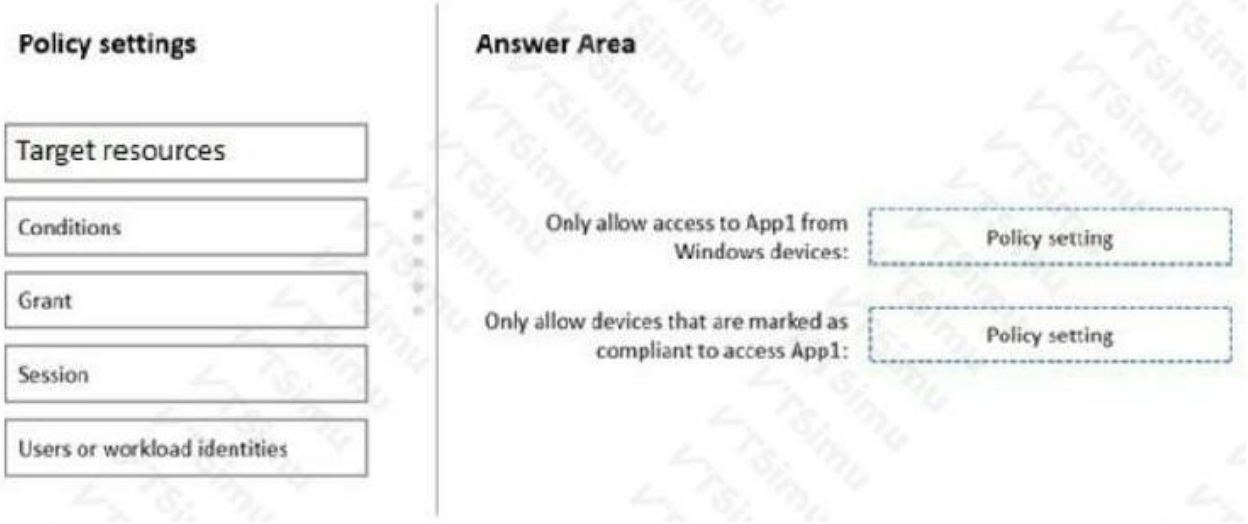
You plan to configure a Conditional Access policy for App1. The solution must meet the following requirements:

• Only allow access to App1 from Windows devices.

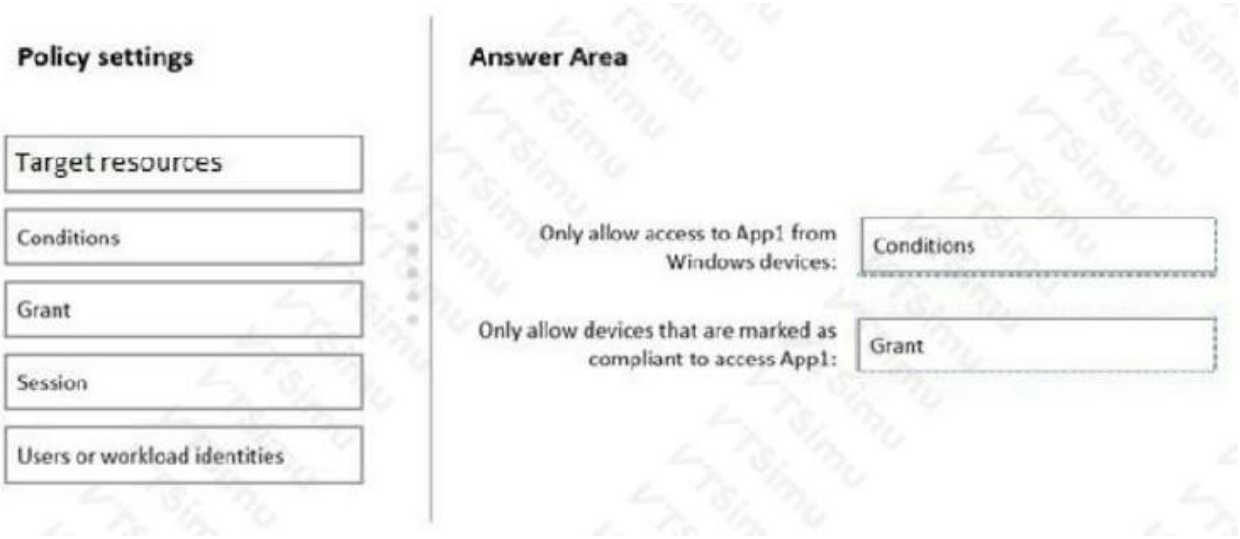
• Only allow devices that are marked as compliant to access App1.

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.



ANSWER:



Explanation:

To meet the requirements, configure the Conditional Access policy using a device-platform condition together with a compliance-based grant control. For the requirement to allow access to App1 only from Windows devices, use **Conditions**. Conditional Access evaluates the platform of a device during sign-in through the *Device platforms* condition. Configure that condition so Windows is included for the policy, which makes the platform restriction part of the sign-in context evaluated before access is granted. Microsoft documents device platforms as a Conditional Access condition at Conditional Access conditions.

For the requirement to allow only compliant devices to access App1, use **Grant**. In the Grant controls section, select *Require device to be marked as compliant*. Compliance is generally assessed by Microsoft Intune against the organization's configured compliance policies, and Conditional Access uses that compliance state as an access requirement. When the policy applies, access to the targeted application is granted only after the device meets the compliance requirement. This control is described in Microsoft's Conditional Access grant controls documentation.

Together, these settings ensure the policy evaluates whether the sign-in comes from a Windows device and requires that device to have a compliant status before the user can access App1. The policy's target resource would be configured separately to scope the policy to App1, while the two stated requirements specifically map to Conditions and Grant.

QUESTION NO: 18

Your organization intends to establish separate Azure subscriptions for each department within the company. Despite having individual subscriptions, they will all be linked to the same Azure Active Directory (Azure AD) tenant. It is essential that each subscription maintains consistent role assignments across the board. Which Azure service should you utilize to achieve this?

A. Azure Security Center

B. Azure Policy

C. Azure AD Privileged Identity Management (PIM)

D. Azure Blueprints

ANSWER: D

Explanation:

Azure Blueprints is the appropriate service because it was designed to define and repeatedly deploy a governed subscription configuration. A blueprint definition can bundle several artifacts, including Azure role-based access control (Azure RBAC) role assignments, Azure Policy assignments, resource groups, and Azure Resource Manager templates. Assigning the same blueprint to each departmental subscription deploys the defined RBAC assignments consistently, while allowing the subscriptions to remain distinct under the shared Microsoft Entra ID tenant.

This approach supports centralized governance because the blueprint assignment records the deployed configuration for each subscription and provides a standardized baseline for newly created departmental subscriptions. Role-assignment

artifacts in a blueprint can target users, groups, or service principals and apply the intended built-in or custom role at the required scope. Microsoft has announced that Azure Blueprints will be retired on July 11, 2026, and recommends transitioning to alternatives such as Template Specs and deployment stacks for future implementations. However, Azure Blueprints remains the service that directly matches this question's stated subscription-governance and repeatable-role-assignment scenario. See the Azure Blueprints overview and Microsoft's Azure Blueprints retirement guidance.

QUESTION NO: 19

Your company has an Azure subscription that includes two virtual machines named VirMac1 and VirMac2, both of which have the status Stopped (Deallocated). These virtual machines belong to separate resource groups, called ResGroup1 and ResGroup2, respectively.

There are two Azure policies in place, each set up for the virtualMachines resource type. The policy configured for ResGroup1 has a policy definition of Not allowed resource types, whereas the policy for ResGroup2 has a policy definition of Allowed resource types.

Additionally, a Read-only resource lock is applied to VirMac1, and another Read-only resource lock is applied to ResGroup2. Considering this scenario, which of the following statements are TRUE? (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: B D

Explanation:

You will NOT be able to start VirMac1 because the Read-only management lock is applied directly to that virtual machine. A Read-only lock prevents authorized users from performing operations that change the locked resource. Starting a deallocated virtual machine is a management-plane operation that changes the VM's state, so Azure blocks that operation until the lock is removed or changed. The VM's stopped/deallocated status does not bypass the lock.

You will NOT be able to create a virtual machine in ResGroup2 because the Read-only lock is applied at the resource-group scope. Management locks are inherited by all resources within the locked scope, and a Read-only lock prevents write operations in that scope. Creating a new VM requires a write operation against the Microsoft.Compute/virtualMachines resource in ResGroup2; therefore, the lock blocks creation. Although an Allowed resource types policy can permit virtual machine resources when that type is included in its allowed list, Azure Resource Manager must still satisfy the resource lock. Locks take precedence for preventing the management operation, so a permitted resource type cannot be created while the resource group remains Read-only locked.

For details, see Lock your Azure resources to protect your infrastructure and What is Azure Policy?.

QUESTION NO: 20

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: C E

Explanation:

An Azure Sentinel alert is generated and An Azure Sentinel incident is created are the applicable Sentinel-native events for starting a response playbook. A playbook is implemented as an Azure Logic App and uses a Microsoft Sentinel trigger to receive the relevant alert or incident payload, including detection details and associated entities. Starting from an alert allows automated enrichment, notification, investigation, or containment as soon as a detection generates an alert. Starting from an incident supports response workflows at the incident level, where Sentinel has grouped one or more related alerts into a case for investigation and management. These event-driven triggers are used with Sentinel automation to invoke playbooks automatically, and playbooks can also be run manually from an alert or incident when configured for the applicable trigger. Microsoft documents alert and incident triggers as the core trigger types for Sentinel playbooks and explains how automation rules can run a playbook when an incident is created or updated. See Automate threat responses with Microsoft Sentinel playbooks and Microsoft Sentinel automation rules.

QUESTION NO: 21

You have an Azure subscription that includes an application called App1. The app registration details for App1 are shown in the table below.

Currently, App1 is configured to use the following permissions:

Microsoft.Graph: User.Read (Delegated) - Admin consent not required
Microsoft.Graph: Calendars.Read (Delegated) - Admin consent not required

Your goal is to ensure that App1 can read all users' calendar data and create new appointments, while adhering to the principle of least privilege.

Which action should you perform to achieve this goal?

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 a new Delegated API permission for Microsoft.Graph Calendars.ReadWrite.Shared.

ANSWER: B

Explanation:

Add a new Application API permission for Microsoft.Graph Calendars.ReadWrite. This Microsoft Graph application permission permits App1 to read and write calendars in all mailboxes in the organization, satisfying both required operations: reading users' calendar data and creating appointments. Application permissions are appropriate when an app must access organizational data independently of a signed-in user, such as a background service or daemon. The permission operates using the app's own identity after an administrator grants tenant-wide consent.

`Calendars.ReadWrite` is the least-privileged application calendar permission that supports both reading and creating or modifying calendar events. Microsoft Graph identifies this permission as allowing an application to read and write calendars in all mailboxes without a signed-in user. Because it provides organization-wide mailbox access, administrator consent is required before the permission can be used. The app can then acquire an app-only access token and call Microsoft Graph calendar and event endpoints for the mailboxes it is authorized to access. For the permission definition and consent requirements, see Microsoft Graph permissions reference. For the app-only authorization model, see Microsoft Graph authentication and authorization concepts.

QUESTION NO: 22

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 Azure Security Center 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 the Tenant Root Group management group.

Does this meet the goal?

A. Yes

B. No

ANSWER: A

Explanation:

Yes. An Azure Policy initiative is a collection of individual policy definitions that are grouped together and managed as one unit. Creating an initiative therefore satisfies the requirement to deploy several existing policy definitions together, rather than creating separate assignments for each definition. Assigning that initiative at the Tenant Root Group management-group scope causes the assignment to be inherited by all subscriptions beneath that management group, including the three subscriptions in the scenario. This provides centralized and consistent governance across the subscription hierarchy. Azure Policy evaluates resources within each inherited scope against the definitions included in the initiative, and the resulting compliance information can be used by Microsoft Defender for Cloud (formerly Azure Security Center) for security posture management. The assignment requires appropriate permissions at the management-group scope, and the subscriptions must be located under the Tenant Root Group hierarchy for inheritance to apply. Microsoft documents that initiatives simplify assigning and managing related policies, and that policy assignments at a management-group scope apply to child subscriptions and their resources. See Azure Policy initiative definitions and Azure management groups.

QUESTION NO: 23

Note: This question is part of a series concerning the same scenario. Each question in this series includes a distinct solution which may or may not fulfill the specified goals. Some sets of questions may contain more than one correct solution, whereas others might not have any correct solution.

Once you answer a question in this section, you cannot revisit it later. These questions therefore will not appear in the review screen.

Scenario: You have an Azure subscription containing 50 virtual machines running either Windows Server 2012 R2 or Windows Server 2016.

Objective: Deploy Microsoft Antimalware to these virtual machines.

Solution: You connect to each virtual machine individually and install it as a Windows feature.

Does this solution achieve the objective?

A. Yes

B. No

ANSWER: B

Explanation:

No is correct. In the Azure VM context used by this scenario, Microsoft Antimalware is deployed to Windows virtual machines by using the Microsoft Antimalware virtual machine extension. VM extensions are Azure-managed components that run post-deployment configuration tasks in a virtual machine. The antimalware extension installs and configures the antimalware agent and supports configuration such as real-time protection, scheduled scans, exclusions, and malware reporting. This provides an Azure-supported and scalable way to deploy protection across a VM fleet, including VMs running the Windows Server versions in the scenario.

Installing software interactively as a Windows Server feature is not the deployment mechanism for the Azure Microsoft Antimalware solution. The objective specifically concerns deploying Microsoft Antimalware to Azure virtual machines, for which the extension model is the relevant management and installation approach. Azure can apply extensions during VM deployment or afterward through Azure management tools and automation, allowing consistent configuration across multiple machines. Microsoft's VM extension documentation describes extensions as the mechanism for post-deployment configuration and management of Azure VMs. See Azure VM extensions overview and Microsoft Antimalware for Azure.

QUESTION NO: 24

You have an Azure subscription that includes the virtual machines listed in the table below:

After enabling Auto Provisioning in Azure Security Center, you deploy these additional virtual machines:

Which of these virtual machines has 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:

VM1, VM2, VM3, and VM4 is correct. In the Azure Security Center behavior addressed by this question, enabling Auto Provisioning causes the service to deploy the Microsoft Monitoring Agent (also known as the Log Analytics agent or MMA) to Azure virtual machines that do not already have the agent. The setting is intended to provide consistent security data collection without requiring an administrator to install the agent separately on every machine.

Auto Provisioning applies to the virtual machines already present when the setting is enabled, which includes VM1 and VM2. It also applies automatically to eligible virtual machines created after the setting has been enabled, which includes VM3 and VM4. As a result, the agent is installed across all four listed virtual machines. The agent sends the security-related telemetry used by the Security Center/Defender for Cloud data-collection experience to the selected Log Analytics workspace, allowing the service to assess security configuration and provide relevant protections and recommendations.

Although current Defender for Cloud deployments commonly use the Azure Monitor Agent for newer collection scenarios, this question uses the legacy Microsoft Monitoring Agent terminology and behavior. See Enable data collection in Microsoft Defender for Cloud and Defender for Cloud monitoring components.

QUESTION NO: 25 - (HOTSPOT)

HOTSPOT (Drag and Drop is not supported) (Drag and Drop is not supported)

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:

Explanation:

A new resource group is created under a subscription, so the relevant Azure RBAC scope for creating RG2 is Subscription1 rather than an existing resource group. The required Azure Resource Manager action is the resource-group write operation, represented by `Microsoft.Resources/subscriptions/resourceGroups/write`. The Contributor role includes permissions to create and manage Azure resources, including resource groups, within its assigned scope. Because Admin3 is assigned Contributor at the Subscription1 scope, that permission applies to resource groups created in Subscription1. Therefore, the correct selection for creating RG2 is **Admin3 only**.

Managing permissions on RG1 means creating, changing, or removing Azure RBAC role assignments at the RG1 scope. This requires permission to manage authorization role assignments, such as `Microsoft.Authorization/roleAssignments/write`. The Owner role provides full management permissions for the assigned scope, including the ability to grant access. Admin4 has the Owner role directly on RG1, so Admin4 can manage RG1 permissions. User Access Administrator is specifically intended to manage user access to Azure resources. Admin1 has that role at the Tenant Root Group scope. Azure RBAC assignments inherit from parent scopes to child management groups, subscriptions, resource groups, and resources. Since RG1 is beneath that root scope, Admin1's access-management permission applies to RG1 as well. Consequently, the correct selection for managing RG1 permissions is **Admin1 and Admin4 only**.

For more detail, see Microsoft's documentation for Azure built-in roles and Azure RBAC scope and inheritance.

