Advanced Complex Dropdown Questions - Results

Back to result overview

Attempt 1

All domains

40 all | 0 correct | 0 incorrect | 40 skipped | 0 marked

Collapse all questions

Question 1 Skipped

You plan to deploy an Azure web app named App1 that will use Azure Active Directory (Azure AD) authentication.

App1 will be accessed from the internet by the users at your company. All the users have computers that run Windows 10 and are joined to Azure AD.

You need to recommend a solution to ensure that the users can connect to App1 without being prompted for authentication and can access App1 only from company-owned computers.

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

NOTE: Each correct selection is worth one point.

Answer Area

The users can connect to App1 without being prompted for authentication:

- An Azure AD app registration
- An Azure AD managed identity
- Azure AD Application Proxy

The users can access App1 only from company-owned computers:

- A Conditional Access policy
- An Azure AD administrative unit
- Azure Application Gateway
- Azure Blueprints
- Azure Policy

Correct selection

The users can connect to App1 without being prompted for authentication:
An Azure AD app registration

The users can connect to App1 without being prompted for authentication:
An Azure AD managed identity

The users can connect to App1 without being prompted for authentication:
Azure AD Application Proxy

Correct selection

The users can access App1 only from company-owned computers:
A Conditional Access Policy

The users can access App1 only from company-owned computers:
An Azure AD administrative unit

The users can access App1 only from company-owned computers:
Azure Application Gateway

The users can access App1 only from company-owned computers:
Azure Blueprints

The users can access App1 only from company-owned computers:
Azure Policy

Overall explanation

Answer Area

The users can connect to App1 without being prompted for authentication:

- An Azure AD app registration
- An Azure AD managed identity
- Azure AD Application Proxy

The users can access App1 only from company-owned computers:

- A Conditional Access policy
- An Azure AD administrative unit
- Azure Application Gateway
- Azure Blueprints
- Azure Policy

An Azure AD app registration: Azure active directory (AD) provides cloud-based directory and identity management services. You can use Azure AD to manage users of your application and authenticate access to your applications using the Azure active directory. You register your application with Azure active directory tenant.

A conditional access policy: Conditional Access policies at their simplest are if-then statements, if a user wants to access a resource, then they must complete an action. By using Conditional Access policies, you can apply the right access controls when needed to keep your organization secure and stay out of your user's way when not needed.

https://codingcanvas.com/using-azure-active-directory-authentication-in-your-web-application

https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview

Question 2 Skipped

You have an Azure subscription that contains 50 Azure SQL databases.

You create an Azure Resource Manager (ARM) template named Template1 that enables Transparent Data Encryption (TDE).

You need to create an Azure Policy definition named Policy1 that will use Template1 to enable TDE for any non-compliant Azure SQL databases.

How should you configure Policy1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Set available effects to:

- DeployIfNotExists
- EnforceRegoPolicy
- Modify

Include in the definition:

- The identity required to perform the remediation task
- The scope of the policy assignments
- The role-based access control (RBAC) roles required to perform the remediation task

Correct selection

Set available effects to:

DeployIfNotExists

Set available effects to:

EnforceRegoPolicy

Set available effects to:

Modify

Include in the definition:

The identity required to perform the remediation task

Include in the definition:

The scope of the policy assignments

Correct selection

Include in the definition:

The role-based access control (RBAC) roles required to perform the remediation task

Overall explanation

1. **Set available effects to:**
   - **DeployIfNotExists**

   The `DeployIfNotExists` effect is used to deploy a resource if it does not exist, which in this case will apply Template1 to enable TDE for any non-compliant Azure SQL databases.
2. **Include in the definition:**
   - **The role-based access control (RBAC) roles required to perform the remediation task**

   This ensures that the necessary permissions are in place for the policy to successfully deploy Template1 and enable TDE for any non-compliant Azure SQL databases.

Question 3 Skipped

You have an Azure subscription that contains 300 virtual machines that run Windows Server 2019.

You need to centrally monitor all warning events in the System logs of the virtual machines.

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

NOTE: Each correct selection is worth one point.

Answer Area

Resource to create in Azure:

- An event hub
- A Log Analytics workspace
- A search service
- A storage account

Configuration to perform on the virtual machines:

- Create event subscriptions
- Configure Continuous delivery
- Install the Azure Monitor agent
- Modify the membership of the Event Log Readers group

Resource to create in Azure:
An event hub

Correct selection

Resource to create in Azure:
A Log Analytics workspace

Resource to create in Azure:
A search service

Resource to create in Azure:
A storage account

Configuration to perform on the virtual machines:
Create event subscriptions

Configuration to perform on the virtual machines:
Configure Continuous delivery

Correct selection

Configuration to perform on the virtual machines:
Install the Azure Monitor agent

Configuration to perform on the virtual machines:
Modify the membership of the Event Log Readers group

Overall explanation

Answer Area

Resource to create in Azure:

- An event hub
- A Log Analytics workspace
- A search service
- A storage account

Configuration to perform on the virtual machines:

- Create event subscriptions
- Configure Continuous delivery
- Install the Azure Monitor agent
- Modify the membership of the Event Log Readers group

A Log Analytics workspace: Send resource logs to a Log Analytics workspace to enable the features of Azure Monitor Logs. You must create a diagnostic setting for each Azure resource to send its resource logs to a Log Analytics workspace to use with Azure Monitor Logs.

Install the Azure Monitor agent: Use the Azure Monitor agent if you need to:

- Collect guest logs and metrics from any machine in Azure, in other clouds, or on-premises.
- Manage data collection configuration centrally

https://docs.microsoft.com/en-us/azure/azure-monitor/essentials/resource-logs

https://docs.microsoft.com/en-us/azure/azure-monitor/agents/agents-overview

Question 4 Skipped

You have several Azure App Service web apps that use Azure Key Vault to store data encryption keys.

Several departments have the following requests to support the web app:

Department	Request
Security	• Review the membership of administrative roles and require users to provide a justification for continued membership. • Get alerts about changes in administrator assignments. • See a history of administrator activation, including which changes administrators made to Azure resources.
Development	• Enable the applications to access Key Vault and retrieve keys for use in code.
Quality Assurance	• Receive temporary administrator access to create and configure additional web apps in the test environment.

Which service should you recommend for each department's request? To answer, configure the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Security:

Development:

Quality Assurance:

Azure AD Privileged Identity Management
Azure Managed Identity
Azure AD Connect
Azure AD Identity Protection

Correct selection

Security:

Azure AD Privileged Identity Management

Security:

Azure Managed Identity

Security:

Azure AD Connect

Security:

Azure AD Identity Protection

Development:

Azure AD Privileged Identity Management

Correct selection

Development:

Azure Managed Identity

Development:

Azure AD Connect

Development:

Azure AD Identity Protection

Correct selection

Quality Assurance:

Azure AD Privileged Identity Management

Quality Assurance:

Azure Managed Identity

Quality Assurance:

Azure AD Connect

Quality Assurance:

Azure AD Identity Protection

Overall explanation

Answer Area

Security:

- Azure AD Privileged Identity Management
- Azure Managed Identity
- Azure AD Connect
- Azure AD Identity Protection

Development:

- Azure AD Privileged Identity Management
- Azure Managed Identity
- Azure AD Connect
- Azure AD Identity Protection

Quality Assurance:

- Azure AD Privileged Identity Management
- Azure Managed Identity
- Azure AD Connect
- Azure AD Identity Protection

Azure AD Privileged Identity Management: Privileged Identity Management provides time-based and approval-based role activation to mitigate the risks of excessive, unnecessary, or misused access permissions on resources that you care about.

Here are some of the key features of Privileged Identity Management:

- Provide just-in-time privileged access to Azure AD and Azure resources
- Assign time-bound access to resources using start and end dates
- Require approval to activate privileged roles
- Enforce multi-factor authentication to activate any role
- Use justification to understand why users activate
- Get notifications when privileged roles are activated
- Conduct access reviews to ensure users still need roles
- Download audit history for internal or external audit
- Prevents removal of the last active Global Administrator role assignment

Azure Managed Identity: Managed identities provide an identity for applications to use when connecting to resources that support Azure Active Directory (Azure AD) authentication. Applications may use the managed identity to obtain Azure AD tokens. With Azure Key Vault, developers can use managed identities to access resources. Key Vault stores credentials in a secure manner and gives access to storage accounts.

Azure AD Privileged Identity Management: Privileged Identity Management provides time-based and approval-based role activation to mitigate the risks of excessive, unnecessary, or misused access permissions on resources that you care about.

Here are some of the key features of Privileged Identity Management:

- Provide just-in-time privileged access to Azure AD and Azure resources
- Assign time-bound access to resources using start and end dates

https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure

https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/overview

Question 5 Skipped

Your company has the divisions shown in the following table.

Division	Azure Subscription	Azure Active Directory (Azure AD) tenant
East	Sub1, Sub2	East.contoso.com
West	Sub3, Sub4	West.Contoso.com

You plan to deploy a custom application to each subscription. The application will contain the following:

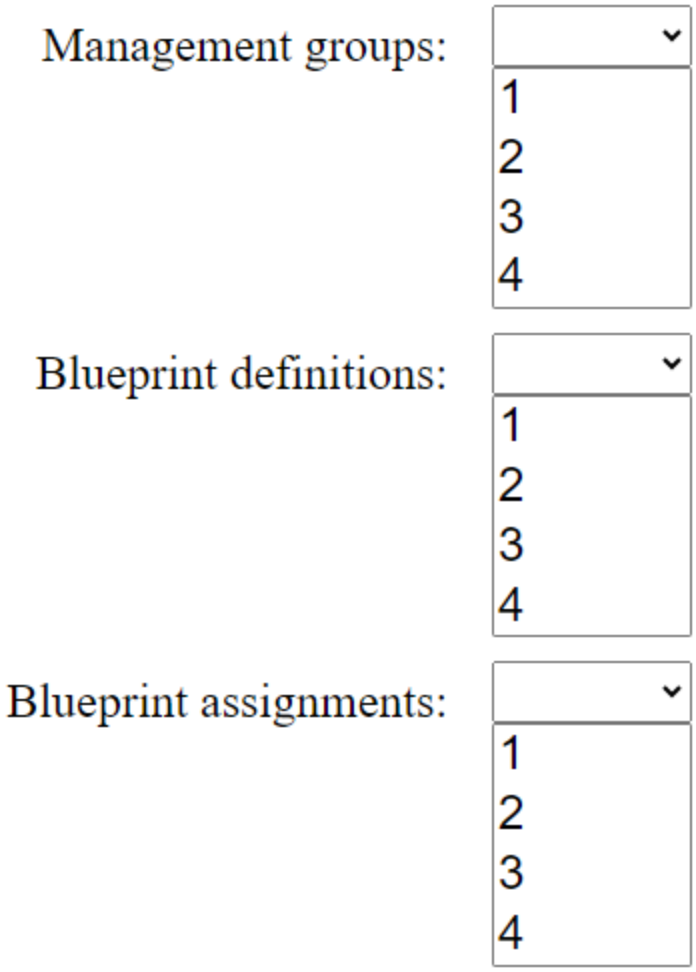
- A resource group
- An Azure web app
- Custom role assignments
- An Azure Cosmos DB account

You need to use Azure Blueprints to deploy the application to each subscription.

What is the minimum number of objects required to deploy the application? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area



Management groups:

1

Correct selection

Management groups:

2

Management groups:

3

Management groups:

4

Blueprint definitions:

1

Correct selection

Blueprint definitions:

2

Blueprint definitions:

3

Blueprint definitions:

4

Blueprint assignments:

1

Blueprint assignments:

2

Blueprint assignments:

3

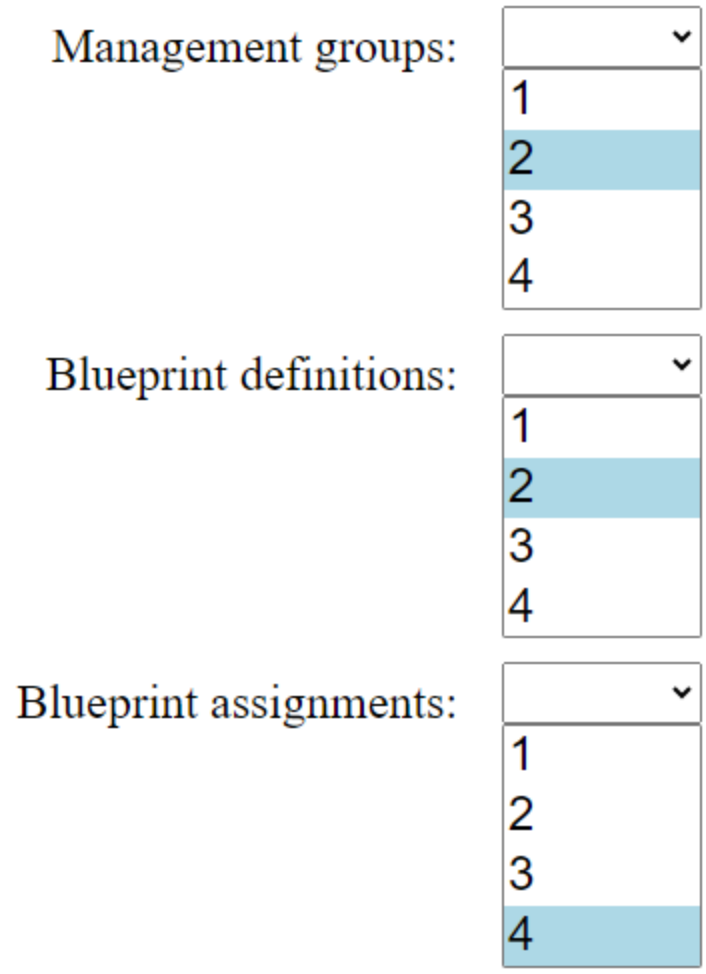
Correct selection

Blueprint assignments:

4

Overall explanation

Answer Area



Management groups give you enterprise-grade management at scale no matter what type of subscriptions you might have. However, all subscriptions within a single management group must trust the same Azure Active Directory (Azure AD) tenant.

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

When creating a **blueprint definition**, you'll define where the blueprint is saved. Blueprints can be saved to a management group or subscription that you have Contributor access to. If the location is a management group, the blueprint is available to assign to any child subscription of that management group.

https://learn.microsoft.com/en-us/azure/governance/blueprints/overview

Assigning a **blueprint definition to a management group means the assignment** object exists in the management group. The deployment of artifacts still targets a subscription.

https://learn.microsoft.com/en-us/azure/governance/blueprints/overview

Question 6 Skipped

You need to design an Azure policy that will implement the following functionality:

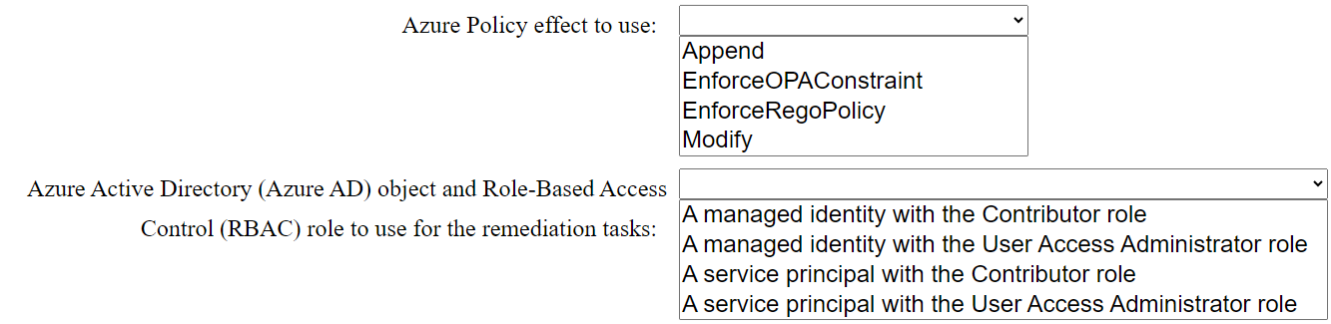
- For new resources, assign tags and values that match the tags and values of the resource group to which the resources are deployed.
- For existing resources, identify whether the tags and values match the tags and values of the resource group that contains the resources.
- For any non-compliant resources, trigger auto-generated remediation tasks to create missing tags and values.

The solution must use the principle of least privilege.

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

NOTE: Each correct selection is worth one point.

Answer Area



Azure Policy effect to use:

Append

Azure Policy effect to use:

EnforceOPAConstraint

Azure Policy effect to use:

EnforceRegoPolicy

Correct selection

Azure Policy effect to use:

Modify

Correct selection

Azure Active Directory (Azure AD) object and Role-Based Access Control (RBAC) role to use for the remediation tasks:

A managed identity with the Contributor role

Azure Active Directory (Azure AD) object and Role-Based Access Control (RBAC) role to use for the remediation tasks:

A managed identity with the User Access Administrator role

Azure Active Directory (Azure AD) object and Role-Based Access Control (RBAC) role to use for the remediation tasks:

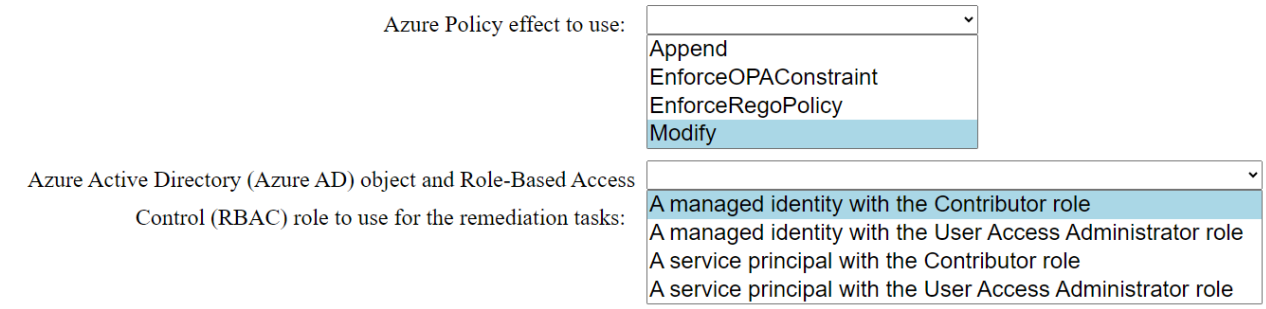
A service principal with the Contributor role

Azure Active Directory (Azure AD) object and Role-Based Access Control (RBAC) role to use for the remediation tasks:

A service principal with the User Access Administrator role

Overall explanation

Answer Area



Modify: Modify is used to add, update, or remove properties or tags on a subscription or resource during creation or update. A common example is updating tags on resources such as cost centers. Existing non-compliant resources can be remediated with a remediation task. A single Modify rule can have any number of operations. Policy assignments with effect set as Modify require a managed identity to do remediation.

A managed identity with the Contributor role: The managed identity needs to be granted the appropriate roles required for remediating resources to grant the managed identity. Contributor - Can create and manage all types of Azure resources but can't grant access to others.

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

https://docs.microsoft.com/en-us/azure/governance/policy/how-to/remediate-resources

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

Question 7 Skipped

You plan to deploy Azure Databricks to support a machine learning application. Data engineers will mount an Azure Data Lake Storage account to the Databricks file system. Permissions to folders are granted directly to the data engineers.

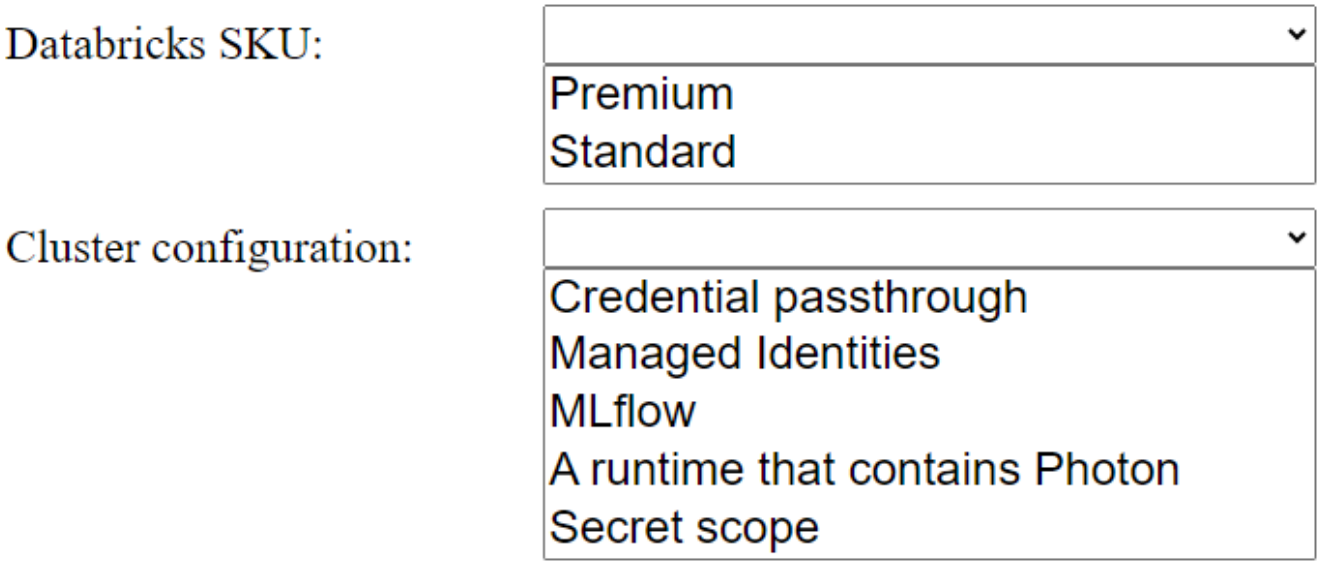
You need to recommend a design for the planned Databrick deployment. The solution must meet the following requirements:

- Ensure that the data engineers can only access folders to which they have permission.
- Minimize development effort.
- Minimize costs.

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

NOTE: Each correct selection is worth one point.

Answer Area



Correct selection

Databricks SKU:

Premium

Databricks SKU:

Standard

Correct selection

Cluster configuration:

Credential passthrough

Cluster configuration:

Managed Identities

Cluster configuration:

MLflow

Cluster configuration:

A runtime that contains Photon

Cluster configuration:

Secret scope

Overall explanation

Answer Area

Databricks SKU:

- Premium
- Standard

Cluster configuration:

- Credential passthrough
- Managed Identities
- MLflow
- A runtime that contains Photon
- Secret scope

Databricks SKU: By choosing the Premium SKU, you can leverage additional features like Delta Lake and AutoML capabilities, which can be beneficial for supporting a machine learning application.

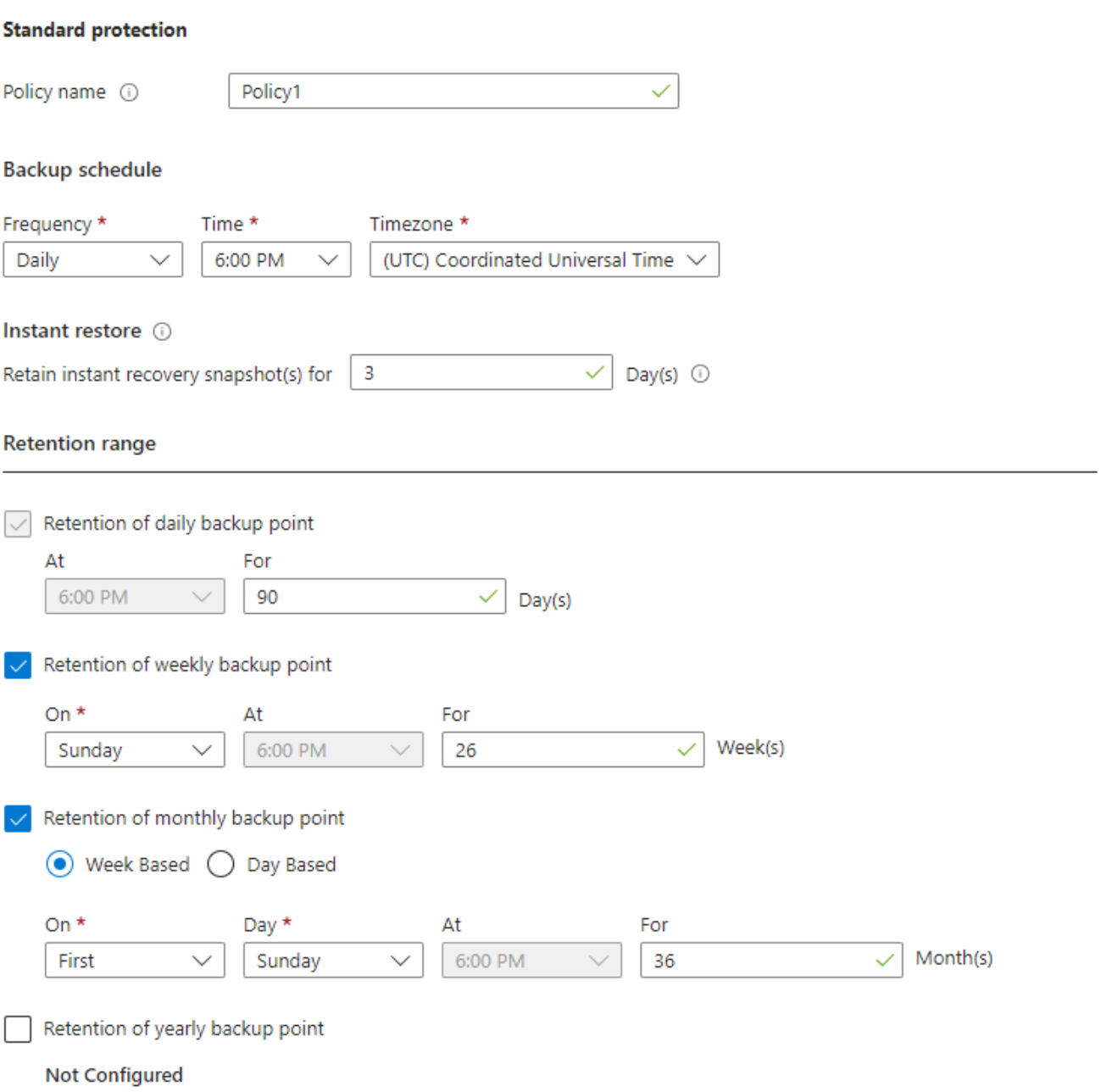
Cluster configuration: Credential passthrough allows users to access data sources using their own credentials, rather than relying on managed identities. This would ensure that data engineers can access the folders to which they have permission without needing to manage separate credentials explicitly. It simplifies the access management process.

https://docs.microsoft.com/en-us/azure/databricks/sql/user/security/cloud-storage-access

https://docs.microsoft.com/en-us/azure/databricks/security/credential-passthrough/adls-passthrough

Question 8 Skipped

You plan to deploy the backup policy shown in the following exhibit.



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

NOTE: Each correct selection is worth one point.

Answer Area

Virtual machines that are backed up by using the policy can be recovered for up to a maximum of:

- 90 days
- 26 weeks
- 36 months
- 45 months

The minimum Recovery Point Objective (RPO) for virtual machines that are backed up by using the policy is:

- 1 hour
- 1 day
- 1 week
- 1 month
- 1 year

Virtual machines that are backed up by using the policy can be recovered for up to a maximum of:

90 days

Virtual machines that are backed up by using the policy can be recovered for up to a maximum of:

26 weeks

Correct selection

Virtual machines that are backed up by using the policy can be recovered for up to a maximum of:

36 months

Virtual machines that are backed up by using the policy can be recovered for up to a maximum of:

45 months

The minimum Recovery Point Objective (RPO) for virtual machines that are backed up by using the policy is:

1 hour

Correct selection

The minimum Recovery Point Objective (RPO) for virtual machines that are backed up by using the policy is:

1 day

The minimum Recovery Point Objective (RPO) for virtual machines that are backed up by using the policy is:

1 week

The minimum Recovery Point Objective (RPO) for virtual machines that are backed up by using the policy is:

1 month

The minimum Recovery Point Objective (RPO) for virtual machines that are backed up by using the policy is:

1 year

Overall explanation

Answer Area

Virtual machines that are backed up by using the policy can be recovered for up to a maximum of:

- 90 days
- 26 weeks
- 36 months
- 45 months

The minimum Recovery Point Objective (RPO) for virtual machines that are backed up by using the policy is:

- 1 hour
- 1 day
- 1 week
- 1 month
- 1 year

RPO: The minimum RPO is 1 day or 24 hours.

https://docs.microsoft.com/en-us/azure/backup/backup-azure-vm-backup-faq

Question 9 Skipped

A company plans to implement an HTTP-based API to support a web app. The web app allows customers to check the status of their orders.

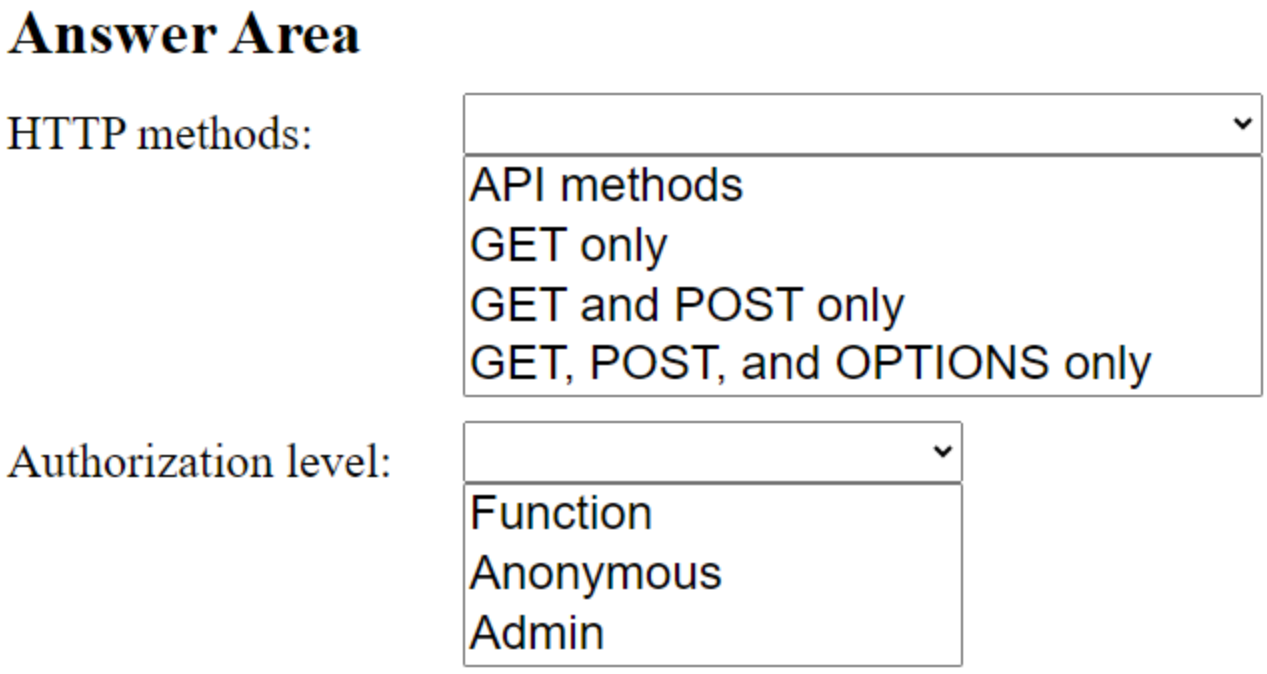
The API must meet the following requirements:

- Implement Azure Functions.
- Provide public read-only operations.
- Prevent write operations.

You need to recommend which HTTP methods and authorization levels to configure.

What should you recommend? To answer, configure the appropriate options in the dialog box in the answer area.

NOTE: Each correct selection is worth one point.



HTTP methods:

API methods

Correct selection

HTTP methods:

GET only

HTTP methods:

GET and POST only

HTTP methods:

GET, POST, and OPTIONS only

Authorization level:

Function

Correct selection

Authorization level:

Anonymous

Authorization level:

Admin

Overall explanation

Answer Area

HTTP methods:

- API methods
- GET only
- GET and POST only
- GET, POST, and OPTIONS only

Authorization level:

- Function
- Anonymous
- Admin

GET: Since the API only needs to provide public read-only operations, the GET method would be sufficient to retrieve data.

Anonymous: Since the API needs to be publicly accessible for read-only operations, an anonymous authorization level should be used to allow unrestricted access without requiring any authentication or authorization.

Question 10 Skipped

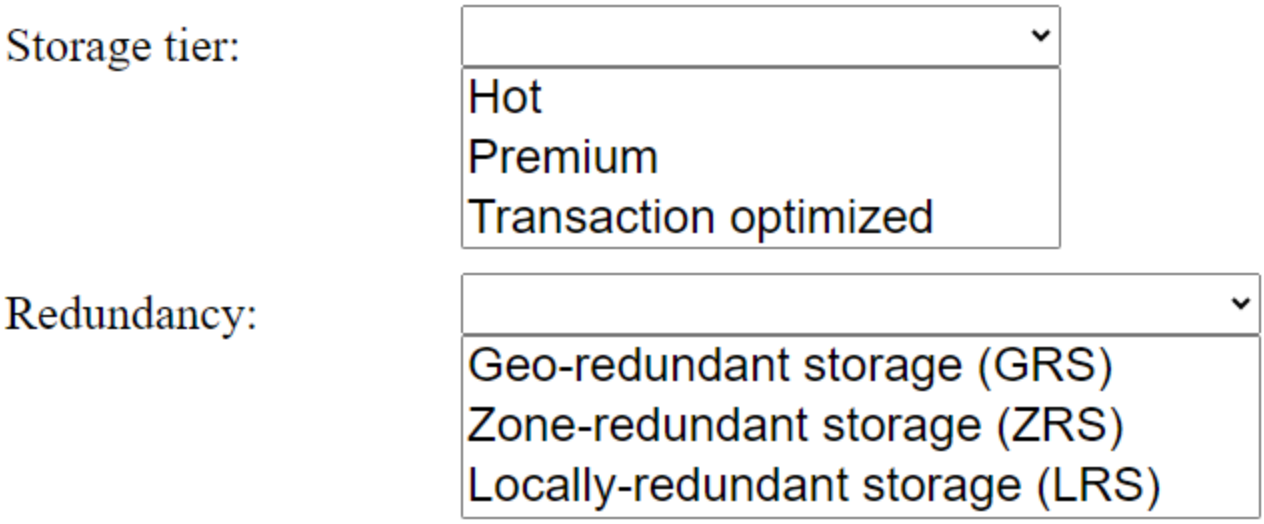
You plan to create an Azure Storage account that will host file shares. The shares will be accessed from on-premises applications that are transaction-intensive.