QUESTION NO: 26

You have an Azure subscription that contains as 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: B C

Explanation:

Azure Files and **Blob storage** support Azure Storage encryption with customer-managed keys stored in Azure Key Vault. Azure Storage always encrypts data at rest, using data encryption keys that are themselves protected by either Microsoft-managed keys or customer-managed keys. When a customer-managed key is configured for a storage account, Azure Storage uses the key from the associated Key Vault to protect the encryption keys used for supported data services.

For Azure Files, this enables file-share data at rest to be encrypted under an organization-controlled key. For Blob storage, the same capability protects blob data, including block blobs, append blobs, and page blobs, with the storage account's configured customer-managed key. This arrangement provides control over key lifecycle operations such as rotation, disabling a key, revoking access, and auditing key use through Azure Key Vault. The storage account must also have appropriate permissions to access the key, typically through a managed identity and either Azure RBAC or a Key Vault access policy.

Microsoft's Azure Storage customer-managed key documentation identifies Azure Blob storage and Azure Files as the supported services for this storage-account encryption scenario. See Customer-managed keys for Azure Storage encryption and Azure Storage encryption for data at rest.

QUESTION NO: 27

You manage a network with 10 virtual machines (VMs) located within a single subnet, which is protected by a single Network Security Group (NSG). Your objective is to log the network traffic of these VMs to an Azure Storage account.

What are the two actions you should take to accomplish this task? Each correct answer contributes to the solution.

NOTE: Each correct choice is worth one point.

A. Install the Network Performance Monitor solution.

B. Enable Azure Network Watcher.

C. Enable diagnostic logging for the NSG.

D. Enable NSG flow logs.

E. Create an Azure Log Analytics workspace.

ANSWER: B D

Explanation:

Enable Azure Network Watcher and **Enable NSG flow logs** are the required actions. Network Watcher provides the network-monitoring capabilities used to configure and manage NSG flow logging in the Azure region that contains the NSG. The service must be available before flow-log collection can be configured for that NSG.

NSG flow logs record IP traffic that is processed by an NSG, including key flow information such as source and destination addresses, ports, protocol, direction, and the NSG rule decision. Because the subnet's VMs are covered by one NSG, enabling flow logs on that NSG captures the relevant traffic evaluation for the protected subnet. During configuration, the flow-log destination is an Azure Storage account, where Azure writes the generated log data to blobs for retention and later analysis.

Microsoft documents NSG flow logs as a Network Watcher capability and describes the Storage account destination in its configuration guidance. See NSG flow logs overview and Configure NSG flow logs. Note that for new designs, Microsoft recommends evaluating virtual network flow logs as the successor capability where applicable.

QUESTION NO: 28

You need to create an Azure Key Vault using PowerShell and ensure that deleted objects are retained for a specified period of 90 days. Which two parameters should you use to meet this requirement? (Choose two.)

A. EnabledForDeployment

B. EnablePurgeProtection

C. EnabledForTemplateDeployment

D. EnableSoftDelete

E. SoftDeleteRetentionInDays

ANSWER: B E

Explanation:

`SoftDeleteRetentionInDays` is the parameter that explicitly sets the Key Vault soft-delete retention interval. Setting it to `90` configures the maximum supported retention duration, during which deleted keys, secrets, and certificates remain available for recovery. Soft delete is enabled by default for newly created Azure Key Vaults, so the retention value is the relevant configuration for specifying the required 90-day period.

`EnablePurgeProtection` complements that retention setting by preventing a soft-deleted vault object from being permanently purged before its soft-delete retention period has elapsed. This is important when the requirement is to ensure that deleted objects are actually retained for the full period, including protection from an intentional or accidental purge. Purge protection can be enabled when the vault is created and cannot be disabled afterward. Together, a retention value of 90 days and purge protection provide recoverability throughout the required period and prevent early permanent deletion. Microsoft documents the soft-delete and purge-protection behavior in the Azure Key Vault soft-delete overview and exposes both settings through New-AzKeyVault.

QUESTION NO: 29

You have an Azure subscription that includes an Azure SQL Database logical server named SQL1 and an Azure virtual machine named VM1, which only has a private IP address.

The Firewall and virtual network settings for SQL1 are displayed in the exhibit below:

To enable VM1 to establish a connection with SQL1 using the least privilege principle, what configuration should you implement?

A. Add an existing virtual network.

B. Set Connection Policy to Proxy.

C. Create a new firewall rule.

D. Set Allow Azure services and resources to access this server to Yes.

ANSWER: A

Explanation:

Add an existing virtual network. This configuration creates a virtual network rule for the Azure SQL logical server and authorizes the specific subnet that contains VM1. The subnet must have the `Microsoft.Sql` service endpoint enabled (or Azure can enable it as part of configuring the rule, where supported). When VM1 connects to SQL1, Azure SQL validates that the traffic originates from the approved virtual network subnet, allowing access without requiring VM1 to have a public IP address.

This is a least-privilege configuration because the permitted scope is limited to a selected subnet rather than a broad set of Azure resources or an internet-facing IP range. Virtual network service endpoint rules provide a secure path over the Azure backbone for resources in the configured subnet to reach the logical server's public endpoint. The rule is configured on the SQL logical server in the networking settings by selecting the existing virtual network and the subnet used by VM1. Microsoft documents virtual network rules as a method for allowing Azure SQL Database access from specified virtual network subnets and recommends restricting network access to only the required networks. See Azure SQL Database network access controls and virtual network service endpoint rules for Azure SQL Database.

QUESTION NO: 30

You have an Azure subscription that includes a resource group named RG1 and several network security groups (NSGs) as listed in the following table:

[IMAGE_1_OCR_EXTRACTED_TEXT_START]

```
Name   Location     Flow logs status
NSG1   West Europe  Off
NSG2   West Europe  Off
```

[IMAGE_1_OCR_EXTRACTED_TEXT_END]

You implemented an Azure policy depicted in the following exhibit:

[IMAGE_2_OCR_EXTRACTED_TEXT_START]

```
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
```

[IMAGE_2_OCR_EXTRACTED_TEXT_END]

What outcome will occur upon assigning the policy to NSG1 and NSG2?

A. Flow logs will be enabled for NSG1 and NSG2.

B. Flow logs will be enabled for NSG2 only.

C. Flow logs will be disabled for NSG1 and NSG2.

D. Flow logs will be enabled for NSG1 only.

E. Flow logs will remain disabled for NSG1 and NSG2, and NSG2 will be reported as non-compliant.

ANSWER: E

Explanation:

Flow logs will remain disabled for NSG1 and NSG2, and NSG2 will be reported as non-compliant. The assignment scope is RG1, which includes both network security groups, but NSG1 is explicitly listed as an exclusion. Azure Policy exclusions remove the specified resource from the effective scope of an assignment. Therefore, NSG1 is not evaluated by this policy assignment and receives no compliance result from it.

NSG2 remains in the effective assignment scope. Its flow logs are off, while the assigned definition audits whether flow logs are enabled for each network security group. The configured **Audit** effect evaluates the resource and records a non-compliant result when the policy condition is not met. Audit does not alter the resource configuration, deploy a flow-log configuration, or otherwise remediate the resource. Consequently, the current flow-log setting for NSG2 remains off while its compliance state is reported as non-compliant. Although the assignment creates a managed identity, no remediation task is created, and the Audit effect itself does not use that identity to make changes. Microsoft documents policy effects, including Audit behavior, at Azure Policy effects. Assignment scopes and excluded scopes are described in Azure Policy assignment structure.

QUESTION NO: 31

You have an Azure Kubernetes Service (AKS) cluster intended to connect with an Azure Container Registry.

To facilitate this connection, you need to utilize the automatically generated service principal from the AKS cluster for authentication with the Azure Container Registry.

Which resource should you create to achieve this?

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:

A role assignment is required because the automatically generated AKS service principal must be authorized to access the Azure Container Registry through Azure role-based access control (Azure RBAC). For an AKS cluster to pull container images, the appropriate identity—typically the kubelet identity for current AKS configurations—needs the built-in *AcrPull* role

assigned at the registry scope. This assignment establishes the required relationship between the AKS identity and the registry, allowing Azure Container Registry to issue authorization for image-pull operations without storing registry usernames or passwords in Kubernetes secrets.

Azure provides the `az aks update --attach-acr` workflow to configure this integration. That operation creates the necessary registry role assignment for the AKS identity, provided the operator has sufficient permissions to create role assignments. This is the recommended least-privilege approach because *AcrPull* grants read access needed for downloading images while keeping authorization centrally managed and auditable through Azure RBAC. Microsoft documents both the AKS-to-ACR integration process and the permissions granted by the built-in container registry roles at AKS and Azure Container Registry integration and Azure Container Registry roles and permissions.

QUESTION NO: 32

You have an Azure subscription named Sub1 that is linked to an Azure Active Directory (Azure AD) tenant named contoso.com. An administrator, Admin1, has access to various identities. You intend to utilize the Azure Account Center to reassign the ownership of Sub1 to Admin1. Which accounts are eligible for transferring 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: D

Explanation:

contoso.com, fabrikam.com, Hotmail, and OpenID-enabled user account is correct. The Azure Account Center ownership-transfer process is based on the subscription's Account Administrator or billing-owner identity, rather than being limited to users in the subscription's current Microsoft Entra tenant. An ownership transfer can be initiated for an Azure account that uses a work or school identity, such as identities in contoso.com or fabrikam.com, as well as a Microsoft account identity such as Hotmail. Azure also supports OpenID Connect-based identities for Azure account sign-in scenarios, so an OpenID-enabled user account can be used where it is a valid Azure account and can receive and accept the ownership-transfer invitation. The receiving identity must be able to complete the transfer process, including accepting the request and providing any required billing information. After the billing ownership transfer is complete, subscription access and resource administration are managed separately through Azure role-based access control and the applicable Microsoft Entra tenant association. Microsoft's subscription transfer guidance describes the billing ownership transfer workflow and acceptance requirements: Transfer billing ownership of an Azure subscription. For the distinction between subscription administrator and Azure RBAC access, see Azure roles, Microsoft Entra roles, and classic subscription administrator roles.

QUESTION NO: 33

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:

Group Owners. is the appropriate reviewer setting when the people responsible for the resource must perform the access review. For an access review whose resource is a group, the group's owners are the resource owners and are therefore the appropriate reviewers to attest whether each user should retain membership. This assignment avoids requiring a central administrator to have detailed knowledge of every member's continuing business need. Group owners receive the review task and can approve or deny members' continued access based on their ownership and operational knowledge of the group. Azure access reviews support assigning review responsibility to resource owners for group-based reviews, enabling access decisions to be made by the individuals accountable for the resource. In the terminology used by the question's access review configuration experience, selecting **Group Owners.** directly satisfies the requirement that resource owners review access. Microsoft's current access review documentation likewise describes using group owners as reviewers for reviews of group membership, including controls for the case where a group has no owners. See Create an access review of groups or applications and Manage access reviews.

QUESTION NO: 34

You have an Azure Active Directory (Azure AD) tenant with several deleted objects, as shown in the table below:

On May 4, 2020, you attempt to restore the deleted objects using the Azure Active Directory admin center.

Which two objects can you restore? Each correct answer represents a complete solution.

Note: Each correct selection is worth one point.

A. Group1

B. Group2

C. User2

D. User1

ANSWER: B C

Explanation:

Group2 and **User2** can be restored because they are eligible soft-deleted Microsoft Entra ID directory objects that remain within the applicable 30-day retention window as of May 4, 2020. When a user is deleted in Microsoft Entra ID, the user is moved to the deleted-users area rather than being immediately and irreversibly removed. An administrator can restore that user during the retention period, which restores the directory account and its associated identity properties. Microsoft 365 groups are also soft-deleted and can be restored during their 30-day recovery period. Restoring an eligible deleted Microsoft 365 group restores the group and its connected Microsoft 365 resources, subject to the documented behavior for those resources. The relevant determining factors are the object type and whether the deletion date falls within the supported recovery period on the date restoration is attempted. In this scenario, Group2 and User2 satisfy those requirements on May 4, 2020. See Restore or remove recently deleted users and Restore a deleted Microsoft 365 group.

QUESTION NO: 35

Your company owns an Active Directory forest with a single domain named weylandindustries.com, as well as an Azure Active Directory (Azure AD) tenant with the same name. After synchronizing all on-premises identities to Azure AD, you have been informed that users whose givenName attribute begins with 'LAB' should not be synced to Azure AD. What action should you take to achieve this?

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. B. 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:

You should make use of the Synchronization Rules Editor to create an attribute-based filtering rule. Azure AD Connect Sync supports advanced, attribute-based filtering through custom synchronization rules created in the Synchronization Rules Editor. This is appropriate when the organization must exclude individual directory objects according to attribute content rather than according to an entire domain or organizational unit.

A custom inbound synchronization rule can evaluate the on-premises `givenName` value and mark users whose value begins with `LAB` as filtered from the cloud, preventing those user objects from being exported to Microsoft Entra ID. In practice, this is commonly implemented by setting the metaverse `cloudFiltered` attribute through a transformation expression in a higher-precedence custom rule. The rule should be created as a custom rule rather than by modifying Microsoft-provided default rules, so that the configuration remains maintainable and is not overwritten by later upgrades. After the rule is added, a full synchronization cycle is required for the filter to be applied to already-synchronized users. Microsoft documents custom synchronization rules and attribute-based filtering in its Azure AD Connect Sync guidance: Microsoft Entra Connect Sync advanced configuration and Microsoft Entra Connect Sync filtering.

QUESTION NO: 36

You have a Microsoft Entra tenant that uses Privileged Identity Management (PIM) for Azure resource roles.

You need to grant User1 the Contributor role for a resource group. User1 must not have permanent access to the role, and User1 must perform multifactor authentication whenever the role is activated.

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

NOTE: Each correct selection is worth one point.

A. Create an eligible Contributor role assignment for User1.

B. Require multifactor authentication on activation for the Contributor role.

C. Create an active permanent Contributor role assignment for User1.

D. Require justification on activation only.

E. Assign User1 the Owner role for the subscription.

ANSWER: A B

Explanation:

You should create an **eligible** assignment for the Contributor role. An eligible assignment does not grant active permissions until the user activates the role through PIM. This minimizes standing privilege while allowing the user to obtain the required role when necessary.

You should configure the role activation settings to require multifactor authentication. PIM evaluates the activation requirements when User1 requests activation, ensuring that the role is not activated until the MFA requirement is met. A permanent active assignment would provide standing access, and requiring approval alone does not meet the MFA requirement. See Assign Azure resource roles in Privileged Identity Management and Configure Azure resource role settings in Privileged Identity Management.

QUESTION NO: 37

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: A B

Explanation:

Role assignments at the subscription level are lost because associating a subscription with a different Microsoft Entra ID tenant changes the directory that Azure uses as the identity and trust boundary for that subscription. Role assignments refer to users, groups, service principals, and managed identities from the original tenant. Those tenant-specific principals cannot be used as the same identities in the destination tenant, so access must be re-created by assigning appropriate Azure roles to identities in the new tenant. Subscription administrators should plan this access recovery before changing the directory association.

Virtual machine managed identities are lost because managed identities depend on service-principal objects in the Microsoft Entra tenant. A system-assigned managed identity is created for a specific Azure resource and is represented in the tenant; after the subscription changes directories, that identity relationship is no longer available for workloads in the destination tenant. Applications running on affected virtual machines may therefore need replacement managed identities and newly configured permissions, such as Azure RBAC assignments or access policies, before they can again access protected Azure services. Microsoft documents the directory-change effects and the tenant-scoped nature of identity access in Transfer an Azure subscription to a different Microsoft Entra directory and Managed identities for Azure resources overview.

QUESTION NO: 38

You have an Azure subscription that contains an Azure Firewall named Firewall1 and an Azure Log Analytics workspace named Workspace1.

You need to ensure that Firewall1 network rule and application rule events are available for Kusto Query Language (KQL) queries in Workspace1.

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

NOTE: Each correct selection is worth one point.

A. Create a diagnostic setting for Firewall1.

B. Select Workspace1 as the destination of the diagnostic setting.

C. Enable NSG flow logs for the AzureFirewallSubnet subnet.

D. Enable Azure DDoS Protection for the virtual network.

E. Create a route table for the AzureFirewallSubnet subnet.

ANSWER: A B

Explanation:

You must create a diagnostic setting for Firewall1 and select the relevant Azure Firewall log categories. Diagnostic settings control the export of platform logs from an Azure resource. Selecting the network rule and application rule log categories makes the corresponding firewall events available for export.

You must also configure Workspace1 as the destination of the diagnostic setting. Azure Monitor then sends the selected log data to the workspace, where it can be queried by using KQL and used by Azure Monitor alerts or Microsoft Sentinel analytics rules. Enabling Network Watcher or creating an NSG flow log does not collect Azure Firewall rule logs. See Azure Firewall logs and metrics and Diagnostic settings in Azure Monitor.