You need to recommend a solution to minimize latency when accessing the file shares. The solution must provide the highest level of resiliency for the selected storage tier.

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

NOTE: Each correct selection is worth one point.

Answer Area



Storage tier:

Hot

Correct selection

Storage tier:

Premium

Storage tier:

Transaction optimized

Redundancy:

Geo-redundant storage (GRS)

Correct selection

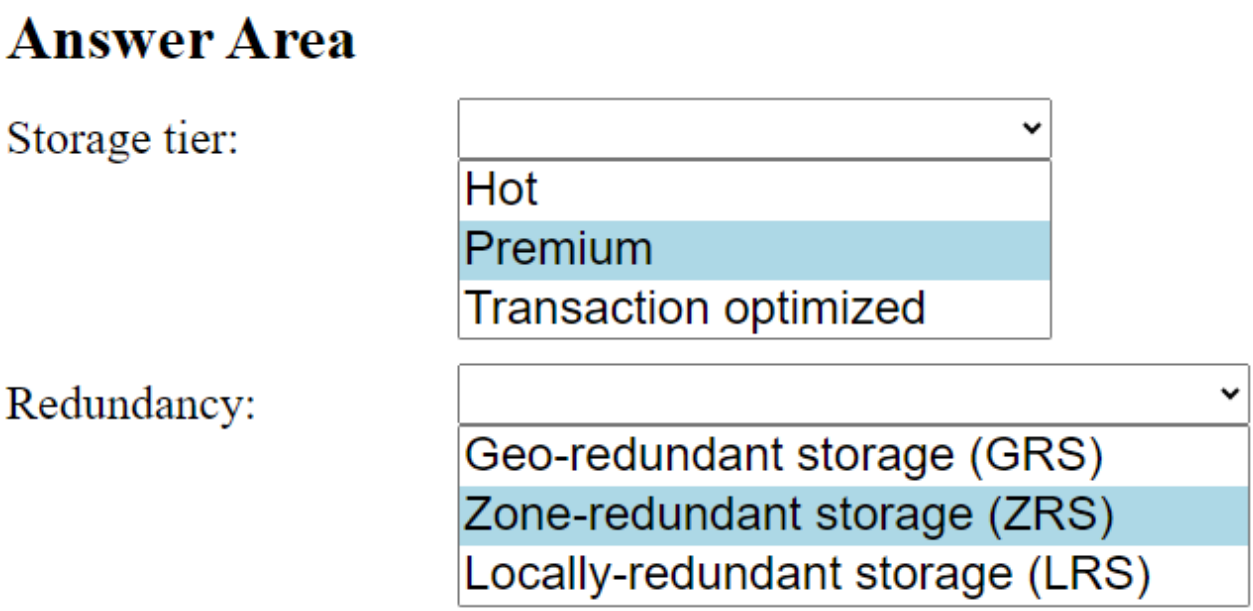
Redundancy:

Zone-redundant storage (ZRS)

Redundancy:

Locally-redundant storage (LRS)

Overall explanation



Premium: Premium file shares are backed by solid-state drives (SSDs) and provide consistent high performance and low latency, within single-digit milliseconds for most IO operations, for IO-intensive workloads.

Zone-redundant storage (ZRS): With ZRS, three copies of each file are stored, however, these copies are physically isolated in three distinct storage clusters in different Azure availability zones.

https://docs.microsoft.com/en-us/azure/storage/files/storage-files-planning

Question 11 Skipped

You need to recommend an Azure Storage account configuration for two applications named Application1 and Application2. The configuration must meet the following requirements:

- Storage for Application1 must provide the highest possible transaction rates and the lowest possible latency.
- Storage for Application2 must provide the lowest possible storage costs per GB.
- Storage for both applications must be available in the event of datacenter failure.
- Storage for both applications must be optimized for uploads and downloads.

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

NOTE: Each correct selection is worth one point.

Answer Area

Application1:

- BlobStorage with Standard performance, Hot access tier, and Read-access geo-redundant storage (RA-GRS) replication
- BlockBlobStorage with Premium performance and Zone-redundant storage (ZRS) replication
- General purpose v1 with Premium performance and Locally-redundant storage (LRS) replication
- General purpose v2 with Standard performance, Hot access tier, and Locally-redundant storage (LRS) replication

Application2:

- BlobStorage with Standard performance, Cool access tier, and Geo-redundant storage (GRS) replication
- BlockBlobStorage with Premium performance and Zone-redundant storage (ZRS) replication
- General purpose v1 with Standard performance and Read-access geo-redundant storage (RA-GRS) replication
- General purpose v2 with Standard performance, Cool access tier, and Read-access geo-redundant storage (RA-GRS) replication

Application1:

BlobStorage with Standard performance, Hot access tier, and Read-access geo-redundant storage (RA-GRS) replication

Correct selection

Application1:

BlockBlobStorage with Premium performance and Zone-redundant storage (ZRS) replication

Application1:

General purpose v1 with Premium performance and Locally-redundant storage (LRS) replication

Application1:

General purpose v2 with Standard performance, Hot access tier, and Locally-redundant storage (LRS) replication

Correct selection

Application2:

BlobStorage with Standard performance, Cool access tier, and Geo-redundant storage (GRS) replication

Application2:

BlockBlobStorage with Premium performance and Zone-redundant storage (ZRS) replication

Application2:

General purpose v1 with Standard performance and Read-access geo-redundant storage (RA-GRS) replication

Application2:

General purpose v2 with Standard performance, Cool access tier, and Read-access geo-redundant storage (RA-GRS) replication

Overall explanation

Answer Area

Application1:

- BlobStorage with Standard performance, Hot access tier, and Read-access geo-redundant storage (RA-GRS) replication
- BlockBlobStorage with Premium performance and Zone-redundant storage (ZRS) replication
- General purpose v1 with Premium performance and Locally-redundant storage (LRS) replication
- General purpose v2 with Standard performance, Hot access tier, and Locally-redundant storage (LRS) replication

Application2:

- BlobStorage with Standard performance, Cool access tier, and Geo-redundant storage (GRS) replication
- BlockBlobStorage with Premium performance and Zone-redundant storage (ZRS) replication
- General purpose v1 with Standard performance and Read-access geo-redundant storage (RA-GRS) replication
- General purpose v2 with Standard performance, Cool access tier, and Read-access geo-redundant storage (RA-GRS) replication

BlockBlobStorage with Premium performance and Zone-redundant storage (ZRS) replication:

- Storage for Application1 must provide the highest possible transaction rates and the lowest possible latency. - Yes
- Storage for both applications must be available in the event of datacenter failure. - Yes
- Storage for both applications must be optimized for uploads and downloads. - Yes

BlobStorage with Standard Performance, Cool access tier, and Geo-redundant storage (GRS) replication:

- Storage for Application2 must provide the lowest possible storage costs per GB. - Yes
- Storage for both applications must be available in the event of datacenter failure. - Yes
- Storage for both applications must be optimized for uploads and downloads. - Yes

Question 12 Skipped

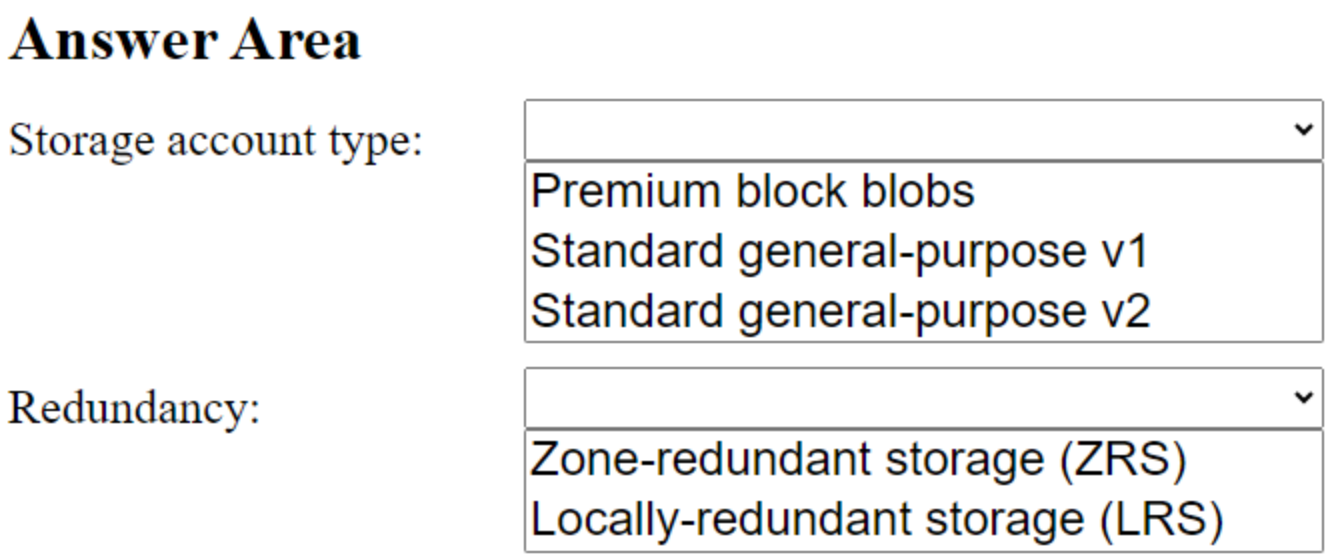
You plan to develop a new app that will store business-critical data. The app must meet the following requirements:

- Prevent new data from being modified for one year.
- Maximize data resiliency.

- Minimize read latency.

What storage solution should you recommend for the app? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Storage account type:
Premium block blobs

Storage account type:
Standard general-purpose v1

Correct selection

Storage account type:
Standard general-purpose v2

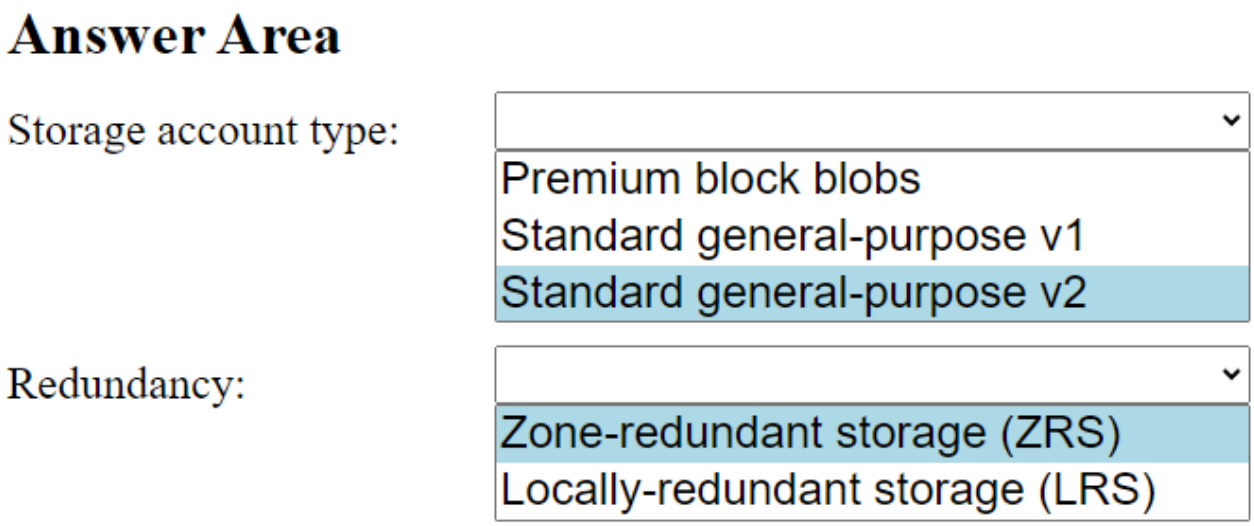
Correct selection

Redundancy:
Zone-redundant storage (ZRS)

Redundancy:

Locally-redundant storage (LRS)

Overall explanation



Standard general-purpose v2 supports immutable storage. In general Standard general-purpose v2 is the preferred Microsoft recommendation.

Zone-redundant storage (ZRS) is more resilient compared to LRS.

Note: RA-GRS is even more resilient, but it is not an option here.

https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blob-immutable-storage

Question 13 Skipped

You have an on-premises file server that stores 2 TB of data files.

You plan to move the data files to Azure Blob Storage in the West Europe Azure region.

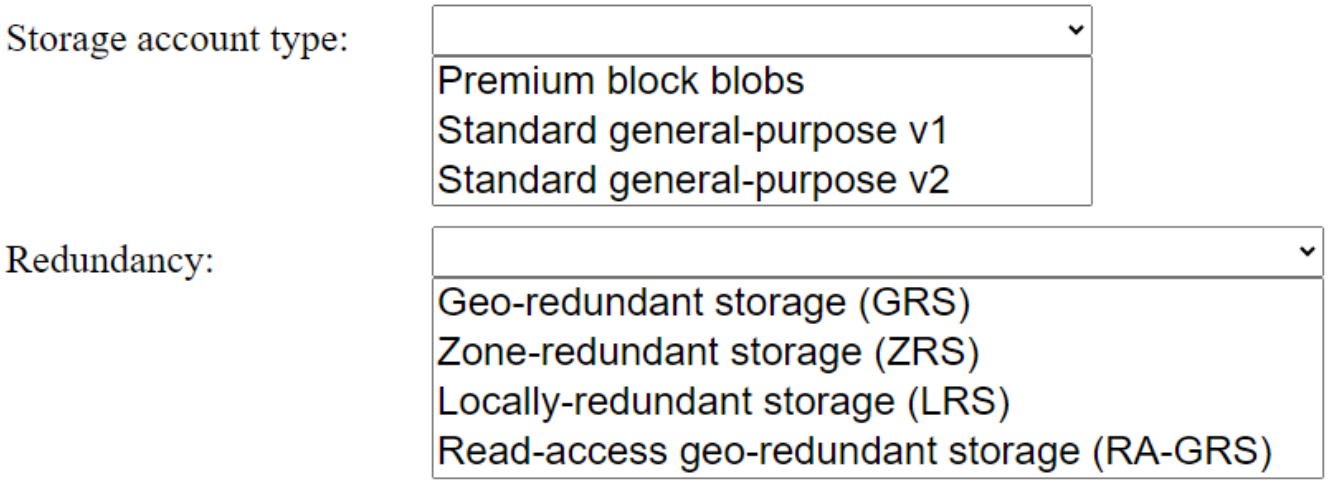
You need to recommend a storage account type to store the data files and a replication solution for the storage account. The solution must meet the following requirements:

- Be available if a single Azure datacenter fails.
- Support storage tiers.
- Minimize cost.

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

NOTE: Each correct selection is worth one point.

Answer Area



Storage account type:
Premium block blobs

Storage account type:
Standard general-purpose v1

Correct selection

Storage account type:
Standard general-purpose v2

Redundancy:
Geo-redundant storage (GRS)

Correct selection

Redundancy:

Zone-redundant storage (ZRS)

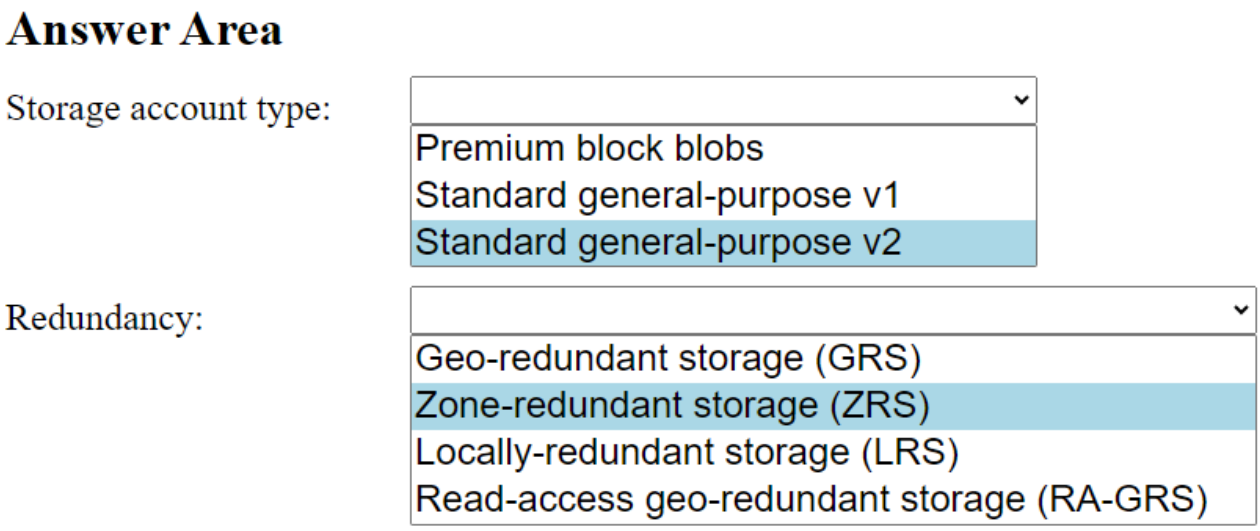
Redundancy:

Locally-redundant storage (LRS)

Redundancy:

Read-access geo-redundant storage (RA-GRS)

Overall explanation



Standard general-purpose v2 meets the requirements and minimizes the costs.

Zone-redundant storage (ZRS) protects against a Datacenter failure while minimizing the costs.

https://docs.microsoft.com/en-us/azure/storage/common/storage-redundancy

Question 14 Skipped

You have an Azure web app named App1 and an Azure key vault named KV1.

App1 stores database connection strings in KV1.

App1 performs the following types of requests to KV1:

- Get

- List
- Wrap
- Delete
- Unwrap
- Backup
- Decrypt
- Encrypt

You are evaluating the continuity of service for App1.

You need to identify the following if the Azure region that hosts KV1 becomes unavailable:

- To where will KV1 failover?
- During the failover, which request type will be unavailable?

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

NOTE: Each correct selection is worth one point.

Answer Area

To where will KV1 failover?

- A server in the same availability set
- A server in the same fault domain
- A server in the paired region
- A virtual machine in a scale set

During the failover, which request type will be unavailable?

- Get
- List
- Wrap
- Delete
- Unwrap
- Backup
- Decrypt
- Encrypt

To where will KV1 failover?

A server in the same availability set

To where will KV1 failover?

A server in the same fault domain

Correct selection

To where will KV1 failover?

A server in the paired region

To where will KV1 failover?

A virtual machine in a scale set

During the failover, which request type will be unavailable?

Get

During the failover, which request type will be unavailable?

List

During the failover, which request type will be unavailable?

Wrap

Correct selection

During the failover, which request type will be unavailable?

Delete

During the failover, which request type will be unavailable?

Unwrap

During the failover, which request type will be unavailable?

Backup

During the failover, which request type will be unavailable?

Decrypt

During the failover, which request type will be unavailable?

Encrypt

Overall explanation

Answer Area

To where will KV1 failover?

- A server in the same availability set
- A server in the same fault domain
- A server in the paired region
- A virtual machine in a scale set

During the failover, which request type will be unavailable?

- Get
- List
- Wrap
- Delete
- Unwrap
- Backup
- Decrypt
- Encrypt

A server in the paired region: The contents of your key vault are replicated within the region and to a secondary region at least 150 miles away, but within the same geography to maintain the high durability of your keys and secrets. Regions are paired for cross-region replication based on proximity and other factors.

Delete: During failover, your key vault is in read-only mode. Requests that are supported in this mode are:

- List certificates
- Get certificates
- List secrets
- Get secrets
- List keys
- Get (properties of) keys
- Encrypt
- Decrypt
- Wrap
- Unwrap
- Verify
- Sign
- Backup

https://docs.microsoft.com/en-us/azure/key-vault/general/disaster-recovery-guidance

Question 15 Skipped

You have an on-premises Microsoft SQL Server database named SQL1.

You plan to migrate SQL1 to Azure.

You need to recommend a hosting solution for SQL1. The solution must meet the following requirements:

- Support the deployment of multiple secondary, read-only replicas.
- Support automatic replication between primary and secondary replicas.
- Support failover between primary and secondary replicas within a 15-minute recovery time objective (RTO).

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

NOTE: Each correct selection is worth one point.

Answer Area

Azure service or service tier:

- Azure SQL Database
- Azure SQL managed instance
- The Hyperscale service tier

Replication mechanism:

- Active geo-replication
- Auto-failover groups
- Standard geo-replication

Correct selection

Azure service or service tier:

Azure SQL Database

Azure service or service tier:

Azure SQL managed instance

Azure service or service tier:

The Hyperscale service tier

Correct selection

Replication mechanism:

Active geo-replication

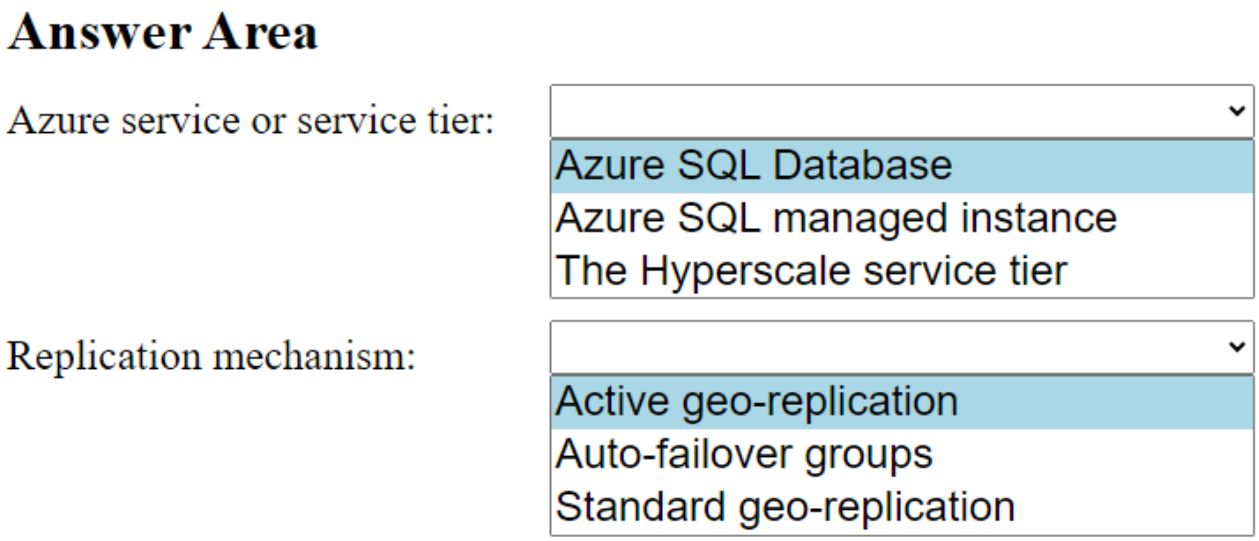
Replication mechanism:

Auto-failover groups

Replication mechanism:

Standard geo-replication

Overall explanation



Azure SQL Database: As part of High Availability architecture, every single database, elastic pool database, and managed instance in the Premium and Business Critical service tier is automatically provisioned with a primary read-write replica and one or more secondary read-only replicas.

Active geo-replication supports the creation of up to four readable secondary replicas within the same or different Azure regions. It provides automatic replication between primary and secondary replicas, and you can initiate failover manually when needed. The recovery time objective (RTO) for active geo-replication is less than 30 seconds, which meets the requirement of a 15-minute RTO.

https://learn.microsoft.com/en-us/azure/azure-sql/database/read-scale-out

Question 16 Skipped

You have two on-premises Microsoft SQL Server 2017 instances that host an Always On availability group named AG1. AG1 contains a single database named DB1.

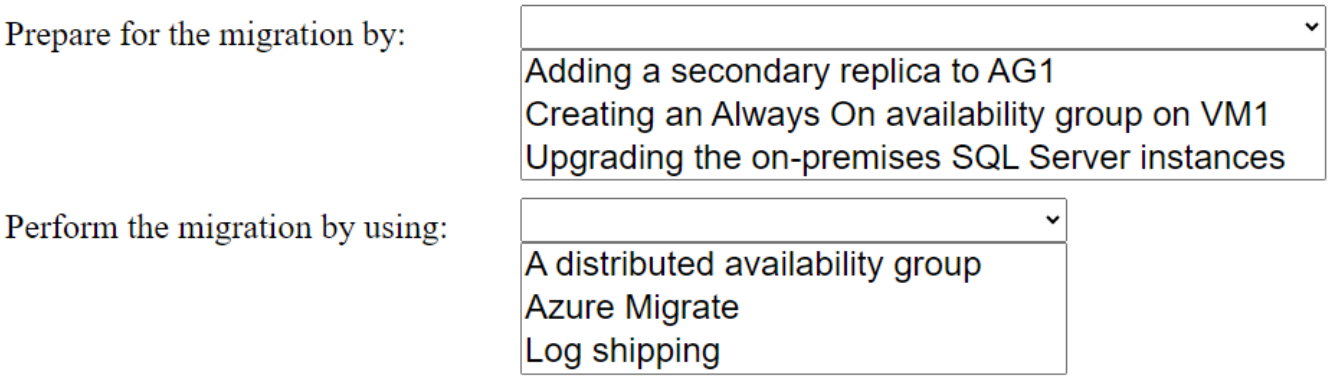
You have an Azure subscription that contains a virtual machine named VM1. VM1 runs Linux and contains a SQL Server 2019 instance.

You need to migrate DB1 to VM1. The solution must minimize downtime on DB1.

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

NOTE: Each correct selection is worth one point.

Answer Area



Correct selection

Prepare for the migration by:

Adding a secondary replica to AG1

Prepare for the migration by:

Creating an Always On availability group on VM1

Prepare for the migration by:

Upgrading the on-premises SQL Server instances

Perform the migration by using:

A distributed availability group

Correct selection

Perform the migration by using:

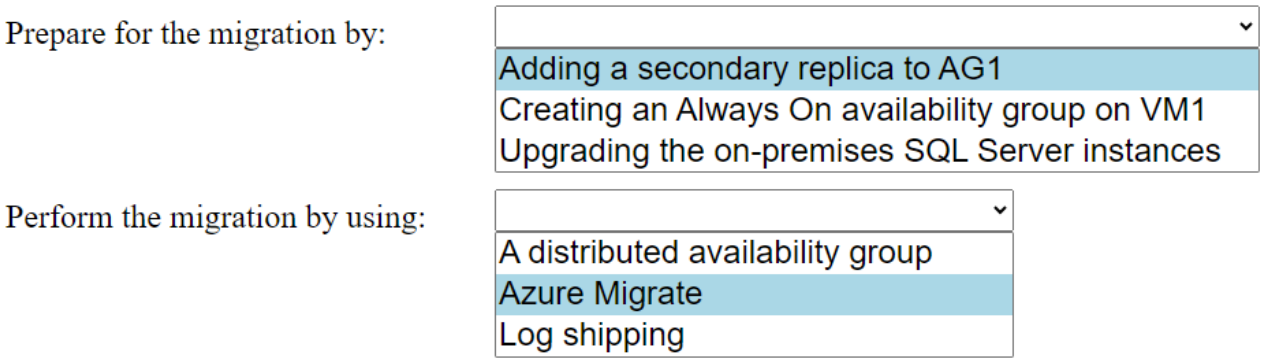
Azure Migrate

Perform the migration by using:

Log shipping

Overall explanation

Answer Area



Adding a secondary replica to AG1: By adding a secondary replica to AG1 on the on-premises SQL Server 2017 instances, you establish a high availability configuration. This allows for continuous data synchronization between the primary and secondary replicas, ensuring data availability and minimizing downtime during the migration process.

Azure Migrate is a service that enables seamless migration of on-premises workloads to Azure. You can use Azure Migrate to migrate the SQL Server availability group from the on-premises instances to the SQL Server 2019 instance on VM1. Azure Migrate provides features like agentless discovery, assessment, and migration, making the migration process smoother and more efficient.

Question 17 Skipped

You are building an Azure web app that will store the Personally Identifiable Information (PII) of employees.

You need to recommend an Azure SQL. Database solution for the web app. The solution must meet the following requirements:

- Maintain availability in the event of a single Datacenter outage.
- Support the encryption of specific columns that contain PII.
- Automatically scale up during payroll operations.
- Minimize costs.

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

NOTE: Each correct selection is worth one point.

Answer Area

Service tier and compute tier:

- Business Critical service tier and Serverless compute tier
- General Purpose service tier and Serverless compute tier
- Hyperscale service tier and Provisioned compute tier

Encryption method:

- Always Encrypted
- Microsoft SQL Server and database encryption keys
- Transparent Data Encryption (TDE)

Service tier and compute tier:

Business Critical service tier and Serverless compute tier

Correct selection

Service tier and compute tier:

General Purpose service tier and Serverless compute tier

Service tier and compute tier:

Hyperscale service tier and Provisioned compute tier

Correct selection

Encryption method:

Always Encrypted

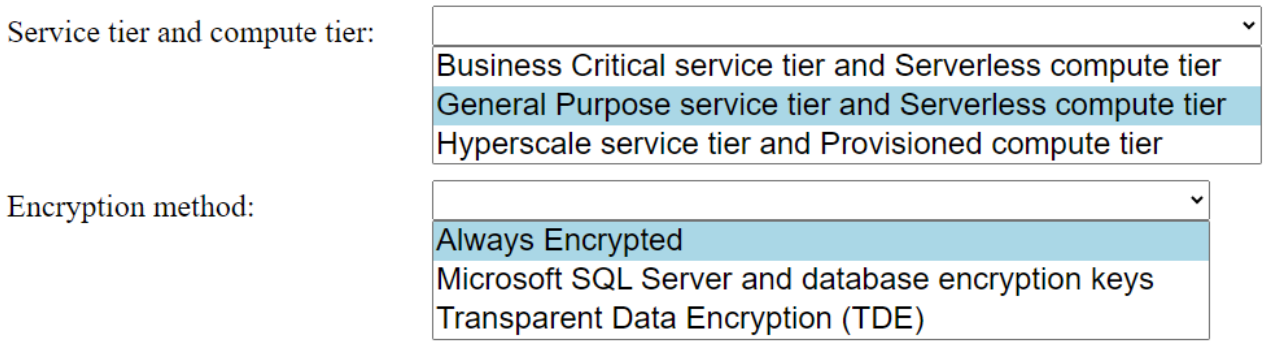
Encryption method:

Microsoft SQL Server and database encryption keys

Encryption method:

Transparent Data Encryption (TDE)

Overall explanation



General Purpose service tier and Serverless compute tier: The General Purpose service tier is designed for common workloads. It offers budget-oriented balanced computing and storage options.

https://learn.microsoft.com/en-us/azure/azure-sql/database/sql-database-paas-overview

Serverless compute tier: Auto-scales compute resources based on workload activity and bills for the amount of compute used, per second. The serverless compute tier is generally available in the General Purpose service tier and is currently in preview in the Hyperscale service tier.

https://learn.microsoft.com/en-us/azure/azure-sql/database/sql-database-paas-overview

Always Encrypted: Always Encrypted is the recommended encryption method for this scenario because it allows you to encrypt specific columns that contain PII. This ensures that sensitive data is encrypted both at rest and in transit, providing a higher level of security for PII. Transparent Data Encryption (TDE) encrypts the entire database at rest but does not provide column-level encryption, and Microsoft SQL Server and database encryption keys would involve additional manual configuration and management of keys.

Question 18 Skipped

You have an Azure subscription named Subscription1 that is linked to a hybrid Azure Active Directory (Azure AD) tenant.

You have an on-premises Datacenter that does NOT have a VPN connection to Subscription1. The Datacenter contains a computer named Server1 that has Microsoft SQL Server 2016 installed. The server is prevented from accessing the internet.

An Azure logic app resource named LogicApp1 requires write access to a database on Server1.

You need to recommend a solution to provide LogicApp1 with the ability to access Server1.

What should you recommend deploying on-premises and in Azure? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

On-premises:
A Web Application Proxy for Windows Server

On-premises:
An Azure AD Application Proxy connector

Correct selection

On-premises:

An On-premises data gateway

On-premises:

Hybrid Connection Manager

Correct selection

Azure:

A connection gateway resource

Azure:

An Azure Application Gateway

Azure:

An Azure Event Grid domain

Azure:

An Enterprise Application

Overall explanation

Answer Area

On-premises:

- A Web Application Proxy for Windows Server
- An Azure AD Application Proxy connector
- An On-premises data gateway
- Hybrid Connection Manager

Azure:

- A connection gateway resource
- An Azure Application Gateway
- An Azure Event Grid domain
- An Enterprise Application

An on-premises data gateway: For logic apps in global, multi-tenant Azure that connect to on-premises SQL Server, you need to have the on-premises data gateway installed on a local computer and a data gateway resource that's already created in Azure.

A connection gateway resource: In Azure, you should deploy a connection gateway resource. This gateway resource will communicate with the on-premises data gateway to provide LogicApp1 with the ability to access the SQL Server 2016 database on Server1 securely.

https://docs.microsoft.com/en-us/azure/connectors/connectors-create-api-sqlazure

Question 19 Skipped

You are designing an Azure App Service web app.

You plan to deploy the web app to the North Europe Azure region and the West Europe Azure region.

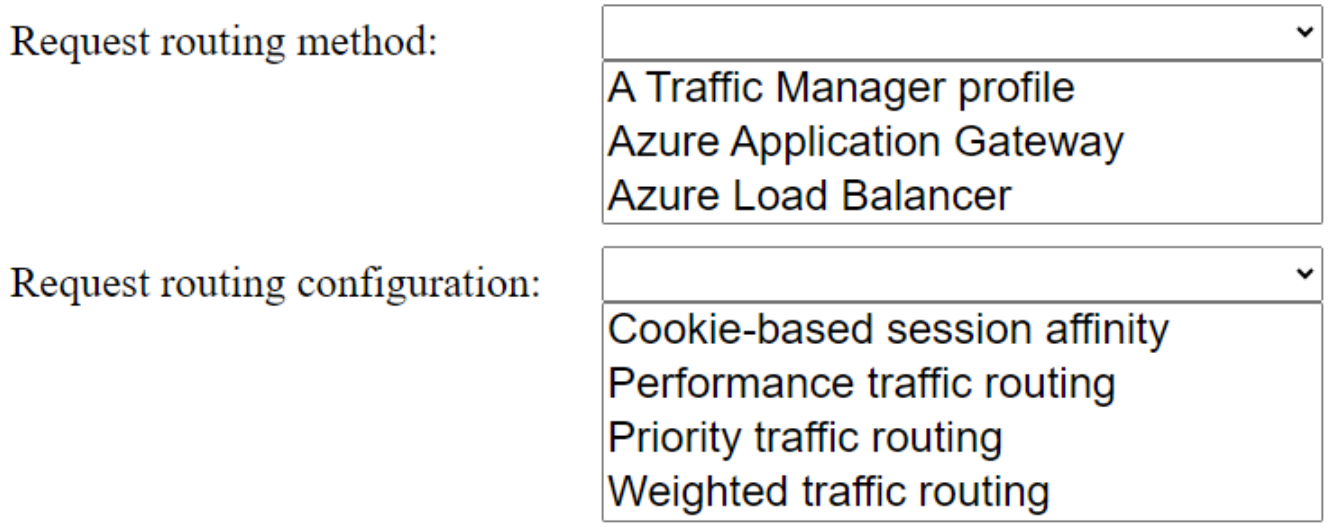
You need to recommend a solution for the web app. The solution must meet the following requirements:

- Users must always access the web app from the North Europe region unless the region fails.
- The web app must be available to users if an Azure region is unavailable.
- Deployment costs must be minimized.