QUESTION NO: 39

You have an Azure subscription named Subscription1, which includes the resources displayed in the following table.

The table contains the initiatives and policies along with their respective categories:

Your task is to determine which initiatives and policies can be incorporated into Subscription1 via the 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: B

Explanation:

Initiative1 only is correct because Azure Security Center, now Microsoft Defender for Cloud, uses Azure Policy initiatives to define and apply a subscription's security policy. An initiative is a policy set: it groups related Azure Policy definitions so that security controls can be assigned, assessed, and reported as one security policy. In the table, Initiative1 is the initiative categorized for Security Center, making it available for incorporation through the Security Center security-policy experience.

Individual Azure Policy definitions are not added directly as the Security Center security policy in this workflow. When custom controls are needed, the supported approach is to create or use an Azure Policy initiative containing the required policy definitions and assign that initiative. This lets Defender for Cloud evaluate the combined controls and surface the associated security posture and recommendations at the subscription scope. Microsoft documents that custom security policies in Defender for Cloud are based on Azure Policy initiatives and can be assigned to subscriptions or management groups.

For further details, see Create custom security policies in Microsoft Defender for Cloud and Azure Policy initiative definition structure.

QUESTION NO: 40

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:

In Azure Key Vault, create an access policy. An application registration has a corresponding service principal in the Microsoft Entra ID tenant, and that security principal must be authorized to access Key Vault data. With a vault configured to use the vault access-policy permission model, an access policy identifies the application's service principal and assigns the required secret permissions. To allow the application to retrieve Secret1, grant at least the `Get` secret permission. The application can then obtain a Microsoft Entra ID access token and use its application identity to request the secret from Vault1. Key Vault evaluates the request against the configured access policy before returning the secret value. Access policies control data-plane operations on Key Vault objects, including secrets, rather than merely granting management access to the Azure resource. Microsoft documents how to assign a Key Vault access policy to an application or service principal at Assign a Key Vault access policy. For the permissions required to read secret values and the general secret model, see Azure Key Vault secrets.

QUESTION NO: 41

You have a multi-cloud environment that contains the following resources:

• An Azure subscription

• A Google Cloud Platform (GCP) project

• An Amazon Web Services (AWS} account

You need to use Microsoft Defender for Cloud to assign a regulatory standard that will improve the security posture. Which regulatory standard can be applied to all cloud environments?

A. Center for Internet Security (CIS)

B. NIST 800-53

C. System and Organization Controls (SOC) 2 Type 2

D. ISO 27001

ANSWER: D

Explanation:

ISO 27001 is the appropriate regulatory standard because it is an internationally recognized information security management standard that Microsoft Defender for Cloud can use as a compliance initiative across connected Azure, AWS, and GCP environments. Assigning the standard enables Defender for Cloud to evaluate the resources in each connected cloud against the security controls and assessments mapped to ISO 27001. The resulting compliance view helps an organization identify unmet controls, prioritize remediation work, and monitor its security posture consistently despite operating resources across different cloud providers. This is especially useful in a multi-cloud environment because ISO 27001 provides a common governance and information-security baseline rather than being tied to only one provider's native security service. Defender for Cloud's regulatory compliance experience presents supported standards, their controls, and the related assessment results so security teams can track progress toward the selected standard. Microsoft documents the supported standards and their availability in the regulatory compliance standards reference and explains how to use the regulatory compliance dashboard to monitor compliance posture.

QUESTION NO: 42

You have an Azure subscription that includes the resources listed 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 allow ServerAdmins to perform the following task: Create a virtual machine in the existing virtual network located in RG2 only. The solution must adhere to the principle of least privilege.
Which two role-based access control (RBAC) roles should you assign to the ServerAdmins group? Each correct answer is part of the needed solution.
NOTE: Each correct selection is worth one point.

A. the Contributor role for the subscription

B. the Network Contributor role for RG2

C. A custom RBAC role for the subscription

D. a custom RBAC role for RG2

E. the Network Contributor role for RG1.

F. the Virtual Machine Contributor role for RG1.

ANSWER: B F

Explanation:

The **Virtual Machine Contributor role for RG1.** supplies the permissions needed to create and manage virtual machines in the resource group designated for virtual machines. This role includes the required Microsoft.Compute permissions and the related network-interface operations that are used as part of VM provisioning. Assigning it only at RG1 limits the group's compute-management access to the intended VM resource group rather than extending that access across the subscription.

The **Network Contributor role for RG2** provides the network-resource permissions needed to use the existing virtual network in RG2 during deployment. In particular, VM deployment requires access to the target virtual network and subnet so that the VM's network interface can be associated with that subnet. Its RG2 scope confines network administration permissions to the resource group containing the approved virtual network. Together, these assignments separate compute permissions from network permissions and scope each assignment to the applicable resource group, meeting the stated least-privilege requirement without granting subscription-wide Contributor access. Microsoft documents the permissions included in these built-in roles in Azure built-in roles. For the access required when connecting resources to a subnet, see Manage Azure virtual network subnets.

QUESTION NO: 43

You have an Azure subscription that contains the resources shown in the following table. You create an Azure DDoS Protection plan named DDoS1 in the West US Azure region. Which resources can you add to DDoS1?

Name	Type	Location
VNet1	Virtual network	West US
VNet2	Virtual network	East US
WebApp1	Web app	West US

A. VNetl1only

B. WebApp1 only

C. VNet1 and VNet2 only

D. VNet1 and WebApp1 only

E. VNet1, VNet2, and WebApp1

ANSWER: C

Explanation:

VNet1 and VNet2 only is correct. Azure DDoS Protection Network Protection is configured by associating an Azure DDoS Protection plan with virtual networks. The plan provides protection for eligible public IP address resources deployed in those protected virtual networks. The plan is not restricted to virtual networks in the region selected when the plan resource was created; a single plan can be associated with virtual networks in multiple Azure regions, provided the applicable subscription and tenant requirements are met. Therefore, both virtual networks in the subscription can be associated with DDoS1, including a virtual network outside West US.

The web app is not a resource that can be directly associated with an Azure DDoS Protection plan. DDoS Network Protection is applied at the virtual-network level rather than by attaching the plan to an individual Azure App Service resource. Associating the plan with VNet1 and VNet2 is consequently the applicable configuration for this scenario. For details on how Azure DDoS Protection is enabled on virtual networks and how plans can protect virtual networks across regions, see Azure DDoS Protection overview and Manage Azure DDoS Protection.

QUESTION NO: 44

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: B E

Explanation:

Image2 and **Image5** will be scanned. The Azure Security Center container-registry vulnerability-scanning capability described in this question scans supported Linux container images when they are pushed to an Azure Container Registry. Image2 is a Linux image pushed after vulnerability scanning was enabled, so it is eligible for assessment. Image5 is also eligible because it is a modified version of the Linux image that is pushed as a new image. A modification and subsequent push creates image content that must be assessed independently; vulnerability results are associated with the image artifact and its digest rather than being inherited merely because the image originated from another image.

This behavior supports continuous assessment of container workloads: each newly pushed supported Linux image can be evaluated against the vulnerability intelligence used by Defender for Cloud, allowing findings to be surfaced for the specific artifact that could be deployed. Microsoft's Defender for Containers documentation describes registry image vulnerability assessment as part of container security posture and workload protection. See Microsoft Defender for Containers overview and vulnerability assessment for container images.

QUESTION NO: 45

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:

No is correct. An Azure Resource Graph is designed to query Azure Resource Manager resources efficiently across subscriptions and management groups. It can help inventory resources, identify configuration states, and analyze resource data, but it does not combine Azure Policy definitions into a deployable policy group. The Azure Policy construct intended for grouping multiple policy definitions is an *initiative definition*, also known as a policy set definition. An initiative provides a single object containing several individual policy definitions, allowing the organization to manage and assign those definitions together consistently.

To apply the grouped policies to all three subscriptions, the initiative assignment should be created at the management group scope, provided that the three subscriptions belong to that management group. Azure Policy inheritance then causes the assignment to apply to resources in the descendant subscriptions. This is an effective approach for centralized security governance and aligns with how policy controls can be consistently applied in Defender for Cloud environments. Creating a Resource Graph does not provide the required grouping or deployment capability, so the proposed solution does not meet the stated goal. See Azure Policy initiative definitions and Azure management groups.

QUESTION NO: 46

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. 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 is correct. Microsoft Entra Password Protection evaluates passwords against both the Microsoft global banned-password list and the tenant's custom banned-password list when custom-list enforcement is enabled. Its evaluation is intentionally resilient to simple attempts to bypass a banned word. Before checking a password, the service normalizes common character substitutions, including number and symbol substitutions used in leetspeak. Therefore, *C0nt0s0*, *F@brikamHQ*, and *Pr0duct123* are evaluated as variants of the relevant banned terms rather than as entirely distinct strings.

Password Protection also uses a scoring process. A password containing a banned term is not automatically acceptable merely because extra characters have been appended. The remaining characters must provide sufficient non-banned complexity to meet the required score. The short suffixes in these attempted passwords do not provide enough score after the banned terms are identified. Consequently, each of the three self-service password reset attempts is rejected by the configured Password Protection policy.

Microsoft documents password normalization, custom banned-password enforcement, and the scoring approach in Microsoft Entra Password Protection and Custom banned password list configuration.

QUESTION NO: 47

You are managing a Microsoft 365 tenant that employs Azure Active Directory (Azure AD), which is synchronized with your on-premises Active Directory domain using Azure AD Connect. Recently, you created a new Azure subscription. However, you notice that the synchronized on-premises user accounts are unable to receive roles in this new subscription. To enable

the assignment of Azure and Microsoft 365 roles to these synced Azure AD user accounts, what is the first step you should take?

A. Change the Azure AD tenant used by the new subscription.

B. Configure the Azure AD tenant used by the new subscription to use pass-through authenticate

C. Configure the Azure AD tenant used by the new subscription to use federated authentication.

D. Configure a second instance of Azure AD Connect.

ANSWER: A

Explanation:

Change the Azure AD tenant used by the new subscription. An Azure subscription has a trust relationship with one Microsoft Entra ID tenant, formerly called Azure AD. Azure RBAC role assignments for that subscription are made to security principals in its associated tenant. Therefore, the synchronized users must be present in the same tenant to be selected and assigned subscription, resource-group, or resource-level Azure roles. Likewise, Microsoft 365 and Microsoft Entra directory roles are managed in the tenant containing the relevant user objects.

Azure AD Connect synchronizes on-premises identities into a specified Entra tenant; it does not make those users automatically available in a separate tenant associated with another subscription. The first remediation step is consequently to move or associate the new subscription with the tenant into which the on-premises directory is synchronized. Once the subscription uses that tenant, administrators can assign the synced accounts the appropriate Azure RBAC roles and, where required, directory roles. Microsoft documents how subscriptions are associated with and transferred between directories, as well as the tenant-scoped identity model used by Azure RBAC. See Transfer an Azure subscription to a different Microsoft Entra directory and Azure role-based access control overview.

QUESTION NO: 48

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:

No is correct because, although Active Directory Federation Services (AD FS) can authenticate users against on-premises Active Directory at sign-in time, deploying federation does not reduce the required server infrastructure. An AD FS deployment generally requires federation servers and, for users connecting from outside the corporate network, Web Application Proxy servers. High availability commonly requires multiple instances of these roles, together with supporting load-balancing, certificates, monitoring, and maintenance processes.

The stated goal requires a design that both preserves the effect of on-premises password policies and sign-in restrictions and minimizes the number of servers. AD FS is an infrastructure-intensive federation solution and therefore fails the server-reduction part of that combined requirement. Microsoft's hybrid identity guidance recommends selecting federation only

when an organization has a specific federation requirement that cannot be met through the simpler managed authentication approaches. Azure AD Connect supports these hybrid identity configurations, but AD FS introduces an additional on-premises authentication service tier rather than minimizing it.

See Microsoft's guidance for choosing an authentication method and its Azure AD Connect overview.

QUESTION NO: 49

You have an Azure subscription named Sub1 that utilizes Microsoft Defender for Cloud. The subscription is organized in a management group hierarchy as depicted in the following exhibit.

![Management Group Hierarchy](IMAGE_1_URL)

The following table lists the definitions that have been created:

![Definitions Table](IMAGE_2_URL)

You aim to establish a security policy using Defender for Cloud. Which of the following definitions can be used as a security policy?

A. Policy1 only

B. Policy1 and Initiative1 only

C. Initiative1 and Initiative2 only

D. Initiative1, Initiative2, and Initiatives only

E. Policy1, Initiative1, Initiative2, and Initiative3

ANSWER: C

Explanation:

Initiative1 and Initiative2 only is correct. Microsoft Defender for Cloud implements security policies by using Azure Policy initiative definitions, also called policy set definitions. An initiative groups one or more individual Azure Policy definitions and can be assigned to a management group or subscription. This grouping is what enables Defender for Cloud to assess a coordinated set of security controls and generate the related recommendations and compliance results for the resources within the assigned scope.

For Sub1, an initiative can be used when it is available at Sub1's scope or at a management-group scope inherited by Sub1. Azure Policy definitions and initiative definitions created at a management group are available for assignment to that management group and its descendant management groups and subscriptions. Therefore, the applicable initiative definitions in the depicted hierarchy are Initiative1 and Initiative2. Defender for Cloud can use either of these initiatives as the basis for the subscription's security policy.

For more information, see Security policies in Microsoft Defender for Cloud and Azure Policy initiative definition structure.

QUESTION NO: 50

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: A E

Explanation:

To configure Google as an identity provider, configure **a client ID** and **a client secret**. These values are obtained by creating an OAuth 2.0 application/client in Google Cloud. The client ID identifies the Google application registration that represents the relying application in the Google authorization flow. The client secret is the confidential credential used with that client registration when the authorization flow exchanges an authorization code for tokens.

During the Google application registration process, the required redirect URI is also configured in Google Cloud so that Google can return the authentication response to the Microsoft Entra external identity service. After the Google client credentials are entered in the Entra identity-provider configuration, the application can offer Google as a sign-in choice alongside Microsoft identities. This establishes the trust needed for Entra to redirect users to Google for authentication and process the resulting identity assertion.

Microsoft documents that Google federation configuration requires the client ID and client secret generated in Google Cloud. See Google federation in Microsoft Entra External ID and Identity providers in Microsoft Entra External ID.

QUESTION NO: 51

You need to implement the planned change for SQLdb1.

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

NOTE: Each correct selection is worth one point.

A. Create a compliance policy.

B. Configure Microsoft Entra authentication for SQLServer1.

C. Create a Conditional Access policy.

D. Configure a user-assigned managed identity for SQLdb1.

E. Configure Federated client identity for SQLdb1.

ANSWER: B C

Explanation:

Configuring Microsoft Entra authentication for SQLServer1 is required to enable Microsoft Entra identities to authenticate to databases hosted by that Azure SQL logical server. An administrator must configure a Microsoft Entra admin for the logical server before Microsoft Entra users and groups can be created and used in the database. This establishes the identity-based authentication foundation for SQLdb1 rather than relying solely on SQL authentication credentials.

Creating a Conditional Access policy is the corresponding control for enforcing Microsoft Entra sign-in requirements, such as multifactor authentication, compliant devices, sign-in risk controls, or location-based access conditions. Conditional Access is evaluated by Microsoft Entra ID during token issuance. Therefore, once clients connect to SQLdb1 by using Microsoft Entra authentication, the applicable Conditional Access policy can govern those sign-ins. Together, these actions enable Microsoft Entra-based database access and apply the required organizational access controls to that access. See Configure Microsoft Entra authentication for Azure SQL Database and Microsoft Entra Conditional Access overview.

QUESTION NO: 52

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: C D

Explanation:

AcrPush and **AcrImageSigner** provide the minimum combination of registry data-plane permissions required to publish a trusted image. AcrPush authorizes User1 to push container images and other supported artifacts into ContReg1. Publishing the image manifest and layers is a necessary part of making an image available in the registry.

With content trust enabled, image publishing also requires a trusted signature so that clients can validate the publisher and image integrity. AcrImageSigner grants the permissions needed to create and manage the image signatures used by Azure Container Registry content trust. Assigning both roles therefore lets User1 upload image content and sign that content, without granting unrelated registry-management, subscription-management, or broad resource permissions.

These built-in roles can be assigned at the scope of ContReg1, further limiting User1's access to only the target registry. Microsoft documents AcrPush as the built-in role for pushing and pulling registry artifacts, while AcrImageSigner is the built-in role intended for signing images when using content trust. See Azure Container Registry roles and permissions and Content trust in Azure Container Registry.

QUESTION NO: 53

You have an Azure subscription and you reconfigure it to use a different Azure Active Directory (Azure AD) tenant. What are two possible outcomes of this configuration change? Select two options that describe complete solutions. 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: A B

Explanation:

Role assignments at the subscription level are lost because Azure RBAC assignments are tied to security principals in the Microsoft Entra ID tenant associated with the subscription. When the subscription is moved to another tenant, identities such as users, groups, and service principals from the original tenant do not exist as equivalent principals in the destination tenant. Access must therefore be planned and re-created by assigning appropriate roles to identities in the new tenant. Microsoft specifically recommends ensuring that an appropriate administrator account exists in the destination directory so access can be restored after the directory change.

Virtual machine managed identities are lost because a managed identity is backed by a service principal in the tenant. A system-assigned managed identity belongs to the original directory association; after the subscription is associated with a different tenant, identity-dependent permissions and authentication relationships must be reestablished. Workloads that use the VM identity to access services such as Azure Key Vault, Storage, or Azure SQL need a newly configured identity and corresponding RBAC role assignments or resource access policies in the destination tenant. Review Microsoft's guidance before changing directories: Transfer an Azure subscription to a different Microsoft Entra directory and Managed identities for Azure resources.

QUESTION NO: 54

You have configured your Azure subscription to use an alternative Azure Active Directory (Azure AD) tenant. What are two possible impacts of this 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: A B

Explanation:

Role assignments at the subscription level are lost because Azure role-based access control assignments are tied to security principals in the Microsoft Entra tenant previously associated with the subscription. When the subscription is moved to a different tenant, users, groups, service principals, and their object identifiers from the former tenant cannot be used to provide access in the new tenant. Administrators must therefore re-create the appropriate role assignments for identities in the destination tenant, including ensuring that an administrator has access after the directory change.

Virtual machine managed identities are lost because a managed identity is represented by a service principal in the subscription's associated Microsoft Entra tenant. A system-assigned managed identity is bound to its Azure resource and tenant identity. Following a directory change, that identity cannot continue to function as an identity in the newly associated tenant. Any permissions that depended on it, such as access to Azure Key Vault, storage, or other protected resources, must be restored by configuring a valid identity in the new tenant and assigning the required roles or access policies.

Microsoft documents the effects and required access steps for a subscription directory change in Transfer an Azure subscription to a different Microsoft Entra directory. For the tenant-backed nature of managed identities, see Managed identities for Azure resources overview.

QUESTION NO: 55

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:

An Azure Log Analytics workspace should be created first because it provides the Azure Monitor Logs data store and query environment needed for log-based security detections. The workspace collects and retains monitoring data from configured sources, including Microsoft Entra ID diagnostic logs when those logs are sent through diagnostic settings. It also provides the Kusto Query Language query capability used to identify security-relevant events and patterns, such as unusual sign-in activity, changes to directory objects, or administrative operations.

After the workspace exists, diagnostic settings and other data-collection configurations can route the required logs to it. Azure Monitor scheduled query alert rules can then evaluate queries against that workspace on a recurring schedule and trigger when the defined criteria are met. This establishes the necessary sequence: provision the log repository and analytics boundary, send the relevant telemetry to it, and create alert rules based on that collected data. A workspace can also be organized with retention, access control, and data-collection considerations appropriate for the organization's security-monitoring requirements. See Log Analytics workspace overview and Log alerts in Azure Monitor.

QUESTION NO: 56

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: A D

Explanation:

Blob storage and **Azure Files** support customer-managed keys for Azure Storage encryption. With customer-managed keys, the storage account uses a key that your organization controls in Azure Key Vault or Azure Key Vault Managed HSM as the key-encryption key for encryption at rest. This provides control over key lifecycle operations, including key rotation, disabling a key, and revoking the storage account's ability to use it, while Azure Storage continues to perform the underlying service encryption.

The customer-managed key setting is configured for the storage account and applies to the supported Blob and Azure Files workloads in that account. The storage account must be granted access to the selected vault key, typically through its managed identity and an appropriate Azure RBAC role or Key Vault access configuration. Microsoft documents support for customer-managed keys specifically for Azure Blob storage and Azure Files, as well as the prerequisites and configuration process. See Customer-managed keys for Azure Storage encryption and Configure customer-managed keys with Azure Key Vault.

QUESTION NO: 57

You are tasked with collecting event logs from your Azure virtual machines into an Azure Log Analytics workspace. Subsequently, you intend to generate alerts based on these events. Your objective is to determine which Azure services can

facilitate the creation of these alerts. Can you identify the two services that would fulfill this requirement? Note that each correct selection is worth one point, and you should select two answers to form a complete solution.

A. Azure Monitor

B. Azure Security Center

C. Azure Analytics Services

D. Azure Sentinel

E. Azure Advisor

ANSWER: A D

Explanation:

Azure Monitor can create alerts from event data stored in a Log Analytics workspace. VM event logs can be collected through the Azure Monitor Agent and data collection rules, then queried by Azure Monitor alert rules. In particular, scheduled query rules run Kusto Query Language queries on a defined schedule and evaluate the returned results against alert criteria. When the configured threshold or condition is met, the rule can create an alert and invoke an action group for notification, automation, or incident-management integration. This directly supports operational alerting based on Windows or Linux VM event logs.

Azure Sentinel, now named Microsoft Sentinel, also supports this requirement for security-focused detections. Microsoft Sentinel is deployed on a Log Analytics workspace and uses analytics rules to examine the workspace data. Scheduled analytics rules execute Kusto queries against collected events and generate security alerts when a detection condition is found. These alerts can additionally be grouped into incidents and investigated or automated through security operations workflows. Therefore, both Azure Monitor and Azure Sentinel can generate alerts from VM event logs collected in the Log Analytics workspace. See Azure Monitor alerts overview and Microsoft Sentinel analytics rules.

QUESTION NO: 58

You are addressing a security concern related to an Azure Storage account. Diagnostic logs have been enabled for this storage account. Which tool would you utilize to access and retrieve these diagnostic logs?

A. Azure Storage Explorer

B. SQL query editor in Azure

C. File Explorer in Windows

D. Azure Security Center

ANSWER: A

Explanation:

Azure Storage Explorer is the appropriate tool because it is Microsoft's desktop client for directly accessing data held in Azure Storage accounts. When diagnostic logging data is written to a storage account, an investigator can use Storage Explorer to authenticate to that account and browse the relevant Blob containers or tables where the log artifacts are retained. It supports common Azure Storage authentication methods, including Microsoft Entra ID, shared access signatures, and account keys, subject to the permissions granted. From the Storage Explorer interface, the investigator can locate log files, open or download blobs, and export data for review during incident investigation or retention activities. This provides direct access to the stored diagnostic-log output without requiring an application-specific query interface. Microsoft documents Storage Explorer as a tool for managing and accessing blobs, Azure Data Lake Storage, queues, tables, and files in Azure Storage accounts. The Azure Storage monitoring documentation also describes sending resource logs to a storage account, where they can be retained and accessed as stored data. See the Azure Storage Explorer overview and Monitor Azure Blob Storage.

QUESTION NO: 59

You have an Azure subscription that includes a user named User1 and an Azure Container Registry named ContReg1. You have enabled content trust for ContReg1. What are the two roles you should assign to User1 to ensure they can create trusted images in ContReg1 while adhering to the principle of least privilege?
Each correct answer represents part of the solution, and each correct selection is worth one point.

A. AcrQuarantineReader

B. Contributor

C. AcrPush

D. AcrImageSigner

E. AcrQuarantineWriter

ANSWER: C D

Explanation:

AcrPush and **AcrImageSigner** provide the required permissions while limiting User1 to the actions necessary to publish trusted container images. AcrPush grants data-plane permissions to push and pull container images and associated registry artifacts. This enables User1 to upload the image layers, manifests, and tags that form the image in ContReg1, without granting broad Azure Resource Manager permissions to modify the registry resource or its configuration.

AcrImageSigner grants the permissions required to sign images when Azure Container Registry content trust is enabled. Content trust uses image signing metadata so that clients can verify that a signed image came from a trusted publisher. Combining the image-push permission with the image-signing permission lets User1 both publish an image and create the trust signature needed for that image to be consumed as trusted. The assignment can be scoped directly to ContReg1, further supporting least privilege. Microsoft documents AcrPush and AcrImageSigner as built-in Azure Container Registry roles and identifies AcrImageSigner as the role for signing trusted images. See Azure Container Registry roles and permissions and Content trust in Azure Container Registry.

QUESTION NO: 60

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: A D

Explanation:

Azure Monitor is correct because Azure Monitor alert rules can evaluate data in a Log Analytics workspace by running scheduled log queries. A log search alert rule uses a KQL query to detect matching VM event records and can trigger an

action group when the configured condition is met. This provides the standard Azure platform mechanism for notifications, automation, and incident-response actions based on collected log data.

Azure Sentinel is also correct. Azure Sentinel, now named Microsoft Sentinel, is a security information and event management service that stores and analyzes security data in a Log Analytics workspace. Its analytics rules run KQL queries against workspace data, including events collected from Azure virtual machines, and create alerts and incidents when suspicious or defined conditions are detected. Analytics rules therefore provide a complete security-focused alerting solution over the same event data.

For more information, see Azure Monitor alert types and Microsoft Sentinel analytics rules.

QUESTION NO: 61

You have 50 Azure virtual machines that run Windows Server.

You need to collect Windows event logs from the virtual machines in a Log Analytics workspace by using the Azure Monitor agent.

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

NOTE: Each correct selection is worth one point.

A. Create a data collection rule.

B. Associate the data collection rule with the virtual machines.

C. Configure the Log Analytics agent workspace settings.

D. Create an Azure Automation account.

E. Enable boot diagnostics on the virtual machines.

ANSWER: A B

Explanation:

You must create a **data collection rule** and associate the rule with the virtual machines. A data collection rule defines the data sources to collect, such as Windows event logs, the event log queries or filters, and the Log Analytics workspace destination. The Azure Monitor agent uses the rule to determine which telemetry it must send.

Associating the data collection rule with the virtual machines applies the collection configuration to those machines. The Azure Monitor agent must also be installed on each machine, but a Log Analytics agent workspace configuration is not used for Azure Monitor agent data collection. See Data collection rules in Azure Monitor and Manage the Azure Monitor Agent.

QUESTION NO: 62

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: B C

Explanation:

Cloud application administrator and **Application administrator** are built-in Microsoft Entra roles that can manage application registrations and enterprise applications in the tenant. This scope includes granting tenant-wide admin consent for permissions requested by applications, enabling User1 to approve an application's requested access on behalf of the organization rather than requiring each user to consent individually. These roles are appropriate delegated-administration choices when User1 must administer published applications without receiving the broader privileges of a Global Administrator.

Admin consent is an organization-wide action: it creates or updates the permission grants associated with the application's service principal in the tenant. Assigning either of these application-focused administrator roles gives User1 the necessary app-management authority to perform that workflow. Microsoft notes an important scope limitation: these roles cannot grant tenant-wide consent for Microsoft Graph *application* permissions; a more privileged role is required for that specific scenario. For the general requirement to grant admin consent for published apps, however, either listed role is a complete solution. See Grant tenant-wide admin consent to an application and Microsoft Entra built-in roles and permissions.

QUESTION NO: 63

You have both an on-premises network and an Azure subscription. Consider the following Microsoft SQL Server instances as depicted in the table below:

1. **sql1:** Azure SQL managed instance
2. **sql2:** SQL Server 2019 hosted on an Azure virtual machine running Windows Server 2019
3. **sql3:** SQL Server 2019 hosted on an Azure virtual machine running Red Hat Enterprise Linux (RHEL) 8.3
4. **sql4:** SQL Server 2016 installed on an on-premises physical server running Windows Server 2016

You are planning to deploy Microsoft Defender for SQL. Which of these SQL Server instances are eligible for protection 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:

sql1, sql2, sql3, and sql4 is correct because Microsoft Defender for SQL is designed to protect both Azure SQL offerings and SQL Server instances running on machines. Azure SQL Managed Instance is an Azure SQL platform service covered by Defender for SQL. SQL Server 2019 running on either a Windows Server or RHEL Azure virtual machine can be protected as SQL Server on machines. This protection covers supported SQL Server workloads regardless of whether the host operating system is Windows or Linux.

Protection can also extend beyond Azure. The on-premises SQL Server 2016 installation can be protected after its host is connected to Azure as an Azure Arc-enabled server and the Defender for SQL plan is enabled. Azure Arc provides the required Azure management connection for non-Azure machines, allowing Defender for Cloud to deploy and manage the relevant SQL security capabilities. In each case, Defender for SQL provides security posture management and threat protection capabilities appropriate to the workload and configured plan. See Microsoft Defender for SQL and Enable and configure Defender for SQL.

QUESTION NO: 64

You have an Azure subscription configured with various resources, detailed as follows:

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

Your task is to enable the ServerAdmins to carry out specific operations, adhering strictly to the principle of least privilege. Which two role-based access control (RBAC) roles should you assign to the ServerAdmins group? Each correct selection contributes to part of the complete solution.

NOTE: Every correct response 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: B F

Explanation:

The appropriate least-privilege assignments are **the Virtual Machine Contributor role for RG1** and **the Network Contributor role for RG2**. These assignments use Azure built-in roles and limit each role assignment to the resource group that contains the applicable resource type. Virtual Machine Contributor grants the permissions required to manage virtual machines and their associated VM operations, while avoiding broad permission to manage every resource type in the subscription. Assigning it at the RG1 scope confines those permissions to the resource group used for virtual machines.

Network Contributor is the built-in role intended for management of Azure network resources, including virtual networks and related networking components. Applying that role only at the RG2 scope provides the necessary management capability for the virtual networks stored there, without extending network-management permissions to RG1 or to unrelated resource groups. This combination follows Azure RBAC best practice: use Microsoft-maintained built-in roles when they satisfy the required access, and assign them at the narrowest practical scope. Resource-group-scoped assignments also make access easier to review and maintain as the environment grows. Microsoft documents the permissions and intended use of these roles in Azure built-in roles and explains scope-based access control in the Azure RBAC overview.

QUESTION NO: 65

You have the following Azure virtual machines listed in the table below:

Image:

For which of these virtual machines can Update Management be enabled?

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 is correct because the operating systems shown for those machines meet the supported operating-system prerequisites for the Azure Automation Update Management scenario assessed by this question. Update Management requires a supported Windows Server version or supported Linux distribution, together with the required monitoring/management agent configuration and connectivity to the associated Log Analytics workspace. VM1, VM2, and VM4 can therefore be onboarded, assessed for missing updates, and included in scheduled update deployments.

This question reflects the legacy Azure Automation Update Management service, which relied on Azure Monitor Logs and Automation runbooks. Microsoft has since retired that legacy offering and recommends Azure Update Manager for current patch-management deployments. However, the platform support criteria in the VM table lead to VM1, VM2, and VM4 as the valid set for the service named in the question. For current implementations, Azure Update Manager provides native Azure update management and can also manage eligible Arc-enabled servers. See Azure Update Manager overview and Azure Automation Update Management overview.

QUESTION NO: 66

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: A D E

Explanation:

Azure SQL Managed Instance is deployed into a dedicated subnet within a virtual network. Therefore, because the existing subnet is already used by VM1, a separate subnet must be created for the managed instance. VM1 can then connect to SQL1 privately over the virtual network, subject to the networking rules applicable to the managed-instance subnet.

A network security group (NSG) and a route table are also components of the required managed-instance subnet configuration in the traditional Azure SQL Managed Instance networking model. Azure applies network intent policies to the subnet and requires the NSG and route-table configuration to preserve the inbound, outbound, and routing behavior needed by the managed-instance service. These controls enable required service communications while allowing virtual-network clients such as VM1 to reach the instance through its private endpoint/IP address and configured SQL connectivity ports. The subnet must remain dedicated to the managed instance and be delegated to `Microsoft.Sql/managedInstances`.

For implementation guidance, see Configure a subnet for Azure SQL Managed Instance and Azure SQL Managed Instance connectivity architecture.

QUESTION NO: 67

You are responsible for configuring Advanced Threat Protection for an Azure SQL Database server. This protection must be set up to detect all types of threats. What occurs when an application generates a faulty SQL statement in the database?