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

NOTE: Each correct selection is worth one point.

Answer Area



Correct selection

Request routing method:
A Traffic Manager profile

Request routing method:
Azure Application Gateway

Request routing method:
Azure Load Balancer

Request routing configuration:
Cookie-based session affinity

Request routing configuration:
Performance traffic routing

Correct selection

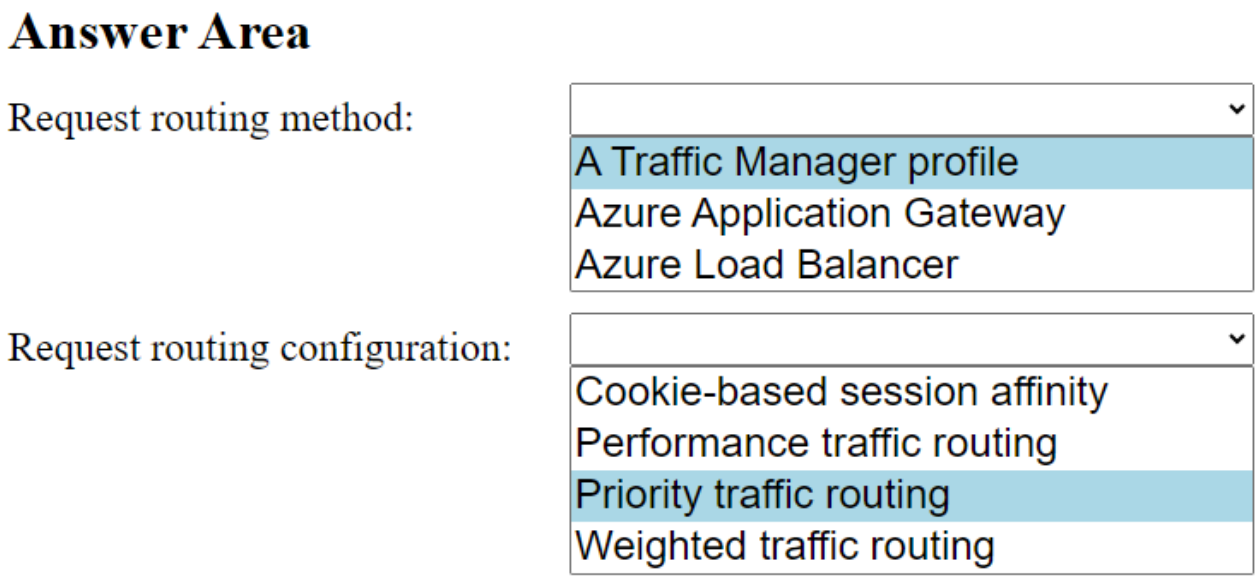
Request routing configuration:

Priority traffic routing

Request routing configuration:

Weighted traffic routing

Overall explanation



A Traffic Manager Profile: To meet the requirements of directing users to the North Europe region and providing high availability, you should use Azure Traffic Manager. Traffic Manager is a DNS-based traffic load balancer that allows you to distribute traffic optimally to services across global Azure regions while providing high availability.

Priority Traffic Routing: To ensure that users access the web app from the North Europe region unless it fails, use priority traffic routing. With priority routing, you can assign a priority value to each endpoint, and Traffic Manager routes the traffic to the endpoint with the highest priority available. In this case, assign a higher priority to the North Europe region, and a lower priority to the West Europe region. This will ensure that users are directed to the North Europe region as long as it is available, and to the West Europe region in case of a failure.

Question 20 Skipped

Your company has two on-premises sites in New York and Los Angeles and Azure virtual networks in the East US Azure region and the West US Azure region.

Each on-premises site has ExpressRoute Global Reach circuits to both regions.

You need to recommend a solution that meets the following requirements:

- Outbound traffic to the internet from workloads hosted on the virtual networks must be routed through the closest available on-premises site.
- If an on-premises site fails, traffic from the workloads on the virtual networks to the internet must reroute automatically to the other site.

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

NOTE: Each correct selection is worth one point.

Answer Area

Routing from the virtual networks to the on-premises locations must be configured by using:

- Azure default routes
- Border Gateway Protocol (BGP)
- User-defined routes

The automatic routing configuration following a failover must be handled by using:

- Border Gateway Protocol (BGP)
- Hot Standby Routing Protocol (HSRP)
- Virtual Router Redundancy Protocol (VRRP)

Routing from the virtual networks to the on-premises locations must be configured by using:

Azure default routes

Correct selection

Routing from the virtual networks to the on-premises locations must be configured by using:

Border Gateway Protocol (BGP)

Routing from the virtual networks to the on-premises locations must be configured by using:

User-defined routes

Correct selection

The automatic routing configuration following a failover must be handled by using:

Border Gateway Protocol (BGP)

The automatic routing configuration following a failover must be handled by using:

Hot Standby Routing Protocol (HSRP)

The automatic routing configuration following a failover must be handled by using:

Virtual Router Redundancy Protocol (VRRP)

Overall explanation

Answer Area

Routing from the virtual networks to the on-premises locations must be configured by using:

- Azure default routes
- Border Gateway Protocol (BGP)
- User-defined routes

The automatic routing configuration following a failover must be handled by using:

- Border Gateway Protocol (BGP)
- Hot Standby Routing Protocol (HSRP)
- Virtual Router Redundancy Protocol (VRRP)

Border Gateway Protocol (BGP): To configure routing between the Azure virtual networks and the on-premises locations, you should use Border Gateway Protocol (BGP). BGP is a dynamic routing protocol that enables automatic route updates between ExpressRoute circuits and the on-premises sites.

Border Gateway Protocol (BGP): BGP can also handle automatic routing configuration in the event of a failover. It can dynamically detect when a site fails and automatically reroute traffic to the other available site. This ensures that traffic from the workloads on the virtual networks to the internet is rerouted to the other on-premises site if one site fails.

Question 21 Skipped

You are designing an application that will use Azure Linux virtual machines to analyze video files. The files will be uploaded from corporate offices that connect to Azure by using ExpressRoute.

You plan to provision an Azure Storage account to host the files.

You need to ensure that the storage account meets the following requirements:

- Supports video files of up to 7 TB
- Provides the highest availability possible
- Ensures that storage is optimized for the large video files
- Ensures that files from the on-premises network are uploaded by using ExpressRoute

How should you configure the storage account? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Storage account type:

- Premium files shares
- Premium page blobs
- Standard general-purpose v2

Data redundancy:

- Zone-redundant storage (ZRS)
- Locally-redundant storage (LRS)
- Geo-redundant storage (GRS)

Networking:

- Azure Route Server
- A private endpoint
- A service endpoint

Storage account type:
Premium files shares

Storage account type:
Premium page blobs

Correct selection

Storage account type:
Standard general-purpose v2

Data redundancy:
Zone-redundant storage (ZRS)

Data redundancy:
Locally-redundant storage (LRS)

Correct selection

Data redundancy:
Geo-redundant storage (GRS)

Networking:
Azure Route Server

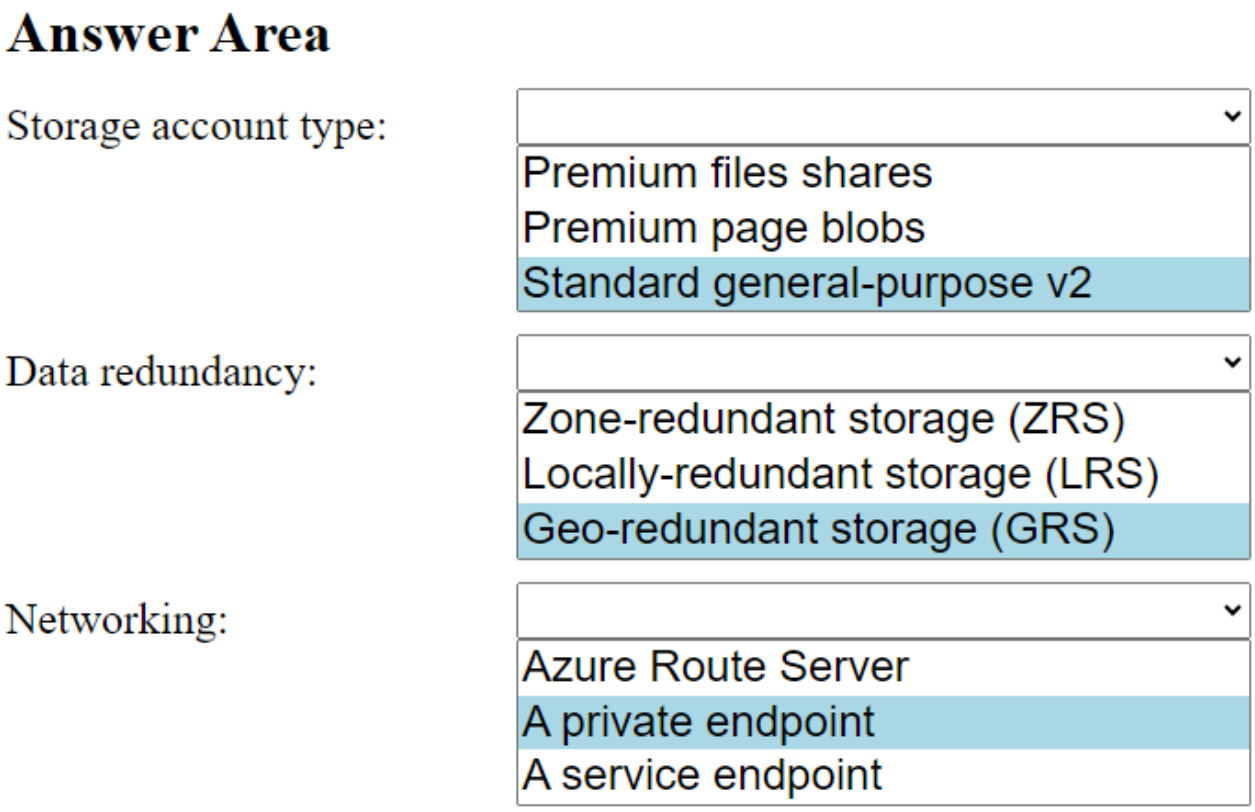
Correct selection

Networking:
A private endpoint

Networking:

A service endpoint

Overall explanation



Standard general-purpose v2 is the only storage account type that supports **Geo-redundant storage (GRS)** & meets the requirement for providing the highest availability possible.

ExpressRoute connects directly to the Azure network, bypassing the internet, so **private endpoint**.

Question 22 Skipped

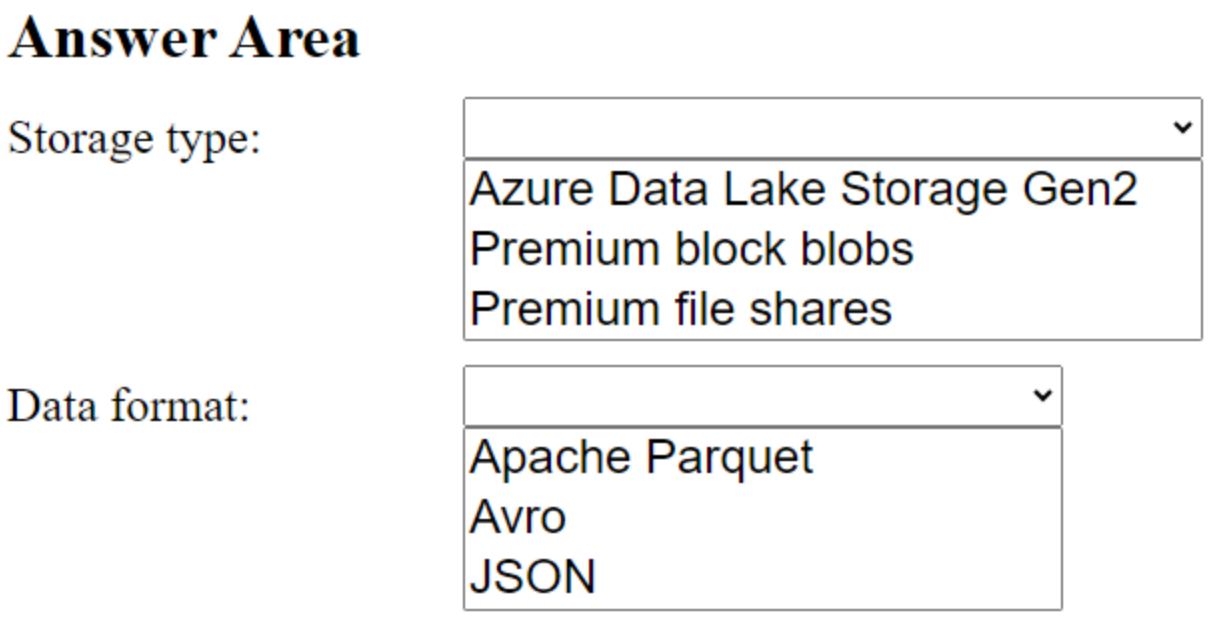
You have an app that generates 50,000 events daily.

You plan to stream the events to an Azure event hub and use Event Hubs Capture to implement cold path processing of the events. The output of Event Hubs Capture will be consumed by a reporting system.

You need to identify which type of Azure storage must be provisioned to support Event Hubs Capture, and which inbound data format the reporting system must support.

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

NOTE: Each correct selection is worth one point.



Correct selection

Storage type:
Azure Data Lake Storage Gen2

Storage type:
Premium block blobs

Storage type:
Premium file shares

Data format:
Apache Parquet

Correct selection

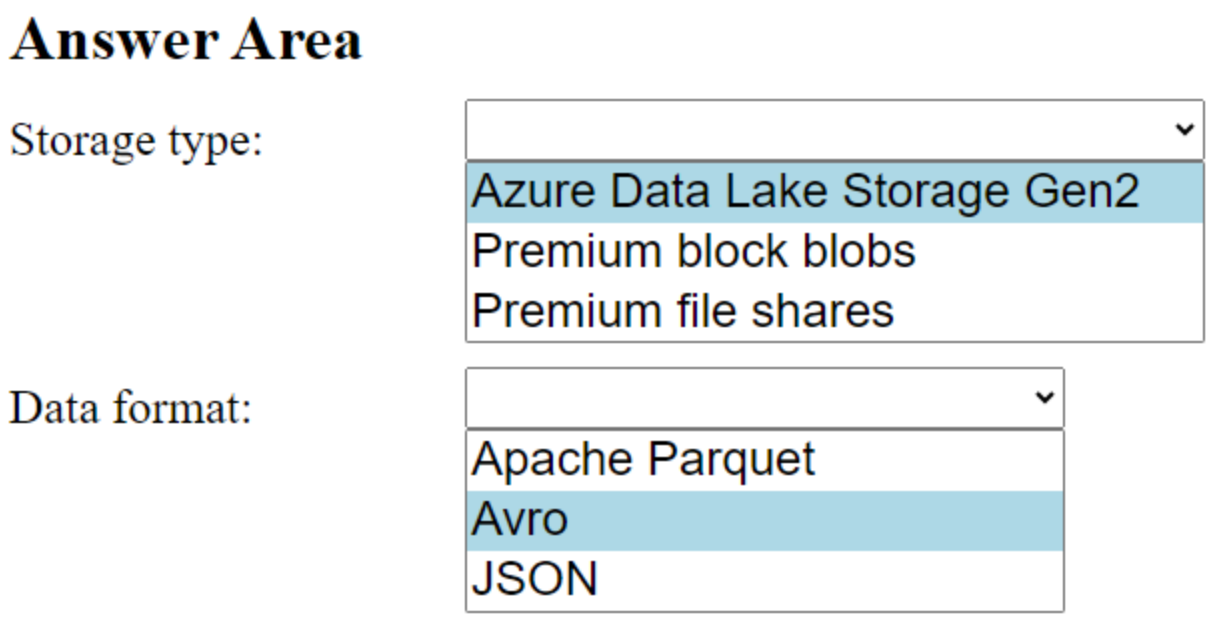
Data format:

Avro

Data format:

JSON

Overall explanation



Azure Data Lake Storage Gen2: Azure Event Hubs Capture allows captured data to be written either to Azure Blob Storage or Azure Data Lake Storage Gen2. Given the nature of the data and its use in reporting and analysis, Azure Data Lake Storage Gen2 is the more appropriate choice because it is designed for big data analytics.

Avro: Event Hubs Capture uses Avro format for the data it captures. Avro is a row-oriented format that is suitable for various data types, it's compact, fast, and binary, and enables efficient and fast serialization of data. This makes it a good choice for Event Hubs Capture.

Question 23 Skipped

You are designing a data analytics solution that will use Azure Synapse and Azure Data Lake Storage Gen2.