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: A

Explanation:

A Potential SQL injection alert is triggered. Microsoft Defender for SQL, formerly called Advanced Threat Protection for Azure SQL, monitors database activity for anomalous and potentially dangerous query behavior. Its threat-detection capabilities include identifying SQL statements whose structure or content resembles a SQL injection attempt. A faulty statement produced by an application can contain malformed syntax, unexpected concatenated input, unmatched quotation marks, or other patterns that are consistent with injection-style payloads. When such activity is observed, Defender for SQL can generate a potential SQL injection security alert so that the security team can review the query details, affected database, source context, and timing to determine whether the activity represents an attack or an application defect. This alerting behavior is valuable even when the source is an internal application, because accidental query-construction errors can be difficult to distinguish from malicious attempts without investigation. Defender for SQL integrates these detections into Microsoft Defender for Cloud, where alerts can be investigated and correlated with other security signals. Microsoft describes Defender for SQL as providing detection for anomalous activities and potential threats to SQL workloads, including SQL injection attempts. See Microsoft Defender for SQL introduction and the Microsoft Defender for Cloud SQL Database alerts reference.

QUESTION NO: 68

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

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: A F

Explanation:

The **Virtual Machine Contributor role for RG1** provides the permissions needed to create and manage virtual machines within RG1. Its permissions include the necessary virtual-machine operations and the ability to create and manage associated network interfaces as part of VM deployment, while its RG1 scope prevents ServerAdmins from creating VMs in other resource groups.

To attach a network interface to a subnet in a virtual network located in RG2, the deployment requires permission on the target subnet, specifically the subnet join operation. A **custom RBAC role for RG2** can grant only the required read permissions for the virtual network and subnet plus `Microsoft.Network/virtualNetworks/subnets/join/action`. Assigning that narrowly scoped custom role at RG2 enables use of the existing networks there without granting broad permission to create, modify, or delete other network resources. This combination separates VM administration in RG1 from the minimal network-attachment permission in RG2 and follows least privilege. See the Virtual Machine Contributor role definition and Azure custom roles documentation.

QUESTION NO: 69

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:

Deploy an Azure Front Door first. An Azure Web Application Firewall policy is enforced only when it is associated with a supported application-delivery service that receives and evaluates web traffic before that traffic reaches the application. Azure Front Door Standard and Premium provide this edge entry point and can apply a WAF policy to incoming HTTP and HTTPS requests. After the Front Door profile and endpoint are deployed, WebApp1 can be configured as an origin, and WAF1 can be associated with the appropriate Front Door domain or route. Requests sent through the Front Door endpoint are then inspected by the policy before they are forwarded to WebApp1. This architecture provides centralized protection for common web threats while allowing the App Service web app to remain the backend application. Microsoft documents that Azure Front Door WAF policies are associated with Azure Front Door resources and protect traffic handled by those resources. For implementation details, see Web Application Firewall on Azure Front Door and Create an Azure Front Door Standard/Premium profile.

QUESTION NO: 70

You have an Azure subscription that includes a storage account containing a blob named blob1.

You need to grant access to user1 to blob1 with the condition that the access should automatically expire after six days. Which method should you implement to achieve this requirement?

A. a shared access policy

B. a shared access signature (SAS)

C. role-based access control (RBAC)

D. a managed identity

ANSWER: B

Explanation:

A shared access signature (SAS) is the appropriate mechanism because it delegates narrowly scoped, time-limited access to Azure Storage resources. A SAS can be generated specifically for `blob1` and configured with only the required permissions, such as read permission. Its signed URI includes an expiry time, which can be set to six days from the time it is issued. Azure Storage validates the SAS on every request and denies requests made after that expiry time, so access ends automatically without requiring an administrator to remove access manually.

For scenarios in which the access recipient should be authenticated through Microsoft Entra ID, a user delegation SAS can be used. This type of SAS is authorized using a user delegation key obtained through Microsoft Entra ID credentials, while retaining the same resource-level permissions and expiry controls. The resulting SAS URL can then be provided to user1 for access to the specified blob during the permitted period. Microsoft recommends user delegation SAS when possible because it avoids signing the SAS with the storage account key. See Grant limited access to Azure Storage resources using shared access signatures and Create a user delegation SAS for a blob.

QUESTION NO: 71

You have an Azure subscription that utilizes Microsoft Defender for Cloud to maintain security protocols. You need to assess your regulatory compliance according to the Azure CIS 1.4.0 standard using Defender for Cloud. The solution should require minimal manual intervention. What is the first step you should take?

A. Assign an Azure policy.

B. Manually add the Azure CIS 1.4.0 standard.

C. Disable one of the Out of the box standards.

D. Add a custom initiative.

ANSWER: A

Explanation:

Assign an Azure policy is the correct first step because Microsoft Defender for Cloud implements regulatory compliance standards through Azure Policy initiatives and assignments. The Azure CIS 1.4.0 benchmark is represented by a built-in compliance standard that can be assigned to the appropriate Azure scope, such as a subscription or management group. This assignment enables the policy definitions associated with the standard to evaluate supported resources automatically and continuously. Defender for Cloud then uses the resulting policy assessment data to populate its Regulatory compliance experience, including the status of controls, affected resources, and remediation information. Assigning the built-in standard avoids the effort and maintenance associated with manually defining individual control checks. It also ensures that compliance evaluation remains ongoing as resources are created or changed within the assigned scope. The assignment should be made at a scope that covers the resources to be assessed, allowing Defender for Cloud to provide centralized compliance visibility with minimal operational intervention. For details on how compliance standards are managed in Defender for Cloud, see Regulatory compliance dashboard in Microsoft Defender for Cloud. For the underlying policy assignment and evaluation model, see Azure Policy overview.

QUESTION NO: 72

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: B F

Explanation:

The required values are **the workspace ID** and **the primary shared key**. In the ARM-template approach used for the Microsoft Monitoring Agent and the Defender for Cloud vulnerability-assessment workflow, the extension settings must identify the Log Analytics workspace that will receive the VM's security and assessment data. The workspace ID is the non-secret identifier that directs the agent to the intended workspace.

The agent must also authenticate when connecting to that workspace. The primary shared key is the workspace authentication key supplied to the agent extension's protected settings. ARM templates commonly retrieve this value at deployment time by using the `listKeys` function against the Log Analytics workspace resource, rather than hard-coding the secret. Together, the workspace ID and primary shared key provide the destination and authentication details needed to deploy and configure the extension consistently across all virtual machines.

Microsoft documents deploying the Log Analytics agent with an ARM template and passing the workspace ID plus key in the extension configuration. See Deploy the Log Analytics agent by using an ARM template and Deploy vulnerability assessment for virtual machines.

QUESTION NO: 73

You have an Azure subscription that includes 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 image:

An app named App1 is planned for deployment.

You need to ensure that User1 can register App1 in Azure AD while adhering to 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:

Application developer in Azure AD is the appropriate least-privileged role for allowing User1 to register App1 when ordinary users are not permitted to create app registrations through the tenant's App registrations user setting. This Microsoft Entra built-in directory role is specifically intended for developers who need to create application registrations. It permits the role holder to create and manage application registrations that they create, including the associated service principals, without providing broad administrative control of all applications in the tenant.

This scope fits the stated requirement because User1 needs to register a planned application, rather than administer existing applications throughout the directory or receive unrelated Azure resource-management permissions. The assignment must be made as a Microsoft Entra directory role; it is not an Azure subscription RBAC assignment. Microsoft documents the Application Developer role's ability to create app registrations and manage applications that the user creates. Microsoft also documents the tenant-level control that determines whether users can register applications and identifies directory roles that can register applications when the general user capability is restricted.

References: Microsoft Entra Application Developer role permissions; Restrict who can create applications in Microsoft Entra ID.

QUESTION NO: 74

You are currently diagnosing a security issue involving an Azure Storage account. You have enabled Azure Storage Analytics logs and configured them to be archived to a designated storage account. What tool should you use to access and retrieve those diagnostic logs?

A. Azure Cosmos DB explorer

B. SQL query editor in Azure

C. AzCopy

D. the Security admin center

ANSWER: C

Explanation:

AzCopy is the appropriate tool because diagnostic log files retained in an Azure Storage account can be retrieved as Azure Storage objects. AzCopy is Microsoft's command-line utility for transferring data to and from Azure Storage, including Blob storage. It can authenticate through Microsoft Entra ID or a shared access signature, list the relevant blob paths, and download selected log files or entire log directories to a local investigation workstation. This makes it suitable for incident-response and troubleshooting workflows where logs need to be collected efficiently, including scripted or repeatable retrieval operations.

Azure Storage Analytics is a legacy logging capability, but its log output is stored in Azure Storage and can therefore be handled with standard Azure Storage data-transfer tools. AzCopy supports copying blobs from a storage account to a local path and supports filtering and recursive operations when a larger set of retained diagnostic files is required. Microsoft recommends AzCopy for high-performance data movement involving Azure Storage. For implementation guidance, see Get started with AzCopy and Storage Analytics logging.

QUESTION NO: 75

You have an Azure subscription that uses Microsoft Entra Privileged Identity Management (PIM) for Azure resource roles.

You need to grant User1 the Contributor role for RG1. User1 must not have permanent access to the role and must perform multifactor authentication whenever the role is activated.

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

NOTE: Each correct selection is worth one point.

A. Create an eligible Contributor assignment for User1 at the RG1 scope.

B. Require multifactor authentication on activation for the Contributor role.

C. Create an active Contributor assignment for User1 at the subscription scope.

D. Assign the Global Administrator role to User1.

E. Create a permanent Owner assignment for User1 on RG1.

ANSWER: A B

Explanation:

You should create an **eligible assignment** for the Contributor role at the RG1 scope. An eligible assignment does not grant active permissions until User1 activates the role through Privileged Identity Management. This limits standing privileged access.

You should also configure the Contributor role activation settings to **require multifactor authentication on activation**. When User1 requests activation, PIM requires the additional authentication step before making the role active for the configured activation duration. An active assignment would provide immediate, ongoing access and would not satisfy the requirement to avoid permanent access. See Assign Azure resource roles in Privileged Identity Management and Configure Azure resource role settings in PIM.

QUESTION NO: 76

You are managing an Azure virtual machine named VM1.

Within the Azure Security Center, you receive a high-severity recommendation stating: "Install endpoint protection solutions on the virtual machine."

Your task is to address the issue that triggered this high-severity recommendation. What action should you take?

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 Advanced Threat Protection (Microsoft Defender ATP).

ANSWER: A

Explanation:

Add the Microsoft Antimalware extension to VM1. This recommendation is generated when Microsoft Defender for Cloud (formerly Azure Security Center) cannot detect a supported endpoint-protection solution on an Azure virtual machine. The Microsoft Antimalware extension is an Azure VM extension that deploys and configures Microsoft antimalware protection on supported Windows virtual machines. It provides real-time protection, scheduled scanning, signature updates, and optional exclusions through extension settings. Once the extension is deployed successfully and the protection solution is detected, VM1 meets the endpoint-protection requirement addressed by the recommendation. VM extensions are appropriate for this task because they provide a centrally managed Azure deployment mechanism and report their provisioning status to the Azure platform. The recommendation is specifically about having endpoint protection installed, so deploying the Microsoft Antimalware extension directly remediates the missing security control. Microsoft documents the endpoint-protection recommendation in its Defender for Cloud recommendations reference and documents deployment and configuration of the Microsoft Antimalware extension for Windows.

QUESTION NO: 77 - (HOTSPOT)

HOTSPOT (Drag and Drop is not supported) (Drag and Drop is not supported)

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

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. 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:

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

Name	Assignment type
User1	Active
User2	Eligible
User3	Eligible

Answer Area

Statements	Yes	No
When User1 signs in, the user is assigned the Password Administrator role automatically.	○	○
User2 can request to activate the Password Administrator role.	○	○
If User3 wants to activate the Password Administrator role, the user can approve their own request.	○	○

ANSWER:

Answer Area

Statements	Yes	No
When User1 signs in, the user is assigned the Password Administrator role automatically.	○	○
User2 can request to activate the Password Administrator role.	○	○
If User3 wants to activate the Password Administrator role, the user can approve their own request.	○	○

Explanation:

An active assignment in Microsoft Entra Privileged Identity Management means that the Password Administrator role is already assigned to User1. It is not a just-in-time eligible assignment that requires the user to open PIM and activate the role first. Therefore, when User1 signs in, the role is available automatically for the duration and scope of that active assignment. This is the intended use of an active role assignment when immediate standing access is required.

User2 has an eligible assignment, so the user is permitted to begin an activation request for the Password Administrator role. The configured activation controls apply to that request. In this case, the activation process requires multifactor authentication and requires approval by the configured approver group. These settings establish the conditions that must be completed before the role becomes active; they do not stop an eligible assignee from submitting the activation request. The two-hour maximum activation duration limits how long an approved activation can remain active.

User3 can submit an activation request if eligible, but cannot approve that same request. PIM approval is a separation-of-duties control: an approver must be a different person from the requester. Being included in Group1 makes User3 a potential approver for requests from other users, but it does not allow User3 to authorize their own elevation to Password Administrator. Thus, the correct hotspot selections are Yes for the statements about User1's automatic active assignment and User2's ability to request activation, and No for the statement that User3 can approve their own request.

Microsoft documents the distinction between active and eligible role assignments and the activation workflow in Activate Microsoft Entra roles in Privileged Identity Management. The approval separation requirement is documented in Configure role settings in Privileged Identity Management.

QUESTION NO: 78

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:

an Azure blueprint
is the appropriate recommendation because Azure Blueprints can define a repeatable governance baseline and apply it consistently when a standard environment is assigned to each team. A blueprint definition can package environment artifacts, including resource group definitions, policy assignments, role assignments, and deployment templates, into a single versioned unit. Critically for this requirement, a blueprint assignment supports a lock mode that protects the assigned blueprint resources from deletion or modification. This allows the organization to apply the same lock behavior automatically across every team environment rather than relying on manual, potentially inconsistent lock configuration after deployment.

Blueprint assignments also provide centralized lifecycle management: the organization can publish versions of the standardized baseline and use those versions when assigning environments. The lock is associated with the blueprint assignment, helping preserve the governance controls that the standard environment requires. Microsoft documents that blueprint resource locking applies managed locks to resources deployed through the assignment and supports modes such as preventing deletion or making resources read-only. See Azure Blueprints resource locking and the Azure Blueprints overview.

QUESTION NO: 79

You have an Azure subscription that contains a user named User1 and an Azure Container Registry named ConReg1.

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: C D

Explanation:

Creating a trusted image requires both publishing the image to the registry and signing that image by using the registry's content-trust workflow. **AcrPush** provides the data-plane permissions needed to push and pull images and artifacts in the container registry. This allows User1 to publish the image that will be trusted. **AcrImageSigner** is the specialized built-in role that grants permission to sign images for Azure Container Registry content trust. Assigning both roles supplies the two distinct capabilities required to push an image and create its associated trust signature.

These roles can be assigned at the registry scope, or at a narrower repository scope when the registry configuration and scenario support that scope. Using these purpose-specific roles follows least privilege because User1 receives only image publishing and signing permissions, rather than broad Azure resource-management permissions. Microsoft documents that content trust uses image signing and that the AcrImageSigner role is required for signing operations; the built-in role definitions also identify AcrPush as the role for pushing registry content. For further details, see Content trust in Azure Container Registry and Azure Container Registry roles and permissions.

QUESTION NO: 80

Note: This question is part of a set of questions that share the same scenario. However, each question features a unique outcome. Determine if the solution meets the requirements.

Your organization's Azure subscription is associated with Azure Active Directory (Azure AD) tenant. After an internally developed application is registered in Azure AD, you are assigned to ensure that the application can access Azure Key Vault secrets on the users' behalf.

Solution: You configure a delegated permission with admin consent.

Does the solution meet the goal?

A. Yes

B. No

ANSWER: B

Explanation:

No is correct because granting a delegated permission with admin consent in an application registration does not authorize the application or a signed-in user to read secrets from an Azure Key Vault. Azure Key Vault is protected as an Azure resource and evaluates data-plane authorization separately from Microsoft Entra application API permissions. The vault must be configured to use either Azure role-based access control or the legacy vault access-policy model. Under Azure RBAC, the appropriate principal must receive a role that includes secret data actions, such as Key Vault Secrets User, at the required vault scope. Under the access-policy model, the vault must contain an access policy granting the necessary secret permissions, such as Get and, where required, List.

When the application acts for a user, it also needs to acquire an appropriate Microsoft Entra access token for the Key Vault service through a supported delegated flow. However, token acquisition and administrator consent do not themselves provide the Key Vault data-plane permissions. The required Key Vault authorization must still be assigned to the user,

application, or relevant identity according to the selected permission model. Microsoft documents Key Vault authentication and authorization separately from app registration API permission consent. See Authenticate to Azure Key Vault and Provide access to Key Vault keys, certificates, and secrets with Azure RBAC.

QUESTION NO: 81 - (SIMULATION)

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: See the explanation for the answer

Explanation:

Assign **Virtual Machine Contributor** to `user2-28681041` at the **RG1lod28681041** resource-group scope.

1. In the Azure portal, open **Resource groups** and select `RG1lod28681041`.
2. Select **Access control (IAM)** > **Add** > **Add role assignment**.
3. On the **Job function roles** tab, select **Virtual Machine Contributor**, then select **Next**.
4. For members, select **User, group, or service principal**, click **Select members**, and select `user2-28681041`.
5. Select **Review + assign**, then select **Review + assign** again to create the assignment.

Why: The Virtual Machine Contributor role permits management of virtual machines while avoiding broader Resource Group Contributor permissions and does not grant access to the VM or management permissions for related network and storage resources. Assigning it at the resource-group scope applies it only to the virtual machines in `RG1lod28681041`.

QUESTION NO: 82

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:

A just in time (JIT) VM access policy in Microsoft Defender for Cloud is designed to provide controlled, time-limited access to management ports such as Remote Desktop Protocol (RDP), which uses TCP port 3389 by default. A JIT policy protects the targeted virtual machines by ensuring the relevant inbound management port is not continuously exposed through the network security group. When an authorized administrator requests JIT access, Defender for Cloud temporarily creates or modifies an NSG rule to permit traffic to the requested port. The policy can specify the maximum access duration, including 60 minutes, after which the temporary access is automatically removed or the NSG rule is reverted.

JIT access also supports limiting the permitted source to the requester's public IP address or another specified IP range. This narrows the exposure period and network scope while preserving an auditable request process for administrative connections. The policy can be configured for the virtual machines protected by NSG1, allowing ServerAdmins to request the RDP access they need without leaving RDP open continuously. Microsoft documents the feature's temporary NSG rule management and configurable access duration in Just-in-time VM access overview and its configuration process in Enable and use just-in-time VM access.

QUESTION NO: 83

You have an Azure subscription that includes a user named User1 and an Azure Container Registry named ConReg1. You have enabled content trust for ContReg1. Your task is to ensure User1 can create trusted images in ConReg1 while adhering to the principle of least privilege. Which two roles should you assign to User1? Each correct answer contributes to the solution.

NOTE: Each correct selection is worth one point.

A. AcrQuarantineReader

B. Contributor

C. AcrPush

D. AcrImageSigner

E. AcrQuarantineWriter

ANSWER: C D

Explanation:

AcrPush and **AcrImageSigner** provide the least-privileged combination required to create trusted images by using Azure Container Registry content trust. AcrPush grants the registry data-plane permissions required to push container images and related artifacts to repositories. This lets User1 publish the image content that will be trusted, without granting broad Azure Resource Manager permissions to modify the registry resource, its networking, or other subscription resources.

AcrImageSigner grants the permissions required to create and manage the trusted-image signatures used by Azure Container Registry content trust. Content trust is based on Notary v1 image-signing metadata: a publisher signs a repository/tag, and clients configured to trust content can validate that signature before using the image. Therefore, a publisher who must both upload an image and establish it as trusted needs image-push capability together with image-signing capability. Assigning these two built-in roles at the ConReg1 registry scope gives User1 only the operational permissions needed for those two tasks and follows least privilege.

Microsoft documents the signing workflow and the required AcrImageSigner and AcrPush role assignments in Content trust in Azure Container Registry. The permissions supplied by these built-in registry roles are listed in Azure Container Registry roles and permissions.

QUESTION NO: 84

You have an Azure subscription containing the virtual machines listed in the table below:

After enabling Auto Provisioning from the Azure Security Center, you deploy additional virtual machines as listed in the table below:

On which virtual machines is the Log Analytics Agent automatically installed?

A. VM3 only

B. VM1 and VM3 only

C. VM3 and VM4 only

D. VM1, VM2, VM3, and VM4

ANSWER: B

Explanation:

VM1 and VM3 only is correct. In the Azure Security Center auto-provisioning behavior assessed by this question, enabling auto provisioning deploys the Log Analytics agent extension to supported Azure virtual machines that are running. This applies to eligible machines already present when the setting is enabled as well as eligible machines created after it is enabled. Therefore, VM1 receives the agent from the existing set and VM3 receives it after deployment. An Azure VM must be in a state in which the VM agent and extensions can run for the Log Analytics agent extension to be deployed and installed. Auto provisioning is designed to ensure that supported, running virtual machines are connected to the selected Log Analytics workspace so that Security Center can collect security data and generate its security assessments and detections. Microsoft's documentation describes automatic provisioning as the mechanism for deploying the monitoring agent to Azure VMs, and notes the dependency on VM extensions for agent deployment. For current Defender for Cloud configurations, Azure Monitor Agent is generally used instead of the legacy Log Analytics agent; however, the question uses the legacy agent terminology and behavior. See Defender for Cloud monitoring components and Azure Monitor agents overview.

QUESTION NO: 85

You have an Azure subscription that includes an Azure key vault and an Azure Storage account. The key vault contains keys that are managed by customers. Additionally, the storage account is set up to utilize these customer-managed keys stored within the key vault.

You intend to store data in Azure using the following services:

Azure Files
Azure Blob Storage
Azure Log Analytics
Azure Table Storage
Azure Queue Storage

Which two of these services support data encryption utilizing the keys stored in the key vault? Each correct selection counts as one point.

NOTE: Each correct selection is worth one point.

A. Queue storage

B. Table storage

C. Azure Files

D. Blob storage

ANSWER: C D

Explanation:

Azure Files and **Blob storage** support Azure Storage customer-managed keys for encryption at rest. The customer-managed key is stored in Azure Key Vault, and Azure Storage accesses it through a managed identity that has the required permissions to use the key. This model gives the organization control over the encryption key lifecycle, including rotating to a new key version or revoking the storage account's ability to use the key when required.

For Azure Storage, customer-managed keys can be configured for Blob storage and Azure Files. Blob storage includes blob data and Azure Data Lake Storage Gen2 data because Data Lake Storage Gen2 is built on the Blob storage platform. Azure Files supports the same customer-managed-key approach for file-share data encryption at rest. The key configuration is applied through the storage account encryption settings and can use a key in Azure Key Vault or Azure Key Vault Managed HSM.

Microsoft's current service-support matrix and configuration guidance are available in Customer-managed keys for Azure Storage encryption. For the underlying encryption behavior and supported Azure Storage services, see Azure Storage encryption for data at rest.

QUESTION NO: 86

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

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.

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

A. Group1

B. Group2

C. User2

D. User1

ANSWER: B C

Explanation:

Group2 and **User2** can be restored because they are eligible soft-deleted directory objects and their deletion dates fall within the applicable 30-day recovery period when the restore is attempted on May 4, 2020. Microsoft Entra ID retains deleted user accounts in a recoverable state for 30 days. During that interval, an administrator can restore the account from the deleted-users experience, returning the user object and its supported directory properties to the tenant. Microsoft 365 groups are likewise soft deleted for 30 days. Restoring an eligible deleted Microsoft 365 group recovers the group and restores its associated Microsoft 365 resources where supported. The retention interval is calculated from the deletion time, so eligibility must be evaluated as of the date on which the administrator performs the restore. In this case, the dates shown for Group2 and User2 place both objects inside that window. Microsoft documents the group recovery process at Restore a deleted Microsoft 365 group in Microsoft Entra ID and the user recovery process at Restore a deleted user in Microsoft Entra ID.

QUESTION NO: 87

You have an Azure Storage account named storage1 that contains a blob container named container1.

You must prevent users from modifying or deleting blobs in container1 for seven years. The retention period must not be shortened or removed after it is configured.

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

NOTE: Each correct selection is worth one point.

A. Create a time-based retention policy for container1.

B. Lock the immutability policy.

C. Create a stored access policy for container1.

D. Enable blob versioning for storage1.

E. Create a legal hold without configuring a retention policy.

ANSWER: A B

Explanation:

You should create a **time-based retention policy** for container1 and configure the retention interval for seven years. A time-based retention policy creates immutable storage for blobs and prevents modification or deletion until the configured retention period expires.

You should then **lock the immutability policy**. While a policy is unlocked, an authorized user can change or delete the policy. After it is locked, the retention interval cannot be reduced and the policy cannot be removed. A legal hold is an alternative immutability mechanism, but it is based on legal-hold tags rather than a defined seven-year retention period. See Time-based retention policies for immutable blobs.

QUESTION NO: 88

You have an Azure subscription that contains 100 virtual machines with the Azure Security Center's Standard tier enabled.

To assess the security posture of these virtual machines, you plan to execute a vulnerability scan on each of them.

In order to automate the deployment of the vulnerability scanner extension across all virtual machines, you intend to utilize an Azure Resource Manager template.

Which two parameters must you specify in the template to ensure successful deployment of the extension to the virtual machines? Each correct answer constitutes part of the total solution.

Note: Each correct selection is worth one point.

A. the user assigned managed identity

B. the Key Vault managed storage account Key

C. the Azure Active Directory (Azure AD) ID

D. the system-assigned managed identity

E. the primary shared key

F. the workspace ID

ANSWER: E F

Explanation:

The required parameters are **the workspace ID** and **the primary shared key**. In the Azure Security Center architecture represented by this scenario, the VM monitoring and assessment extension must be configured to connect to the Log Analytics workspace associated with the security solution. The workspace ID identifies the destination Log Analytics workspace. The primary shared key is the workspace authentication secret that permits the extension to register and send its collected data to that workspace.

In an ARM deployment, these values are normally supplied as template parameters. The workspace ID is used in the extension’s regular settings, while the primary shared key is treated as sensitive data and should be passed through protected settings or retrieved securely during deployment. This lets the same template deploy consistently to a large VM estate while ensuring that assessment and security data reaches the intended workspace for centralized security-posture analysis.

Microsoft documents that the legacy Log Analytics agent uses a workspace ID and workspace key for connection and authentication to a Log Analytics workspace. Microsoft also documents VM extension resources and protected settings for securely deploying VM extensions through ARM templates. See Log Analytics agent overview and Microsoft.Compute virtual machine extension ARM resource reference.

QUESTION NO: 89

You have an Azure Active Directory (Azure AD) tenant named contoso.com that includes a user called User1. You are planning to publish several applications in the tenant. You need to ensure that User1 can grant admin consent for these published applications. Which two user roles can you assign to User1 to achieve this goal? Each correct answer provides a complete solution.

NOTE: Each correct selection is worth one point.

A. Application developer

B. Security administrator

C. Application administrator

D. User administrator

E. Cloud application administrator

ANSWER: C E

Explanation:

Application administrator and **Cloud application administrator** are the appropriate Microsoft Entra built-in roles for delegating application-management responsibilities, including granting tenant-wide admin consent for applications. These roles allow a user to manage application registrations and enterprise applications in the tenant, which includes approving requested delegated permissions and application permissions on behalf of the organization where the role's consent permissions apply. This enables User1 to approve access centrally rather than requiring each individual user to consent when using a published application.

Assigning either role supports least privilege more effectively than assigning a broad tenant-administration role. The roles are specifically intended for administrators responsible for application onboarding, service principals, app registrations, and organizational consent. There are important protected-resource limitations: for example, these roles do not grant consent for Microsoft Graph application permissions; a more highly privileged role is required for that scenario. For the stated requirement to grant admin consent for published applications generally, however, both roles provide a complete solution. Microsoft documents the consent process and eligible administrative roles at Grant tenant-wide admin consent to an application and details each role's permissions at Microsoft Entra built-in roles.

QUESTION NO: 90

You have an Azure AD tenant that contains the users shown in the following table. 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?

Name	Description
User1	Uses app password authentication for the Mail and Calendar app in Windows 10
User2	Uses Outlook on the web

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. App passwords are a legacy per-user Microsoft Entra multifactor authentication feature designed for older, non-browser applications that cannot complete modern authentication prompts. The MFA service settings include the tenant-wide control, “Allow users to create app passwords to sign in to non-browser apps.” Setting this control to *No* prevents users from creating app passwords, directly satisfying the requirement for all users in the tenant.

This setting does not prevent applications that support modern authentication from signing in. The Windows Mail and Calendar app can use modern authentication, so User1 can continue to authenticate interactively with their normal account credentials and any required MFA challenge rather than relying on an app password. Microsoft recommends modern authentication and advises against app passwords because they are less secure and are intended only as a legacy compatibility mechanism. Administrators should therefore disable app-password creation where modern-authentication-capable clients are in use.

For the service-setting procedure and the app-password control, see Manage app passwords for Microsoft Entra multifactor authentication. Microsoft’s current guidance on authentication methods is available in Authentication methods in Microsoft Entra ID.

QUESTION NO: 91

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: D E

Explanation:

Creating an Azure Log Analytics workspace and upgrading the pricing tier of Security Center to Standard provide the required data platform and security-service capability for this scenario. Microsoft Defender for Cloud, previously named Azure Security Center, uses a Log Analytics workspace to store and query security data collected from protected resources. Custom detections are based on log-query logic, so a workspace is needed to make the relevant data available for analysis and to support the underlying alert-query configuration. The workspace must be associated with the subscription and configured to receive the applicable security data.

The Standard tier, now represented by paid Defender for Cloud plans, enables the advanced workload-protection capabilities that produce and manage security alerts. In the terminology used by this question, upgrading from the free tier to Security Center Standard is therefore necessary before using the advanced alerting functionality. In a current Azure deployment, an administrator should also ensure that they have sufficient Azure RBAC permissions to configure the workspace and alert rules. Microsoft documents Defender for Cloud’s security-alert capabilities at Security alerts in Microsoft Defender for Cloud and the Log Analytics workspace architecture at Log Analytics workspace overview.

QUESTION NO: 92

After enabling Azure Container Registry vulnerability scanning via Azure Security Center for images contained in Registry1, you perform specific operations. Which two images will be subjected to vulnerability scanning? Each correct selection represents a complete answer.

NOTE: Each correct answer is worth one point.

A. Image4

B. Image2

C. Image1

D. Image3

E. Image5

ANSWER: B C

Explanation:

Image2 and **Image1** will be subjected to vulnerability scanning. Azure Security Center, now Microsoft Defender for Cloud, integrates container-image vulnerability assessment with Azure Container Registry to assess images when they are introduced or updated in the protected registry. The relevant operations for these images cause the registry to receive an image artifact or a new image version, which triggers the vulnerability-assessment workflow. This lets Defender for Cloud identify known vulnerabilities in operating-system packages and application dependencies and surface the results as security recommendations and findings for the registry workload.

In practice, image assessment is designed to be part of the container supply-chain workflow: build or obtain an image, place it in Azure Container Registry, and have its security posture evaluated before it is deployed. The assessment results are associated with the image and can be reviewed in Defender for Cloud, enabling remediation of detected vulnerabilities before the image is used by a container host or orchestration service. For current implementation details and supported registry protection capabilities, see Microsoft Defender for container registries and Microsoft Defender for Containers overview.

QUESTION NO: 93

You have an Azure subscription named Subscription1 that contains a resource group named RG1 and the users shown in the following table.

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?

Name	User principal name (UPN)	Type
User1	User1@outlook.com	Guest
User2	User2@outlook.com	Guest

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: C

Explanation:

The Compliance State of the policy assignment to Subscription1 is Non-compliant, and the Compliance State of the policy assignment to RG1 is Compliant. User1 is an external account, as indicated by the guest user type in the table, and has the Network Contributor role assigned directly at the subscription scope. Network Contributor includes permissions to create and modify Azure networking resources, so it grants write-capable access. The policy therefore identifies the external principal with write permissions within Subscription1 and reports the subscription-scoped assignment as non-compliant.

Azure Policy evaluates resources and role assignments within the scope of each individual assignment. The resource group assignment is evaluated in the context of RG1. User2 is not an external account according to the table, so that role assignment does not meet the policy condition for an external identity with write permissions. As a result, the policy assignment at RG1 remains compliant. This illustrates that a policy assigned at a broader scope can detect relevant role assignments in that scope, while a separate assignment at a resource group is evaluated independently against identities and assignments applicable to that resource group. For details on Azure Policy compliance evaluation, see Microsoft Learn. For the write capabilities included in the Network Contributor role, see Microsoft Learn.

QUESTION NO: 94

Note: The following question is part of a series of related questions, each with a distinct outcome. Determine if the proposed solution meets the stated requirements.

Your company's Azure subscription includes a virtual network with a single configured subnet.

You have created a service endpoint for this subnet, which contains an Azure virtual machine running Ubuntu Server 18.04.

You are planning to deploy Docker containers to this virtual machine. It is crucial to ensure that these containers are able to access Azure Storage resources and Azure SQL databases through the service endpoint.

The task is to perform a necessary configuration on the virtual machine before deploying the containers.

Proposed Solution: You create an application security group.

Does this solution meet the objective?