You need to recommend Azure Synapse pools to meet the following requirements:

- Ingest data from Data Lake Storage into hash-distributed tables.
- Implement query, and update data in Delta Lake.

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

NOTE: Each correct selection is worth one point.

Answer Area

Ingest data from Data Lake Storage into hash-distributed tables:

- A dedicated SQL pool
- A serverless Apache Spark pool
- A serverless SQL pool

Implement query, and update data in Delta Lake:

- A dedicated SQL pool
- A serverless Apache Spark pool
- A serverless SQL pool

Correct selection

Ingest data from Data Lake Storage into hash-distributed tables:
A dedicated SQL pool

Ingest data from Data Lake Storage into hash-distributed tables:
A serverless Apache Spark pool

Ingest data from Data Lake Storage into hash-distributed tables:
A serverless SQL pool

Implement query, and update data in Delta Lake:
A dedicated SQL pool

Correct selection

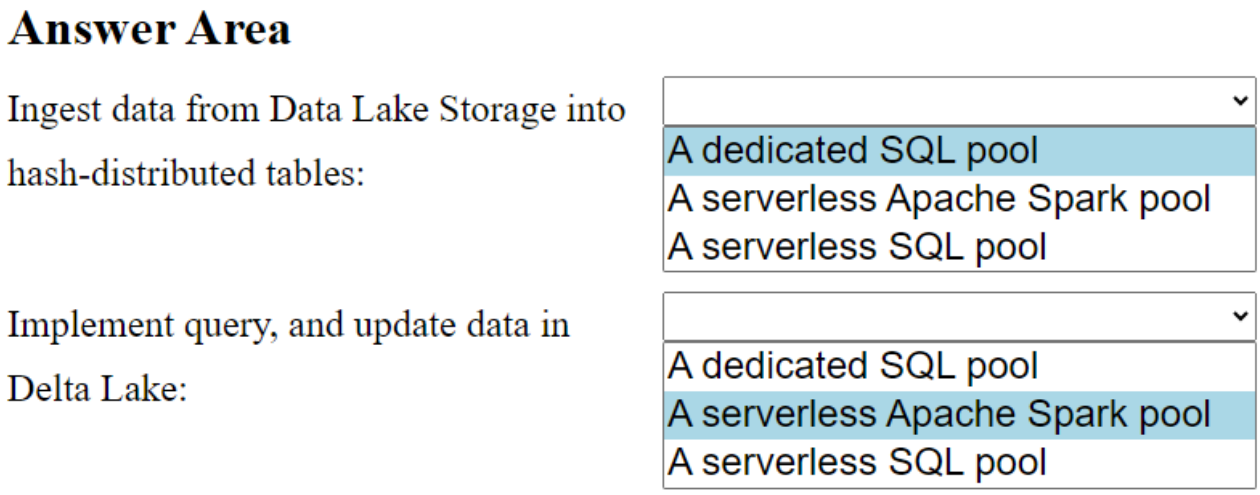
Implement query, and update data in Delta Lake:

A serverless Apache Spark pool

Implement query, and update data in Delta Lake:

A serverless SQL pool

Overall explanation



A dedicated SQL pool in Azure Synapse provides the ability to create hash-distributed tables, which help distribute data evenly across multiple nodes and improve query performance. This option is well-suited for ingesting data from Data Lake Storage into hash-distributed tables.

A serverless Apache Spark pool in Azure Synapse allows you to run Apache Spark jobs on-demand without having to manage the underlying infrastructure. This option is ideal for working with Delta Lake, as it provides native support for querying and updating data stored in Delta Lake format.

Question 24 Skipped

You are designing a data storage solution to support reporting.

The solution will ingest high volumes of data in the JSON format by using Azure Event Hubs. As the data arrives, Event Hubs will write the data to storage. The solution must meet the

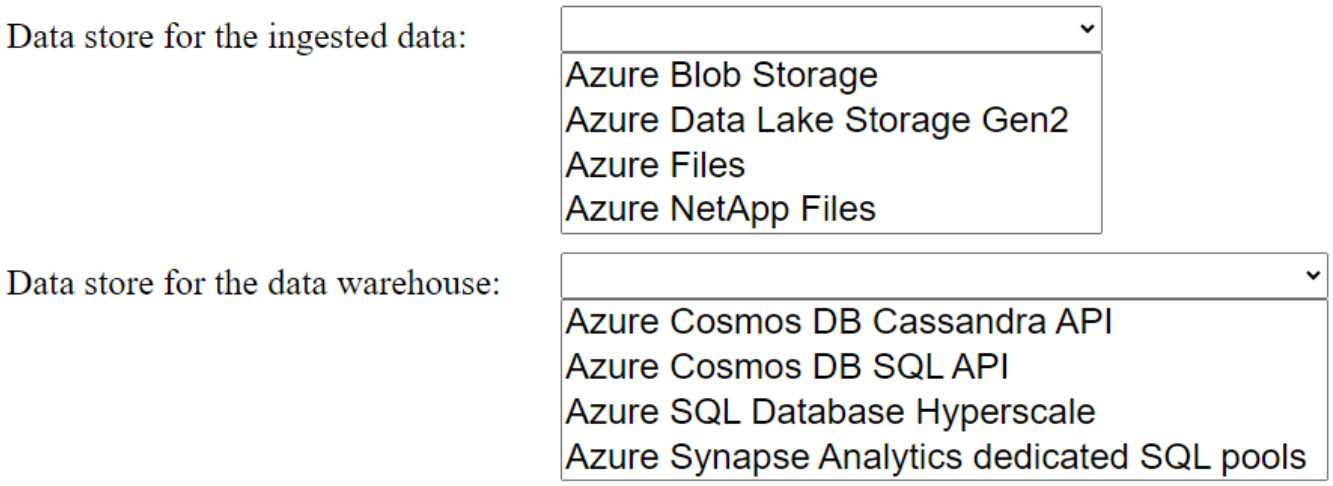
following requirements:

- Organize data in directories by date and time.
- Allow stored data to be queried directly, transformed into summarized tables, and then stored in a data warehouse.
- Ensure that the data warehouse can store 50 TB of relational data and support between 200 and 300 concurrent read operations.

Which service should you recommend for each type of data store? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area



Data store for the ingested data:
Azure Blob Storage

Correct selection

Data store for the ingested data:
Azure Data Lake Storage Gen2

Data store for the ingested data:
Azure Files

Data store for the ingested data:
Azure NetApp Files

Data store for the data warehouse:
Azure Cosmos DB Cassandra API

Data store for the data warehouse:
Azure Cosmos DB SQL API

Correct selection

Data store for the data warehouse:
Azure SQL Database Hyperscale

Data store for the data warehouse:
Azure Synapse Analytics dedicated SQL pools

Overall explanation

Answer Area

Data store for the ingested data:

- Azure Blob Storage
- Azure Data Lake Storage Gen2
- Azure Files
- Azure NetApp Files

Data store for the data warehouse:

- Azure Cosmos DB Cassandra API
- Azure Cosmos DB SQL API
- Azure SQL Database Hyperscale
- Azure Synapse Analytics dedicated SQL pools

Azure Data Lake Storage Gen2: Azure Data Explorer integrates with Azure Blob Storage and Azure Data Lake Storage (Gen1 and Gen2), providing fast, cached, and indexed

access to data stored in external storage. You can analyze and query data without prior ingestion into Azure Data Explorer. You can also query across ingested and uningested external data simultaneously. Azure Data Lake Storage is optimized storage for big data analytics workloads. Use cases: Batch, interactive, streaming analytics, and machine learning data such as log files, IoT data, click streams, and large datasets.

Azure SQL Database Hyperscale: Azure SQL Database Hyperscale is optimized for OLTP and high throughput analytics workloads with storage up to 100TB. A Hyperscale database supports up to 100 TB of data and provides high throughput and performance, as well as rapid scaling to adapt to the workload requirements. Connectivity, query processing, database engine features, etc. work like any other database in Azure SQL Database. Hyperscale is a multi-tiered architecture with caching at multiple levels. Effective IOPS will depend on the workload.

Compare to:

- General purpose: 500 IOPS per vCore with 7,000 maximum IOPS
- Business critical: 5,000 IOPS with 200,000 maximum IOPS

https://docs.microsoft.com/en-us/azure/data-explorer/data-lake-query-data

https://docs.microsoft.com/en-us/azure/azure-sql/database/service-tier-hyperscale

https://docs.microsoft.com/en-us/azure/synapse-analytics/sql-data-warehouse/sql-data-warehouse-service-capacity-limits

Question 25 Skipped

You are planning an Azure Storage solution for sensitive data. The data will be accessed daily. The dataset is less than 10 GB.

You need to recommend a storage solution that meets the following requirements:

- All the data written to storage must be retained for five years.
- Once the data is written, the data can only be read. Modifications and deletions must be prevented.
- After five years, the data can be deleted, but never modified.
- Data access charges must be minimized.

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

NOTE: Each correct selection is worth one point.

Answer Area

Storage account type:

- General purpose v2 with Archive access tier for blobs
- General purpose v2 with Cool access tier for blobs
- General purpose v2 with Hot access tier for blobs

Configuration to prevent modifications and deletions:

- Container access level
- Container access policy
- Storage account resource lock

Storage account type:

General purpose v2 with Archive access tier for blobs

Storage account type:

General purpose v2 with Cool access tier for blobs

Correct selection

Storage account type:

General purpose v2 with Hot access tier for blobs

Configuration to prevent modifications and deletions:

Container access level

Correct selection

Configuration to prevent modifications and deletions:

Container access policy

Configuration to prevent modifications and deletions:

Storage account resource lock

Overall explanation

Answer Area

Storage account type:

- General purpose v2 with Archive access tier for blobs
- General purpose v2 with Cool access tier for blobs
- General purpose v2 with Hot access tier for blobs

Configuration to prevent modifications and deletions:

- Container access level
- Container access policy
- Storage account resource lock

General purpose v2 with Hot access tier for blobs:

- All the data written to storage must be retained for five years.
- Data access charges must be minimized.

Hot tier has higher storage costs, but lower access and transaction costs.

Container access policy: The Container access policy is indeed the place to configure Azure's Immutable Blob Storage to ensure data is retained without modifications or deletions for a specified amount of time, which suits your needs. The Azure Blob Storage's Immutable Blob Storage feature provides a WORM (Write Once, Read Many) capability which aligns with your requirements perfectly.

Question 26 Skipped

You have an on-premises database that you plan to migrate to Azure.

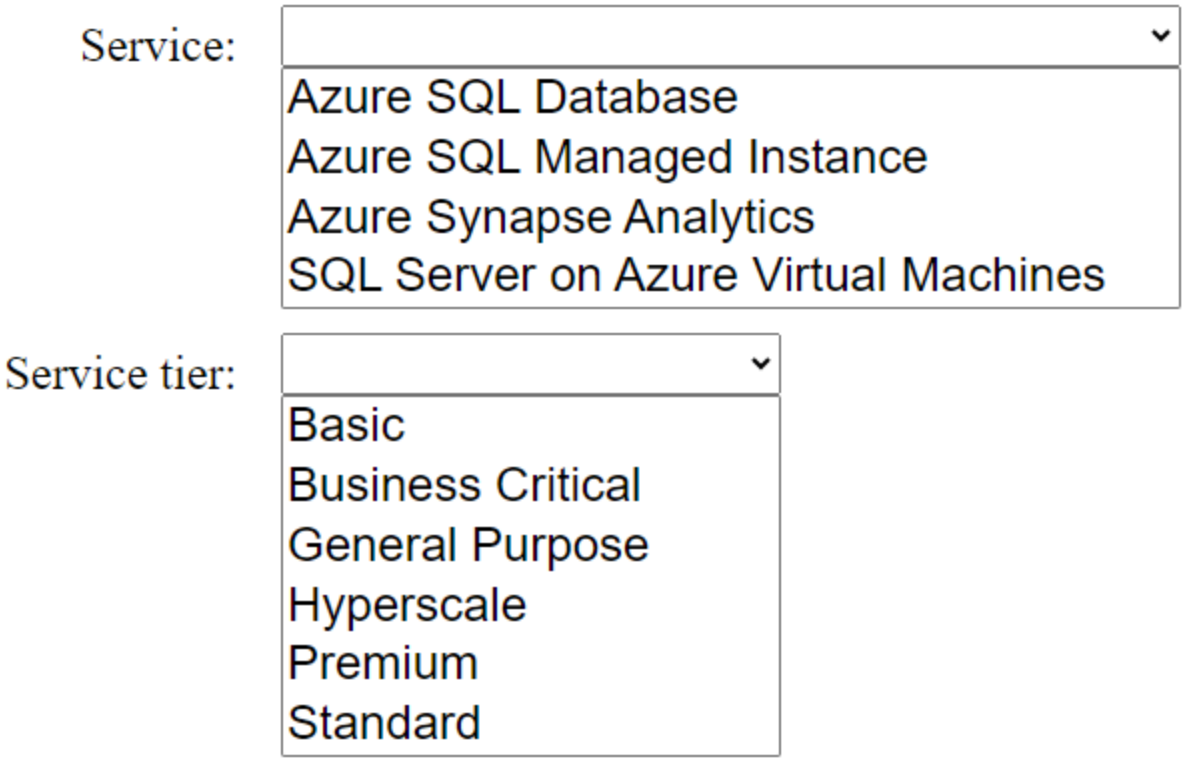
You need to design the database architecture to meet the following requirements:

- Support scaling up and down.
- Support geo-redundant backups.
- Support a database of up to 75 TB.
- Be optimized for online transaction processing (OLTP).

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

NOTE: Each correct selection is worth one point.

Answer Area



Correct selection

Service:

Azure SQL Database

Service:

Azure SQL Managed Instance

Service:

Azure Synapse Analytics

Service:

SQL Server on Azure Virtual Machines

Service tier:

Basic

Service tier:

Business Critical

Service tier:

General Purpose

Correct selection

Service tier:

Hyperscale

Service tier:

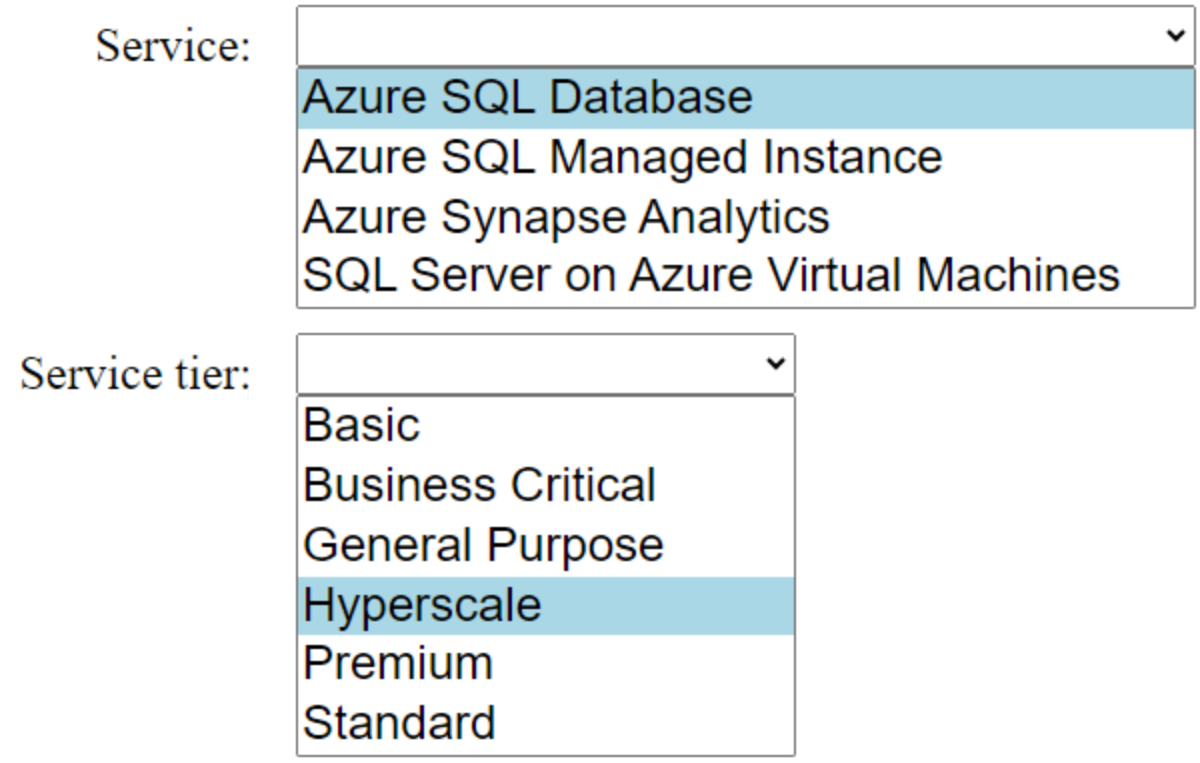
Premium

Service tier:

Standard

Overall explanation

Answer Area



Azure SQL Database: Database size always depends on the underlying service tiers (e.g. Basic, Business Critical, Hyperscale). It supports databases of up to 100 TB with a **Hyperscale** service tier model. Active geo-replication is a feature that lets you create a continuously synchronized readable secondary database for a primary database. The readable secondary database may be in the same Azure region as the primary, or, more commonly, in a different region. This kind of readable secondary database is also known as geo-secondaries or geo-replicas. Azure SQL Database and SQL Managed Instance enable you to dynamically add more resources to your database with minimal downtime.

https://docs.microsoft.com/en-us/azure/azure-sql/database/active-geo-replication-overview

https://medium.com/awesome-azure/azure-difference-between-azure-sql-database-and-sql-server-on-vm

Question 27 Skipped

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

Name	Type	Performance
storage1	StorageV2	Standard
storage2	StorageV2	Premium
storage3	BlobStorage	Standard
storage4	FileStorage	Premium

You plan to implement two new apps that have the requirements shown in the following table.