A. Yes

B. No

ANSWER: B

Explanation:

No is correct because an application security group does not configure the virtual machine or its container networking to use an Azure service endpoint. Service endpoints are enabled on a virtual-network subnet and extend that subnet's identity to supported Azure platform services. Access is then granted at the target Azure Storage account or Azure SQL logical server by adding the subnet to the service's virtual network rules. Container traffic must leave through the virtual machine's network interface in the endpoint-enabled subnet so that Azure recognizes the permitted subnet source.

An application security group is a logical grouping of network interfaces used when authoring Network Security Group rules. It can help express security policy for VM workloads, but it does not alter routes, enable endpoint traffic, establish a virtual network rule on Storage or SQL, or change Docker's outbound traffic behavior. Therefore, creating one does not perform the required configuration and cannot by itself ensure that the deployed containers access Azure Storage and Azure SQL Database through the subnet service endpoint. See Azure Virtual Network service endpoints and Application security groups.

QUESTION NO: 95

You have an Azure SQL database configured with Always Encrypted. You need to ensure that application developers have the necessary information to retrieve and decrypt the data within the database.

Which two pieces of information should you provide to the developers? Each correct answer represents a 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: C E

Explanation:

The column encryption key and the column master key are the two key types used by Always Encrypted. The column encryption key is a symmetric key associated with encrypted columns and is used to encrypt values before they are sent to Azure SQL Database and to decrypt encrypted values after they are returned to the client. A client application does not perform this cryptographic work on the database server; an Always Encrypted-capable driver performs it locally.

The column master key is a key-protecting key. It encrypts, or wraps, the column encryption key. Its metadata identifies the trusted key store and key location, such as Azure Key Vault, while the actual master-key material remains in that external store. Developers must configure their application and its identity so the client driver can locate and use the column master key to unwrap the column encryption key. The driver can then use the resulting column encryption key to transparently decrypt query results and encrypt parameter values for supported operations. This separation ensures that the database stores encrypted data and encrypted column encryption keys without receiving access to plaintext key material. See Always Encrypted keys and Always Encrypted (Database Engine).

QUESTION NO: 96

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.

Nantes's 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: C E

Explanation:

The column encryption key and the column master key are required components of Always Encrypted. A column encryption key encrypts the actual values stored in encrypted database columns. The database stores the encrypted column encryption key as metadata; it is not stored in plaintext.

A column master key is a key-protecting key that encrypts one or more column encryption keys. Its definition contains the location of the key material in a trusted key store, such as Azure Key Vault. When an Always Encrypted-enabled application queries encrypted columns, the client driver obtains the encrypted column encryption key metadata, uses the column master key to decrypt that key, and then uses the resulting column encryption key to decrypt the returned column values locally in the application. This client-side design ensures that Azure SQL Database does not receive plaintext data or plaintext encryption keys.

Therefore, developers need the column encryption key metadata and access to the column master key/key store needed by the application driver to perform decryption. For implementation details, see Always Encrypted and Always Encrypted key metadata.

QUESTION NO: 97

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:

No is correct. The requirement is to deploy several policy definitions *as a group* across three Azure subscriptions. Azure Policy provides an initiative definition, also called a policy set, specifically to group multiple policy definitions into one logical collection that can be assigned together. Creating an individual policy definition does not create that grouped deployment unit.

In addition, resource-group-scoped assignments apply only to resources within the selected resource group. This scope would require separate assignments for every applicable resource group and would not provide one centralized assignment that consistently covers all three subscriptions. For centralized governance spanning multiple subscriptions, the initiative should generally be assigned at a management group that contains those subscriptions. A management-group assignment is inherited by the child subscriptions and their resources, enabling the same security controls to be applied consistently throughout the hierarchy.

Microsoft Defender for Cloud uses Azure Policy and initiatives to assess and govern security posture. Using an initiative at an appropriate higher scope supports the stated goal of managing the policies centrally while deploying the collection uniformly. See Azure Policy overview and Azure Policy initiative definitions.

QUESTION NO: 98

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 Analytics Services

D. Microsoft Sentinel

E. Azure Advisor

ANSWER: A D

Explanation:

Azure Monitor is correct because it provides the Azure Monitor alerting platform for data stored in a Log Analytics workspace. An alert rule can use a log search query to evaluate collected virtual-machine event data on a schedule. When the query result meets the configured condition, Azure Monitor creates an alert and can invoke an action group for notifications or automated responses. This directly supports operational monitoring of Windows and Linux events collected into the workspace.

Microsoft Sentinel is also correct. Microsoft Sentinel is built on top of a Log Analytics workspace and uses analytics rules to query workspace data, including events from Azure virtual machines. Analytics rules detect specified patterns or conditions in the ingested data and create alerts when a rule generates a match. Those alerts can then be investigated as incidents and can initiate response workflows through automation rules and playbooks. The option text uses the former product name, Azure Sentinel; Microsoft renamed Azure Sentinel to Microsoft Sentinel, but it identifies the same service. See Create a log search alert rule in Azure Monitor and Detect threats with built-in analytics rules in Microsoft Sentinel.

QUESTION NO: 99

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:

KeyVault1 is the appropriate vault because Azure Disk Encryption requires the Azure Key Vault used for the virtual machine's disk-encryption secrets and keys to be located in the same Azure region as the virtual machine. This requirement ensures that the Azure Disk Encryption extension can access the vault during encryption and subsequent VM operations. In the scenario, VM4 is deployed in West US and KeyVault1 is the vault deployed in West US, so it satisfies the regional requirement. The vault must also be configured to support Azure Disk Encryption access, including enabling the required deployment permissions and ensuring that the identity performing the operation has the necessary Key Vault permissions or Azure RBAC role assignments. Azure Disk Encryption uses Key Vault to safeguard the disk-encryption key material rather than storing that material on the VM itself. For Microsoft's configuration requirements and supported Key Vault settings, see Create and configure a key vault for Azure Disk Encryption. For an overview of how Azure Disk Encryption protects managed disks and uses Key Vault, see Azure Disk Encryption overview.

QUESTION NO: 100

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

Name	Type
DB1	Azure Cosmos DB account
VM1	Virtual machine
VM2	Virtual machine
VNET1	Virtual network
NSG1	Network security group (NSG)

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. For an Azure SQL logical server and its databases, access can be restricted by creating a virtual network rule for the subnet in VNET1 that contains VM1 and VM2. The rule uses a Microsoft.Sql service endpoint on that subnet, allowing Azure SQL Database to identify connections as originating from the approved virtual network rather than relying on the VMs' potentially changing private or public IP addresses. With access limited to VNET1, DB1 accepts connectivity from the workloads hosted in that authorized virtual network, which includes VM1 and VM2 as stated in the scenario. This is enforced at the database service boundary, where Azure SQL evaluates whether to permit a connection. The virtual network rule is configured in the networking/firewall settings of the Azure SQL logical server that hosts DB1, and the relevant subnet must have the Microsoft.Sql service endpoint enabled. Microsoft documents that virtual network rules enable Azure SQL Database access from specific virtual network subnets through service endpoints. See Virtual network service endpoint rules for Azure SQL Database and Configure Azure SQL Database firewall rules.

QUESTION NO: 101

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

From Azure Security Center, you turn on Auto Provisioning. You deploy the virtual machines shown in the following table.

On which virtual machines is the Microsoft Monitoring Agent installed?

Name	Operating system
VM1	Windows Server 2016
VM2	Ubuntu Server 18.04 LTS

Name	Operating system
VM3	Windows Server 2016
VM4	Ubuntu Server 18.04 LTS

A. VM3 only

B. VM1 and VM3 only

C. VM3 and VM4 only

D. VM1, VM2, VM3, and VM4

ANSWER: B

Explanation:

VM1 and VM3 only is correct. In the Azure Security Center experience applicable to this question, enabling Auto Provisioning deploys the Microsoft Monitoring Agent (MMA), also called the Log Analytics agent, to eligible Azure Resource Manager virtual machines. Auto Provisioning uses the VM extension mechanism to install and configure the agent so that the machine can send the security data required by Security Center to the configured Log Analytics workspace. VM1 and VM3 meet the deployment-model requirement shown in the table, so the MMA extension is automatically installed when those virtual machines are deployed after Auto Provisioning is enabled.

This automated deployment is intended to ensure that supported Resource Manager-based VMs are onboarded consistently for security monitoring without separately installing the agent on each VM. The agent provides the data collection path used by the historical Security Center data-collection configuration, including collection of security-related events. Microsoft has since moved newer deployments toward Azure Monitor Agent and Defender for Cloud agentless capabilities, but MMA Auto Provisioning is the behavior tested by this question. See Enable data collection in Microsoft Defender for Cloud and Log Analytics agent overview.

QUESTION NO: 102

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 Active Directory (Azure AD) Identity Protection

B. Microsoft Defender for Cloud

C. Microsoft Defender for Identity

D. Microsoft Sentinel

ANSWER: B

Explanation:

Microsoft Defender for Cloud is the appropriate service because its regulatory compliance capability evaluates Azure resources and workloads against compliance controls defined in standards such as ISO 27001:2013. The Regulatory compliance dashboard presents compliance posture by standard, showing the applicable controls, assessments, resource-level findings, and recommendations that require remediation. This allows a security team to identify configurations that do not meet the mapped ISO requirements and investigate the affected workloads directly from the compliance view.

Defender for Cloud implements these evaluations through Azure Policy initiatives and policy definitions. When the relevant ISO 27001:2013 standard is assigned to the subscription or management group, Azure Policy assesses supported resources and reports their compliance state; Defender for Cloud then organizes those assessment results into a standards-focused compliance experience. This makes it suitable not only for locating non-compliant resources, but also for tracking the overall posture and prioritizing remediation work. Microsoft documents the Regulatory compliance dashboard and its use for monitoring standards and controls at Microsoft Learn. Details on the built-in ISO 27001:2013 initiative and its policy mappings are available in the Azure Policy ISO 27001:2013 initiative documentation.

QUESTION NO: 103

Your organization utilizes Azure DevOps with established branch policies. Which of the following statements accurately describe branch policies? (Select 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: A C

Explanation:

“It enforces your team's change management standards.” is correct because Azure Repos branch policies establish required conditions for completing pull requests into protected branches. A team can require reviewer approval, linked work items, comment resolution, and other checks before a change is merged. These requirements make the agreed change-control process consistent and auditable for contributions targeting an important branch.

“It enforces your team's code quality.” is also correct. Branch policies can require build validation and external status checks, which can run automated compilation, tests, security scanning, linting, or other quality gates. Policies can also require a minimum number of reviewers or designated reviewers, adding peer review to the validation process. Pull requests cannot be completed until required policies are satisfied, except where an authorized user is permitted to override them. Together, these controls help ensure that changes merged into protected branches meet the team’s defined review and engineering-quality requirements. Microsoft documents branch policies as a way to enforce pull-request requirements and improve code quality for branches. See Configure branch policies in Azure Repos and Pull request status policy.

QUESTION NO: 104

You manage an Azure subscription that includes a web application named App1. Users need to have the option to authenticate using either a Google identity or a Microsoft identity. How can you add Google as an identity provider in Azure Active Directory (Azure AD)?

Select the two pieces of information you need to configure. Each correct choice contributes to part of the solution.

Each correct selection is worth one point.

A. a tenant name

B. a tenant ID

C. the endpoint URL Of an application

D. a client ID

E. a client secret

ANSWER: D E

Explanation:

To configure Google as an identity provider, you first create OAuth credentials for the application in Google Cloud. Google issues a client ID and client secret for those credentials. The client ID identifies the Google OAuth application that Azure uses when redirecting a user to Google for authentication. The client secret is the confidential credential Azure uses when it exchanges the authorization code returned by Google for tokens. Together, these values establish the application's OAuth trust configuration and enable the authorization-code flow required for users to sign in with their Google accounts.

For App Service built-in authentication, these values are supplied in the Google provider configuration along with the redirect URI registered in Google Cloud. Microsoft's configuration guidance specifically identifies the Google application client ID and client secret as required provider settings. The same OAuth principles apply when configuring external identity-provider integration: the client ID identifies the relying application and the secret authenticates its server-side token exchange. See Configure Google authentication for Azure App Service and OAuth 2.0 authorization code flow.

QUESTION NO: 105

You have an Azure subscription with a virtual machine named VM1.

You have also created an Azure Key Vault with the following configurations:

Name: Vault5
Region: West US
Resource group: RG1

Your objective is to use Vault5 to enable Azure Disk Encryption on VM1. The solution must also support VM1's backup using Azure Backup.

Which settings in the key vault should you configure?

A. Access policies

B. Secrets

C. Keys

D. Locks

ANSWER: A

Explanation:

Access policies is the required Key Vault setting because Azure Disk Encryption must be explicitly permitted to use the vault for volume encryption. In a vault configured with the access-policy permission model, this is enabled through the vault's access configuration, including the advanced access-policy setting that allows Azure Disk Encryption to retrieve and use the secrets and, where applicable, keys that protect the virtual machine disks. The deployment process also grants the appropriate secret and key permissions to the identity used by the encryption extension, allowing encryption material to be written to and read from Vault5.

This configuration is important for the ongoing lifecycle of an encrypted virtual machine, not just the initial encryption operation. Azure Backup supports Azure Disk Encryption scenarios and uses the VM's encryption configuration and Key Vault references when required during protected VM operations, such as restore. Configuring access policies therefore provides the vault-side authorization foundation for using Vault5 with Azure Disk Encryption while retaining Azure Backup support. Microsoft documents the Key Vault prerequisites and access configuration for disk encryption in Azure Disk Encryption and Azure Key Vault, and documents backup considerations for encrypted virtual machines in Back up encrypted Azure virtual machines.

QUESTION NO: 106

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: C E

Explanation:

The information required is **the column encryption key** and **the column master key**. Always Encrypted is designed so that encryption and decryption occur in the client application, not in Azure SQL Database. The column encryption key is a symmetric key used to encrypt and decrypt values in protected database columns. A client driver that supports Always Encrypted obtains the encrypted column encryption key metadata and uses it when processing encrypted values.

The column master key protects the column encryption key. It is held in a trusted external key store, such as Azure Key Vault, a certificate store, or a hardware security module. The application must be configured to locate the column master key and the identity used by the application must have the necessary permission to use that key. The client driver uses the column master key to decrypt, or unwrap, the column encryption key; it can then transparently decrypt returned column values for the application.

Together, the column encryption key and column master key form the Always Encrypted key hierarchy that enables authorized client-side access to protected data. For details, see Always Encrypted keys and Always Encrypted (Database Engine).

QUESTION NO: 107

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 should be implemented because they enforce the organization’s required validation and review controls before a pull request can be completed into a protected branch, such as *main*. A policy can require a specified minimum number of reviewers, require approval from designated reviewers or groups, and reset approvals when source code changes. These controls make code review standards enforceable rather than voluntary.

Branch policies can also enforce code-quality validation through build validation. Azure DevOps can queue a build pipeline for a pull request and require it to succeed before the change is merged. The pipeline can compile the application, execute automated tests, run code analysis, and apply any organization-specific quality gates. Policies also support external status checks, allowing integrated tools to report required validation results directly on the pull request.

Together, these requirements provide a consistent, auditable gate for both human review and automated quality checks. The pull request cannot be completed until the configured policies are satisfied, helping ensure that all changes entering critical branches meet the company's established standards. For configuration details, see Configure branch policies and Azure Repos build validation policy.

QUESTION NO: 108

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

F. Verified ID Administrator

ANSWER: D F

Explanation:

Verified ID Administrator is the least-privileged Microsoft Entra built-in role for configuring and administering Microsoft Entra Verified ID in a tenant. The role is intended for users who must manage the Verified ID service and its associated settings without receiving broad tenant-level authority. This directly provides the permission scope needed to configure contoso.com for use with Verified ID.

Application Administrator provides the directory permissions required to create and manage application registrations and enterprise applications. Assigning this role enables User1 to register App1 in contoso.com while avoiding more extensive directory-administration roles. Together, these roles separate the required Verified ID administration and application-registration duties into narrowly scoped permissions, which follows the principle of least privilege.

Microsoft documents the permissions and intended use of these roles in the Microsoft Entra built-in roles reference. For service configuration context, see Configure a Microsoft Entra Verified ID tenant.

QUESTION NO: 109

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

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

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: B F

Explanation:

The **Virtual Machine Contributor role for RG1** gives ServerAdmins the permissions required to create and manage virtual machines within RG1. Assigning this built-in role at the RG1 scope limits its effective permissions to that resource group, so VM creation is not granted elsewhere in the subscription. This role supports VM management without granting general management permissions across all Azure resource types.

The **Network Contributor role for RG2** supplies the network-resource permissions needed at the location of the existing virtual networks. In particular, creating a VM that connects to a subnet in another resource group requires authorization to join the subnet. Network Contributor includes the relevant virtual-network and subnet permissions, including the subnet join capability, and scoping it to RG2 limits that access to the intended existing networks. Together, these assignments separate compute administration in RG1 from network access in RG2, meeting the cross-resource-group deployment requirement while retaining least-privilege scope.

Microsoft documents the permissions included in the built-in Virtual Machine Contributor and Network Contributor roles in Azure built-in roles. For how scope constrains the effective permissions of each assignment, see Understand scope for Azure RBAC.

QUESTION NO: 110 - (SIMULATION)

You have an Azure subscription that contains an Azure key vault and an Azure SQL database named SQL1.

You generate a key named Key1.

You need to enable Transparent Data Encryption (TDE) for SQL1 by using Key1.

Which two settings should you modify for Key1? To answer, select the appropriate settings in the answer area.

NOTE: Each correct selection is worth one point.

ANSWER: See the explanation for the answer

Explanation:

Modify the following settings for `Key1`:

Key type: `RSA`
RSA key size: `2048` bits

Azure SQL Database Transparent Data Encryption with a customer-managed key requires an asymmetric RSA key in Azure Key Vault. A 2048-bit RSA key is supported for the TDE protector.

QUESTION NO: 111

You have an active Azure subscription and have created an Azure web application named Contoso1812, which is utilizing an S1 App Service plan. You intend to set up a CNAME DNS record for the domain www.contoso.com to direct it towards Contoso1812.

Your objective is to allow users to access Contoso1812 through the URL https://www.contoso.com. What two actions must you undertake? Each correct action constitutes a part of the solution.

Note: Each correct answer 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: B F

Explanation:

Adding a hostname to Contoso1812 is required because an Azure App Service app must be configured to recognize and accept the custom host name **www.contoso.com**. After the CNAME record points the host name to the app's default App Service domain, adding the hostname in the app's custom-domain configuration validates the mapping and associates that incoming host header with the app. An S1 App Service plan supports custom domains.

Uploading a PFX file to Contoso1812 provides the private-key certificate material required to secure the custom hostname with TLS. The certificate is uploaded or imported into App Service and is then used to create an SSL/TLS binding for **www.contoso.com**. That binding lets App Service present a certificate matching the requested custom domain when users browse to **https://www.contoso.com**. App Service supports private certificates in PFX format for this purpose, and the Standard tier supports SNI SSL bindings. See Map an existing custom DNS name to Azure App Service and Secure a custom DNS name with a TLS/SSL binding in Azure App Service.

QUESTION NO: 112

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.

Each correct selection is worth one point

A. a tenant name

B. a tenant ID

C. the endpoint URL Of an application

D. a client ID

E. a client secret

ANSWER: D E

Explanation:

To configure Google as an identity provider in Microsoft Entra ID, you must first create OAuth 2.0 credentials for the application in Google Cloud. Google issues a client ID that uniquely identifies the application during authentication requests. This value is entered in the Google identity-provider configuration so Microsoft Entra ID can initiate the OAuth/OpenID Connect sign-in flow with the correct Google application registration.

You must also configure the client secret generated for those Google OAuth credentials. The client secret is used with the client ID when Microsoft Entra ID authenticates itself to Google during the authorization-code exchange. It is a sensitive credential and should be stored and managed securely, with rotation performed before expiration where applicable. After these credentials are configured, the Google provider can be made available to users alongside Microsoft identity sign-in, subject to the tenant's external identity and application configuration.

Microsoft's guidance for adding Google as an identity provider specifies supplying the Google application's client ID and client secret: Add Google as an identity provider. See also Authentication methods for external users.

QUESTION NO: 113

Your network includes an Active Directory forest with the domain contoso.com, and an Azure Active Directory (Azure AD) tenant also named contoso.com. You plan to set up synchronization using the Express Settings installation option in Azure AD Connect. You need to determine the necessary roles and groups required to perform this configuration while following the principle of least privilege. Which two roles and groups should you select? Each correct choice contributes to the solution and is valued at 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: C E

Explanation:

Express Settings in Azure AD Connect requires credentials in both Microsoft Entra ID (formerly Azure AD) and the on-premises Active Directory forest. The **Global administrator role in Azure AD** is required when using the Express installation path because the wizard uses this privileged tenant role to configure directory synchronization and create or configure the Microsoft Entra connector account and related tenant settings. Microsoft documents Global Administrator as the required Microsoft Entra credential for an Express installation.

The **Enterprise Admins group in Active Directory** supplies the necessary forest-wide permissions for the Express wizard to create and configure the on-premises AD DS connector account and apply the permissions needed for synchronization. Because the requirement is for an Active Directory *forest*, Enterprise Admins is the appropriate built-in group for this installation method. More granular, delegated permission models can be used with customized Azure AD Connect configurations, but Express Settings uses the documented elevated forest credential. These selections provide the permissions required by the Express workflow without assigning unrelated Azure roles. See Install Microsoft Entra Connect using express settings and Microsoft Entra Connect accounts and permissions.

QUESTION NO: 114

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:

Azure Logic Apps Designer is the appropriate tool because Microsoft Defender for Cloud workflow automation uses an associated Azure Logic App to carry out response and notification actions. The workflow automation defines when the automation runs, such as when Defender for Cloud generates an alert or recommendation, while the Logic App workflow contains the operational steps that occur after it is triggered. For an email-based workflow, the relevant email connector action contains the recipient configuration. Opening the associated Logic App in Azure Logic Apps Designer lets an administrator edit that action and replace User1's address with the Alerts distribution group's email address. The designer provides the visual authoring experience for inspecting and changing the workflow's triggers, actions, connector settings, and parameters, then saving the updated workflow. This keeps the existing Defender for Cloud automation in place while changing the target of its notification. Microsoft documents that workflow automation can trigger Logic Apps for automated responses, and that Logic Apps provides the workflow authoring and design experience used to configure those actions. See Workflow automation in Microsoft Defender for Cloud and Azure Logic Apps overview.

QUESTION NO: 115

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:

Kerberos is the token type used for SMB access to an Azure file share when identity-based authentication is configured. Azure Files supports identity-based SMB authentication through domain services, including Active Directory Domain Services and Microsoft Entra Domain Services. In this model, the Windows client authenticates the user with the configured domain and obtains a Kerberos service ticket for the Azure Files SMB service. The client presents that ticket when connecting to the file share.

Azure Files uses the identity represented by the Kerberos ticket to authorize access. Authorization includes evaluating the user's share-level permissions, typically assigned through Azure RBAC roles such as Storage File Data SMB Share Reader

or Contributor, and then enforcing NTFS access control lists on files and directories where applicable. This allows SMB access to follow familiar Windows integrated-authentication behavior without requiring storage account keys or shared access signatures. Kerberos is therefore the relevant credential mechanism for User1's SMB request from the Windows device. For implementation details, see Azure Files identity-based authentication overview and Enable AD DS authentication for Azure file shares.

QUESTION NO: 116

Your Azure subscription includes several resources as shown in the image below. You intend to activate Microsoft Defender for Cloud for this subscription. Identify which of the listed resources are eligible for protection under Microsoft Defender for Cloud.

A. VM1, VNET1, and storage1 only

B. VM1, storage1, and Vault1 only

C. VM1.VNET1, storage1, and Vault1

D. VM1 and storage1 only

E. VM1 and VNET only

ANSWER: B

Explanation:

VM1, storage1, and Vault1 only is correct. Microsoft Defender for Cloud provides cloud security posture management across an Azure subscription and workload-protection plans for supported resource types. A virtual machine such as VM1 is covered by Defender for Servers, which provides server-focused protections and security alerts. An Azure Storage account such as storage1 is eligible for Defender for Storage, which helps detect potentially malicious activity affecting storage services. An Azure Key Vault such as Vault1 is eligible for Defender for Key Vault, which analyzes Key Vault activity to identify suspicious attempts to access secrets, keys, and certificates. These plans are enabled through the Defender for Cloud environment settings at subscription scope, allowing protection to apply to eligible resources in that subscription. The relevant protection is based on the supported workload resource type, so the listed VM, storage account, and Key Vault are the eligible resources represented in this scenario. See the Microsoft Defender for Cloud overview and Defender for Key Vault documentation.

QUESTION NO: 117

You have an Azure subscription that includes the following Azure Log Analytics workspaces:

Workspace1 located in East US, which is utilized by Azure Sentinel.
Workspace2 located in West US, with no specific usage noted.

The subscription also contains the following virtual machines:

VM1 located in East US, running Windows Server 2019, not connected to any workspace.
VM2 located in East US, running Windows Server 2019, connected to Workspace2.
VM3 located in West US, running Windows Server 2019, not connected to any workspace.
VM4 located in West US, running Windows Server 2019, connected to Workspace2.

You intend to leverage Azure Sentinel to monitor the Windows Defender Firewall on these virtual machines. Which virtual machines can you connect to Azure Sentinel?

A. VM1 and VM3 only

B. VM1 Only

C. VM1 and VM2 only

D. VM1, VM2, VM3 and VM4

ANSWER: D

Explanation:

VM1, VM2, VM3 and VM4 is correct. Microsoft Sentinel ingests data through the Log Analytics workspace on which Sentinel is enabled, so each machine must send its applicable Windows Firewall event data to Workspace1. A virtual machine's Azure region does not need to match the region of the Sentinel-enabled workspace for the machine to be monitored. Therefore, both East US and West US virtual machines can be onboarded to send the required logs to Workspace1.

For machines that are not currently connected to a workspace, such as VM1 and VM3, the appropriate monitoring agent and configuration can be deployed to collect the firewall events for Workspace1. Machines already associated with Workspace2, such as VM2 and VM4, can also be configured to send data to the Sentinel workspace. The legacy Log Analytics agent supports connecting a Windows computer to multiple Log Analytics workspaces, and Azure Monitor Agent configurations can be managed through data collection rules. Once the relevant firewall events arrive in Workspace1, Microsoft Sentinel can use them for investigation, hunting, analytics rules, and incident generation.

See Microsoft Sentinel Windows Firewall connector documentation and Microsoft documentation on adding Log Analytics workspaces to the agent.

QUESTION NO: 118

You have an Azure Application Gateway named AppGW1.

You need to protect a web application published through AppGW1 from common web attacks, including SQL injection. Requests that match attack signatures must be blocked, and the events must be logged.

Which two Web Application Firewall (WAF) policy settings should you configure? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Enable a managed rule set in the WAF policy.

B. Set the WAF policy mode to Prevention.

C. Set the WAF policy mode to Detection.

D. Enable Azure DDoS Protection Standard.

E. Create an NSG rule that allows TCP port 443.

ANSWER: A B

Explanation:

A managed rule set supplies the OWASP Core Rule Set signatures that detect common web attacks, including SQL injection, cross-site scripting, and protocol anomalies. The managed rules must be enabled in the WAF policy so that Application Gateway evaluates incoming requests against the available attack signatures.

The WAF policy must use **Prevention** mode. In Prevention mode, Application Gateway blocks requests that match enabled WAF rules and records the matching events in the WAF logs. Detection mode only logs matching requests and does not block them. See What is Azure Web Application Firewall on Azure Application Gateway? and Web Application Firewall managed rules for Application Gateway.

QUESTION NO: 119

You have an Azure subscription containing 100 virtual machines with Azure Defender enabled.

Your plan is to conduct a vulnerability scan on each virtual machine.

You aim to deploy the vulnerability scanner extension to these virtual machines utilizing an Azure Resource Manager template.

Which two specific values must you include in the template code to ensure the automated deployment of the extension to the virtual machines?

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: B F

Explanation:

The required values are **the workspace ID** and **the primary shared key**. In the Azure Defender for Cloud deployment model represented by this question, the VM monitoring/assessment extension must be configured to connect to the Log Analytics workspace that receives the security and assessment telemetry. The workspace ID identifies the destination Log Analytics workspace. In an ARM template, this is commonly obtained from the workspace resource's `customerId` property. The primary shared key supplies the credential used by the extension or monitoring agent to authenticate when it connects and sends data to that workspace. It is normally retrieved at deployment time by using the ARM `listKeys` function and placed in protected settings so that the secret is not exposed in the template's ordinary deployment settings. Supplying both values enables a repeatable deployment across the virtual-machine fleet while associating each deployed instance with the intended workspace. Microsoft documents the workspace ID and workspace key as the connection information required for the legacy Log Analytics agent deployment configuration, and Defender for Cloud documents deployment of vulnerability assessment solutions to Azure VMs. See Log Analytics agent overview and Deploy vulnerability assessment solutions on Azure VMs.

QUESTION NO: 120

Consider a scenario where you have an Azure subscription that includes the resources as outlined in the table below.

[IMAGE_1_OCR_EXTRACTED_TEXT_START] Name Type storage1 Storage account Vault1 Azure Key vault Vault2 Azure Key vault [IMAGE_1_OCR_EXTRACTED_TEXT_END]

You are planning to deploy virtual machines with the roles depicted in the following table:

[IMAGE_2_OCR_EXTRACTED_TEXT_START] Name Role VM1 • Storage Blob Data Reader for storage1 • Key Vault Reader for Vault1 VM2 • Storage Blob Data Reader for storage1 • Key Vault Reader for Vault1 VM3 • Storage Blob Data Reader for storage1 • Key Vault Reader for Vault1 • Key Vault Reader for Vault2 VM4 • Storage Blob Data Reader for storage1 • Key Vault Reader for Vault1 • Key Vault Reader for Vault2 [IMAGE_2_OCR_EXTRACTED_TEXT_END]

Your task is to assign managed identities to these virtual machines, ensuring the following criteria are met:

Each virtual machine should only be assigned the necessary roles
Follow 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:

2 is the minimum number of managed identities because the virtual machines form two distinct, reusable permission groups. One user-assigned managed identity can be assigned the Storage Blob Data Reader role scoped to storage1 and the Key Vault Reader role scoped to Vault1. That identity can then be attached to VM1 and VM2, whose required access is identical. A second user-assigned managed identity can have the same two role assignments plus Key Vault Reader scoped to Vault2, and it can be attached to VM3 and VM4. This gives each virtual machine only the access specified for its workload while avoiding unnecessary duplication of identities.

User-assigned managed identities are Azure resources with an independent lifecycle and can be assigned to more than one supported Azure resource. Consequently, they are appropriate when several VMs require the same Azure RBAC permissions. Assigning roles at the individual storage-account and Key Vault scopes limits authorization to the intended resources, supporting least privilege. The first identity must not include access to Vault2, because the VMs using it do not require that scope. See Managed identities for Azure resources overview and Azure role-based access control overview.

QUESTION NO: 121

You have an Azure Sentinel workspace, and you need to create a playbook. Which two triggers can initiate the playbook? Each correct answer provides 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: C E

Explanation:

An Azure Sentinel alert is generated and An Azure Sentinel incident is created are the two supported Sentinel-specific events that can initiate a playbook. Microsoft Sentinel playbooks are implemented as Azure Logic Apps and use a Microsoft Sentinel trigger to receive the relevant alert or incident payload. An alert-triggered playbook is appropriate when an analytics rule generates an alert and an immediate response is needed, such as enriching entities, sending a notification, or initiating a containment workflow. The playbook receives alert details that can be used by subsequent Logic Apps actions.

An incident-triggered playbook supports workflows based on the incident lifecycle. Incidents can group related alerts and include incident context, entities, severity, status, and ownership information. This makes the incident trigger suitable for actions such as creating an ITSM ticket, assigning an owner, adding a comment, running enrichment, or coordinating response actions through automation rules. Microsoft Sentinel automation rules can run an incident-triggered playbook when an incident is created or updated, while analysts can also run supported playbooks from the incident experience. For current implementation guidance, see Automate threat response with playbooks in Microsoft Sentinel and Tutorial: Use playbooks to respond to threats in Microsoft Sentinel.

QUESTION NO: 122

You have the following Azure virtual machines as listed in the table below:

Each virtual machine is equipped with a single network interface. You have added the network interface of VM1 to an application security group named ASG1.

Your task is to determine which virtual machine network interfaces can also be included in 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:

VM2 and VM3 only is correct. Application security groups provide a way to group virtual-machine network interfaces by workload or application role, allowing network security group rules to use the logical group rather than individual IP addresses. An application security group is associated with a virtual network, and every network interface assigned to that group must be in that same virtual network. The relevant eligibility criterion is therefore the virtual network containing VM1's network interface, which is already a member of ASG1. Based on the virtual machine configuration in the table, VM2 and VM3 have network interfaces in that same virtual network and can be added to ASG1. This remains valid even when the interfaces are located on different subnets within the virtual network; ASG membership is not restricted to one subnet. Using ASGs in this manner enables security rules to remain stable as application instances are added, removed, or receive different private IP addresses. Microsoft documents that all network interfaces assigned to an application security group must exist in the same virtual network as the application security group. See Application security groups and Network security groups overview.