Name	Requirement
App1	Use lifecycle management to migrate app data between storage tiers
App2	Store app data in an Azure file share

Which storage accounts should you recommend using for each app? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

App1:

- Storage1 and storage2 only
- Storage1 and storage3 only
- Storage1, storage2, and storage3 only
- Storage1, storage2, storage3 and storage4

App2:

- Storage4 only
- Storage1 and storage4 only
- Storage1, storage2, and storage4 only
- Storage1, storage2, storage3, and storage4

App1:
Storage1 and storage2 only

Correct selection

App1:
Storage1 and storage3 only

App1:
Storage1, storage2, and storage3 only

App1:
Storage1, storage2, storage3 and storage4

App2:
Storage4 only

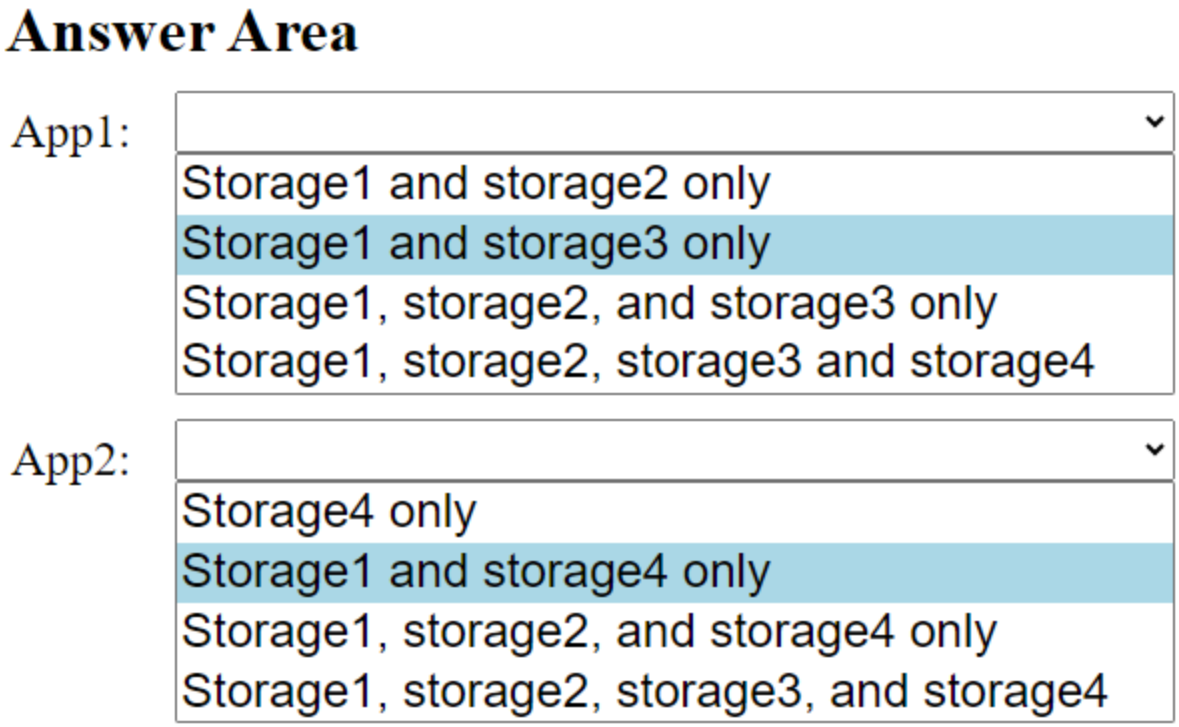
Correct selection

App2:
Storage1 and storage4 only

App2:
Storage1, storage2, and storage4 only

App2:
Storage1, storage2, storage3 and storage4

Overall explanation



Storage1 and storage3 only: Need to use Standard accounts. Data stored in a premium block blob storage account cannot be tiered to hot, cool, or archive using Set Blob Tier or using Azure Blob Storage lifecycle management.

Storage1 and storage4 only: Azure File shares require Premium accounts. Only Storage1 and storage4 are premium.

https://docs.microsoft.com/en-us/azure/storage/blobs/access-tiers-overview

https://docs.microsoft.com/en-us/azure/storage/files/storage-how-to-create-file-share

Question 28 Skipped

You need to design a storage solution for an app that will store large amounts of frequently used data. The solution must meet the following requirements:

- Maximize data throughput.
- Prevent the modification of data for one year.
- Minimize latency for read and write operations.

Which Azure Storage account type and storage service should you recommend? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Storage account type:

- BlobStorage
- BlockBlobStorage
- FileStorage
- StorageV2 with Premium performance
- StorageV2 with Standard performance

Storage service:

- Blob
- File
- Table

Storage account type:

BlobStorage

Correct selection

Storage account type:

BlockBlobStorage

Storage account type:

FileStorage

Storage account type:

StorageV2 with Premium performance

Storage account type:

StorageV2 with Standard performance

Correct selection

Storage service:

Blob

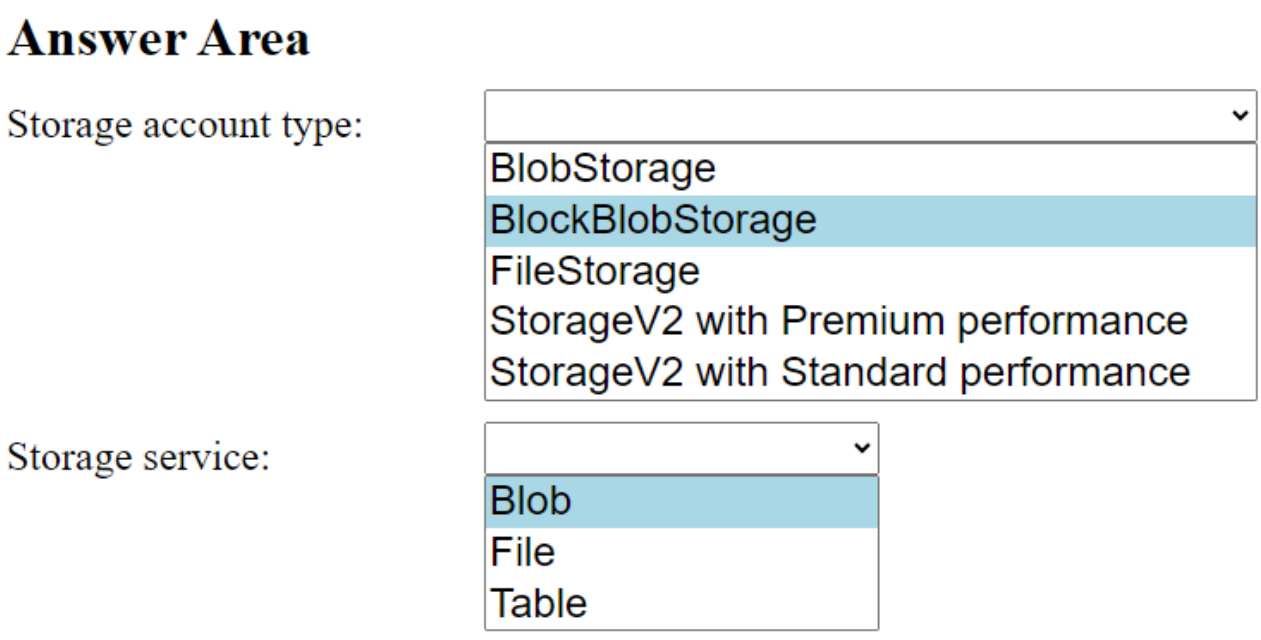
Storage service:

File

Storage service:

Table

Overall explanation



BlockBlobStorage - Block Blob is a premium storage account type for block blobs and append blobs. Recommended for scenarios with high transaction rates, or scenarios that use smaller objects or require consistently low storage latency.

Blob - The Archive tier is an offline tier for storing blob data that is rarely accessed. The Archive tier offers the lowest storage costs, but higher data retrieval costs and latency compared to the online tiers (Hot and Cool). Data must remain in the Archive tier for at least 180 days or be subject to an early deletion charge.

https://docs.microsoft.com/en-us/azure/storage/blobs/archive-blob

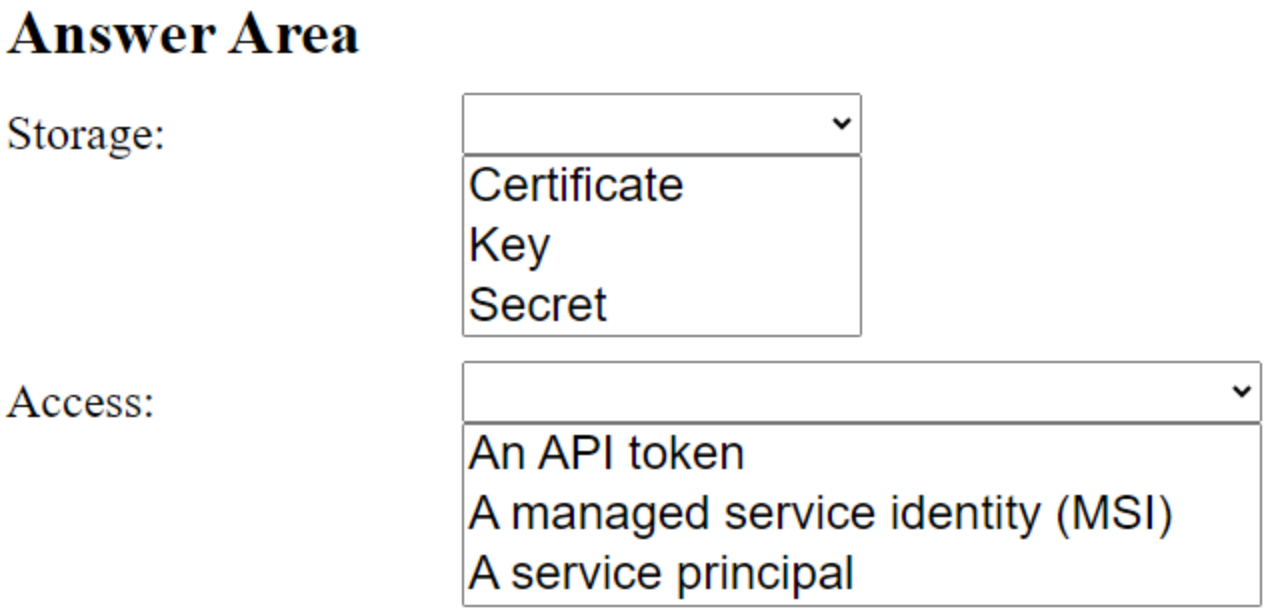
Question 29 Skipped

You are designing an app that will be hosted on Azure virtual machines that run Ubuntu. The app will use a third-party email service to send email messages to users. The third-party email service requires that the app authenticate by using an API key.

You need to recommend an Azure Key Vault solution for storing and accessing the API key. The solution must minimize administrative effort.

What should you recommend using to store and access the key? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Storage:

Certificate

Storage:

Key

Correct selection

Storage:

Secret

Access:

An API token

Correct selection

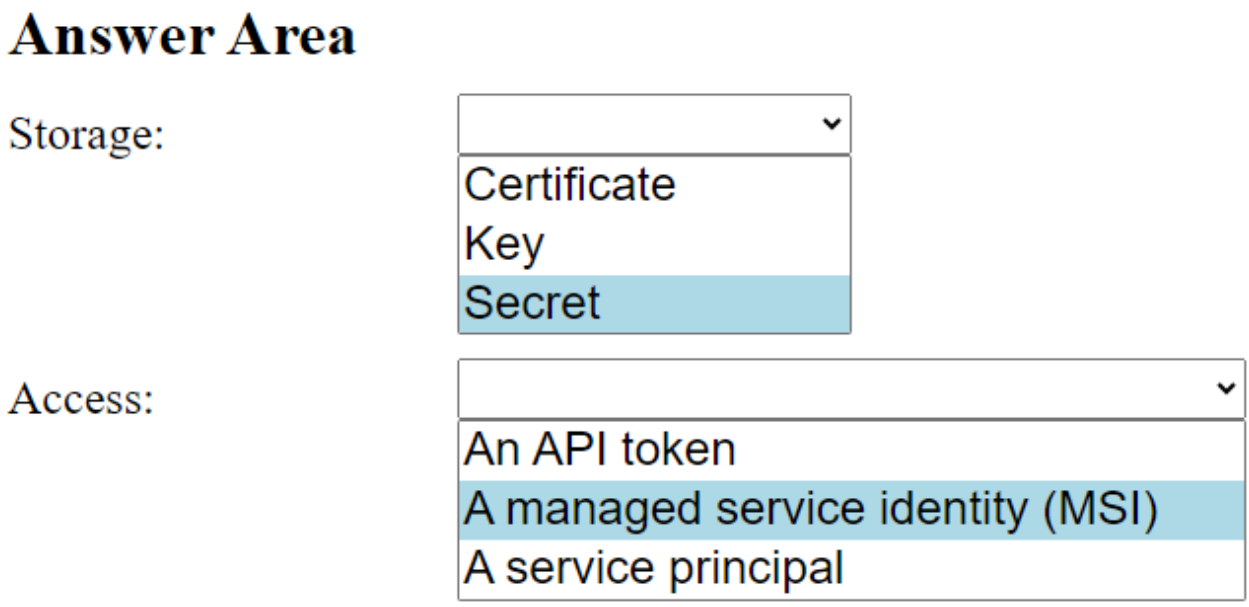
Access:

A managed service identity (MSI)

Access:

A service principal

Overall explanation



Secret: API keys are typically stored as secrets in Azure Key Vault. The key vault can store and manage secrets like API keys, passwords, or database connection strings.

A managed service identity (MSI): A managed service identity (MSI) is used to give your VM access to the key vault. The advantage of using MSI is that you do not have to manage credentials yourself. Azure takes care of rolling the credentials and ensuring their lifecycle. The application running on your VM can use its managed service identity to get a token to Azure AD, and then use that token to authenticate to Azure Key Vault.

Question 30 Skipped

You have an Azure subscription named Sub1 that is linked to an Azure AD tenant named contoso.com.

You plan to implement two ASP.NET Core apps named App1 and App2 that will be deployed to 100 virtual machines in Sub1. Users will sign in to App1 and App2 by using their contoso.com credentials.

App1 requires read permissions to access the calendar of the signed-in user. App2 requires write permissions to access the calendar of the signed-in user.

You need to recommend an authentication and authorization solution for the apps. The solution must meet the following requirements:

- Use the principle of least privilege.
- Minimize administrative effort.

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

NOTE: Each correct selection is worth one point.

Answer Area

Authentication:

- Application registration in Azure AD
- A system-assigned managed identity
- A user-assigned managed identity

Authorization:

- Application permissions
- Azure role-based access control (Azure RBAC)
- Delegated permissions

Correct selection

Authentication:

Application registration in Azure AD

Authentication:

A system-assigned managed identity

Authentication:

A user-assigned managed identity

Authorization:

Application permissions

Authorization:

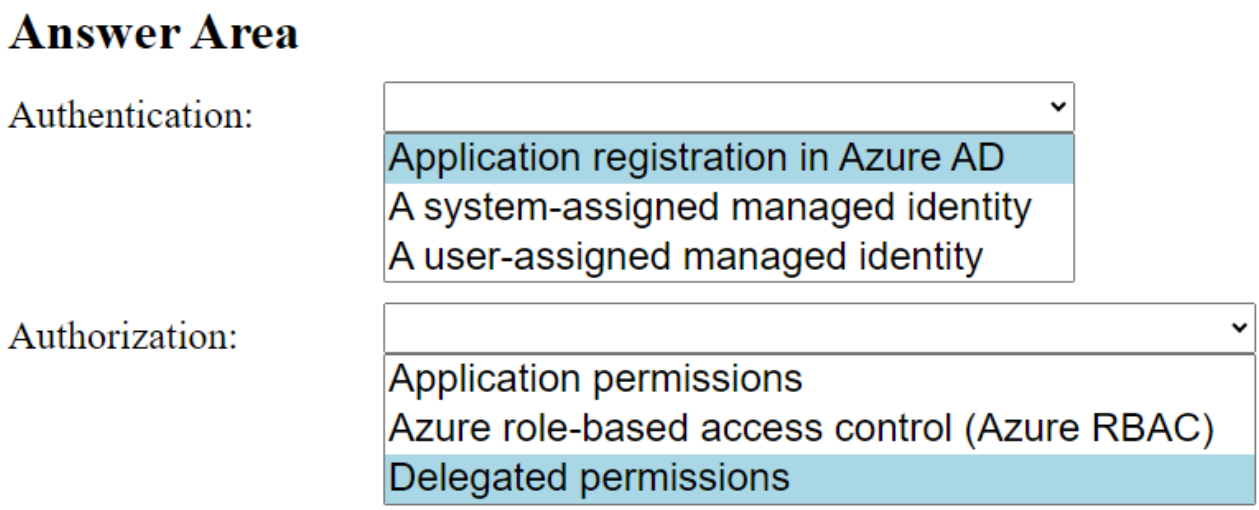
Azure role-based access control (Azure RBAC)

Correct selection

Authorization:

Delegated permissions

Overall explanation



The important point here is that both apps are deployed to the same machines. So Managed identity will violate the principle of least privilege. As a user/system-managed identity will have to be assigned both read and write permission to the user's calendar.

App registration will provide the ability to use the service principal per app to set the correct permission required for the app.

https://learn.microsoft.com/en-us/azure/active-directory/develop/app-objects-and-service-principals

Use **delegated permissions** to access user's data as admin allowed/forces users to delegate the permission to the app.

https://learn.microsoft.com/en-us/azure/active-directory/develop/permissions-consent-overview

Question 31 Skipped

You have an Azure subscription that contains an Azure key vault named KV1 and a virtual machine named VM1. VM1 runs Windows Server 2022: Azure Edition.

You plan to deploy an ASP.Net Core-based application named App1 to VM1.

You need to configure App1 to use a system-assigned managed identity to retrieve secrets from KV1. The solution must minimize development efforts.

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

NOTE: Each correct selection is worth one point.

Answer Area

Configure App1 to use OAuth 2.0:

- Authorization code grant flows
- Client credentials grant flows
- Implicit grant flows

Configure App1 to use a REST API call to retrieve an authentication token from the:

- Azure Instance Metadata Service (MDS) endpoint
- OAuth 2.0 access token endpoint of Azure AD
- OAuth 2.0 access token endpoint of Microsoft Identity Platform

Configure App1 to use OAuth 2.0:

Authorization code grant flows

Correct selection

Configure App1 to use OAuth 2.0:

Client credentials grant flows

Configure App1 to use OAuth 2.0:

Implicit grant flows

Configure App1 to use a REST API call to retrieve an authentication token from the:

Azure Instance Metadata Service (MDS) endpoint

Correct selection

Configure App1 to use a REST API call to retrieve an authentication token from the:

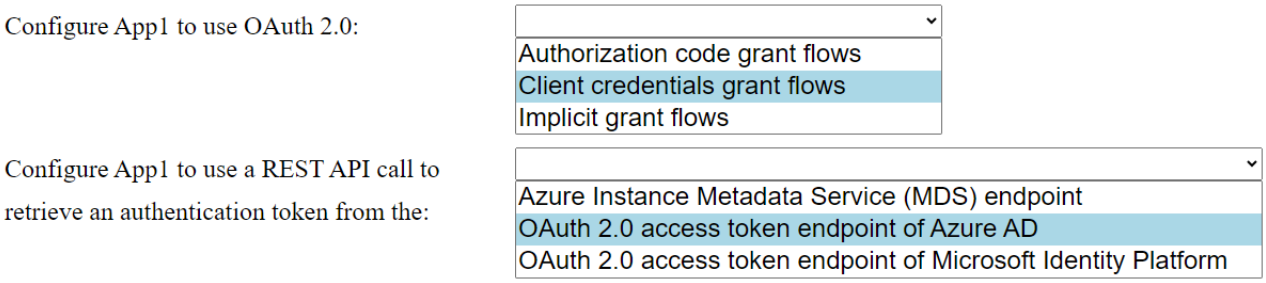
OAuth 2.0 access token endpoint of Azure AD

Configure App1 to use a REST API call to retrieve an authentication token from the:

OAuth 2.0 access token endpoint of Microsoft Identity Platform

Overall explanation

Answer Area



Client credentials grant flows: We need server-based authentication so client credentials are to be used.

https://learn.microsoft.com/en-us/azure/active-directory/develop/v2-oauth2-auth-code-flow

OAuth 2.0 access token endpoint of Azure AD: Because Microsoft Identity Platform is user based.

https://learn.microsoft.com/en-us/azure/active-directory/develop/v2-overview

Question 32 Skipped

Your company has 20 web APIs that were developed in-house.

The company is developing 10 web apps that will use the web APIs. The web apps and the APIs are registered in the company s Azure Active Directory (Azure AD) tenant. The web APIs are published by using Azure API Management.

You need to recommend a solution to block unauthorized requests originating from the web apps from reaching the web APIs. The solution must meet the following requirements:

- Use Azure AD-generated claims.
- Minimize configuration and management efforts.

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

NOTE: Each correct selection is worth one point.

Answer Area

Grant permissions to allow the web apps to access the web APIs by using:

- Azure AD
- Azure API Management
- The web APIs

Configure a JSON Web Token (JWT) validation policy by using:

- Azure AD
- Azure API Management
- The web APIs

Correct selection

Grant permissions to allow the web apps to access the web APIs by using:
Azure AD

Grant permissions to allow the web apps to access the web APIs by using:
Azure API Management

Grant permissions to allow the web apps to access the web APIs by using:
The web APIs

Configure a JSON Web Token (JWT) validation policy by using:
Azure AD

Correct selection

Configure a JSON Web Token (JWT) validation policy by using:
Azure API Management

Configure a JSON Web Token (JWT) validation policy by using:
The web APIs

Overall explanation

Answer Area

Grant permissions to allow the web apps to access the web APIs by using:

- Azure AD
- Azure API Management
- The web APIs

Configure a JSON Web Token (JWT) validation policy by using:

- Azure AD
- Azure API Management
- The web APIs

Azure AD - Grant permissions in Azure AD.

Azure API Management - Configure a JWT validation policy to pre-authorize requests. Pre-authorize requests in API Management with the Validate JWT policy, by validating the access tokens of each incoming request. If a request does not have a valid token, API Management blocks it.

https://docs.microsoft.com/en-us/azure/api-management/api-management-howto-protect-backend-with-aad

Question 33 Skipped

You have an Azure subscription that contains a virtual network named VNET1 and 10 virtual machines. The virtual machines are connected to VNET1.

You need to design a solution to manage virtual machines from the internet. The solution must meet the following requirements:

- Incoming connections to the virtual machines must be authenticated by using Azure Multi-Factor Authentication (MFA) before network connectivity is allowed.
- Incoming connections must use TLS and connect to TCP port 443.
- The solution must support RDP and SSH.

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

NOTE: Each correct selection is worth one point.

Answer Area

To provide access to virtual machines on VNET1, use:

- Azure Bastion
- Just-in-time (JIT) VM access
- Azure Web Application Firewall (WAF) in Azure Front Door

To enforce Azure MFA, use:

- An Azure Identity Governance access package
- A Conditional Access policy that has the Cloud apps assignment set to Azure Windows VM Sign-In
- A Conditional Access policy that has the Cloud apps assignment set to Microsoft Azure Management

Correct selection

To provide access to virtual machines on VNET1, use:

Azure Bastion

To provide access to virtual machines on VNET1, use:

Just-in-time (JIT) VM access

To provide access to virtual machines on VNET1, use:

Azure Web Application Firewall (WAF) in Azure Front Door

To enforce Azure MFA, use:

An Azure Identity Governance access package

Correct selection

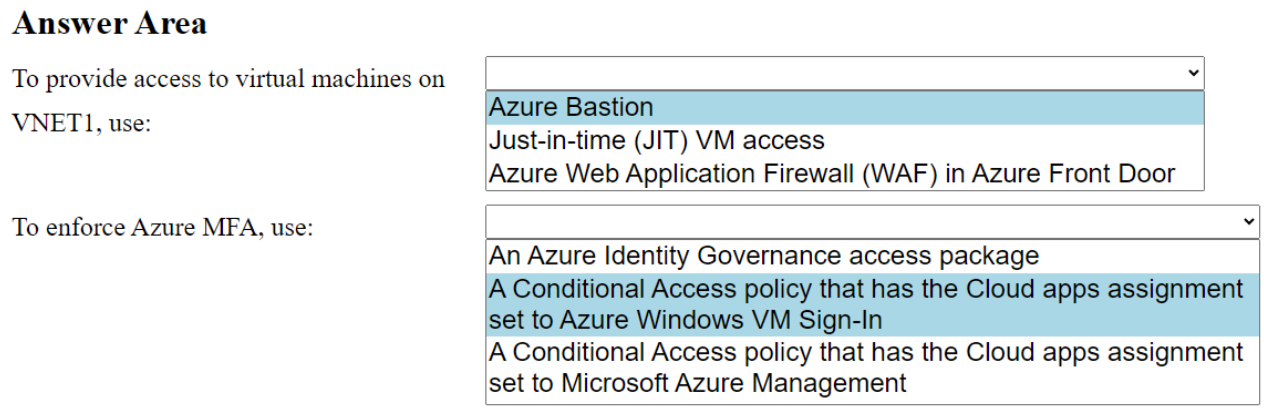
To enforce Azure MFA, use:

A Conditional Access policy that has the Cloud apps assignment set to Azure Windows VM Sign-In

To enforce Azure MFA, use:

A Conditional Access policy that has the Cloud apps assignment set to Microsoft Azure Management

Overall explanation



Azure Bastion: It provides secure and seamless RDP/SSH connectivity to your virtual machines directly from the Azure portal over TLS.

https://docs.microsoft.com/en-us/azure/bastion/bastion-overview

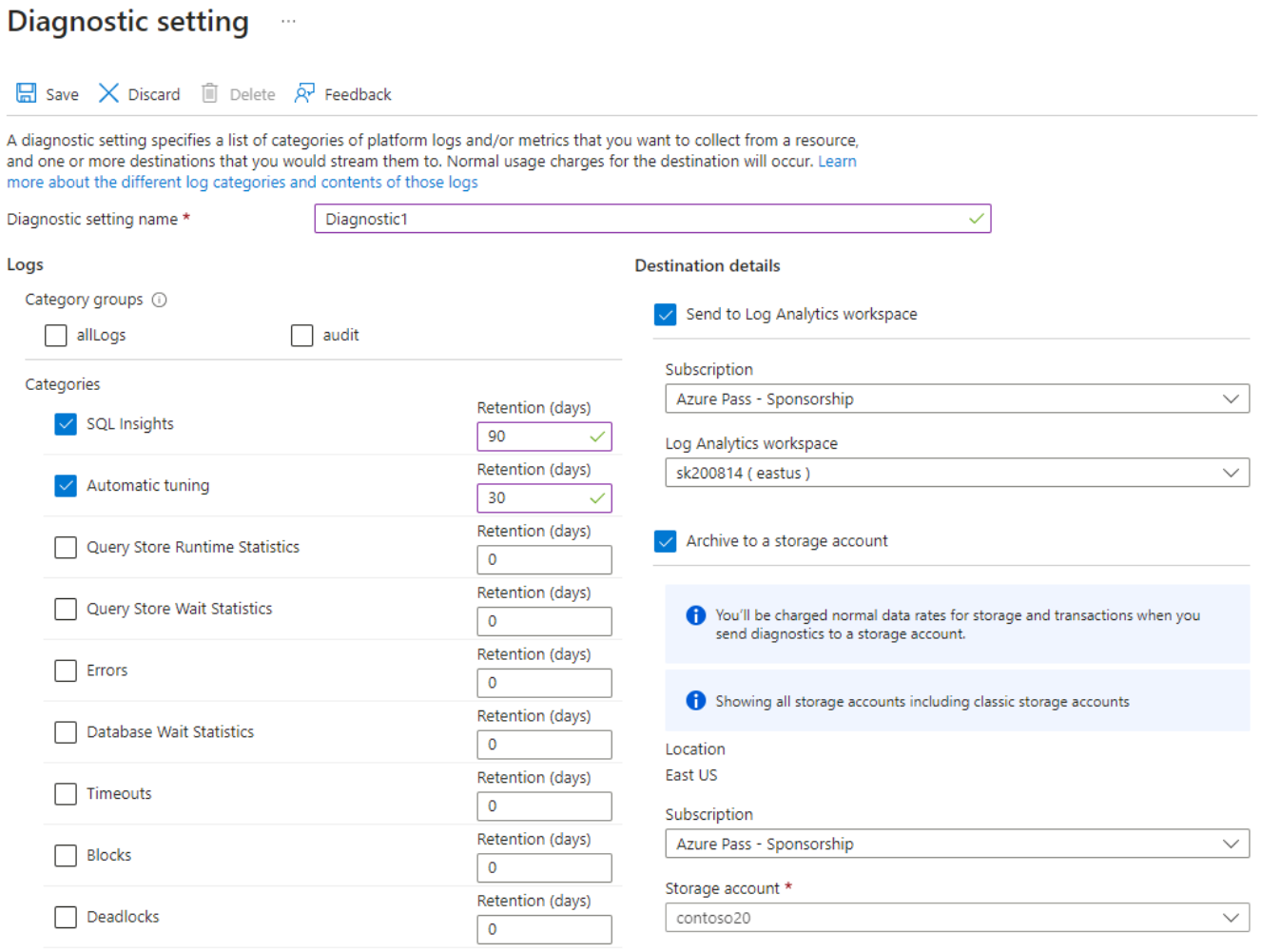
A conditional Access policy that has Cloud Apps assignment set to Azure Windows VM Sign-In: You can enforce Conditional Access policies such as multi-factor authentication or user sign-in risk check before authorizing access to Windows VMs in Azure that are enabled with Azure AD sign-in. To apply the Conditional Access policy, you must select the "Azure Windows VM Sign-In" app from the cloud apps or actions assignment option and then use Sign-in risk as a condition and/or require multi-factor authentication as a grant access control.

https://docs.microsoft.com/en-us/azure/active-directory/devices/howto-vm-sign-in-azure-ad-windows

Question 34 Skipped

You deploy several Azure SQL Database instances.

You plan to configure the Diagnostics settings on the databases as shown in the following exhibit.



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

NOTE: Each correct selection is worth one point.

Answer Area

The amount of time that SQLInsights data will be stored in blob storage is:

- 30 days
- 90 days
- 730 days
- indefinite

The maximum amount of time that SQLInsights data can be stored in Azure Log Analytics is:

- 30 days
- 90 days
- 730 days
- indefinite

The amount of time that SQLInsights data will be stored in blob storage is:

30 days

Correct selection

The amount of time that SQLInsights data will be stored in blob storage is:

90 days

The amount of time that SQLInsights data will be stored in blob storage is:

730 days

The amount of time that SQLInsights data will be stored in blob storage is:

indefinite

The maximum amount of time that SQLInsights data can be stored in Azure Log Analytics is:

30 days

The maximum amount of time that SQLInsights data can be stored in Azure Log Analytics is:

90 days

Correct selection

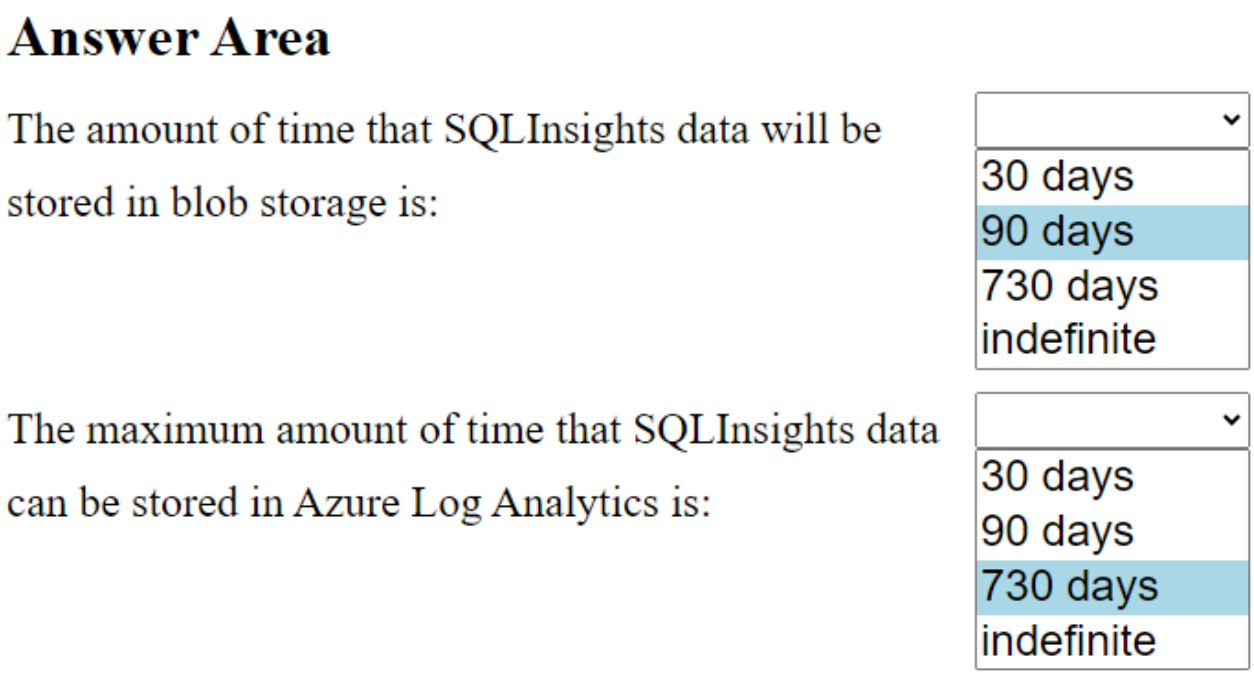
The maximum amount of time that SQLInsights data can be stored in Azure Log Analytics is:

730 days

The maximum amount of time that SQLInsights data can be stored in Azure Log Analytics is:

indefinite

Overall explanation



90 days - As per exhibit.

730 days - Raw data points (that is, items that you can query in Analytics and inspect in Search) are kept for up to 730 days.

https://docs.microsoft.com/en-us/azure/azure-monitor/app/data-retention-privacy

Question 35 Skipped

You have an Azure App Service web app that uses a system-assigned managed identity.

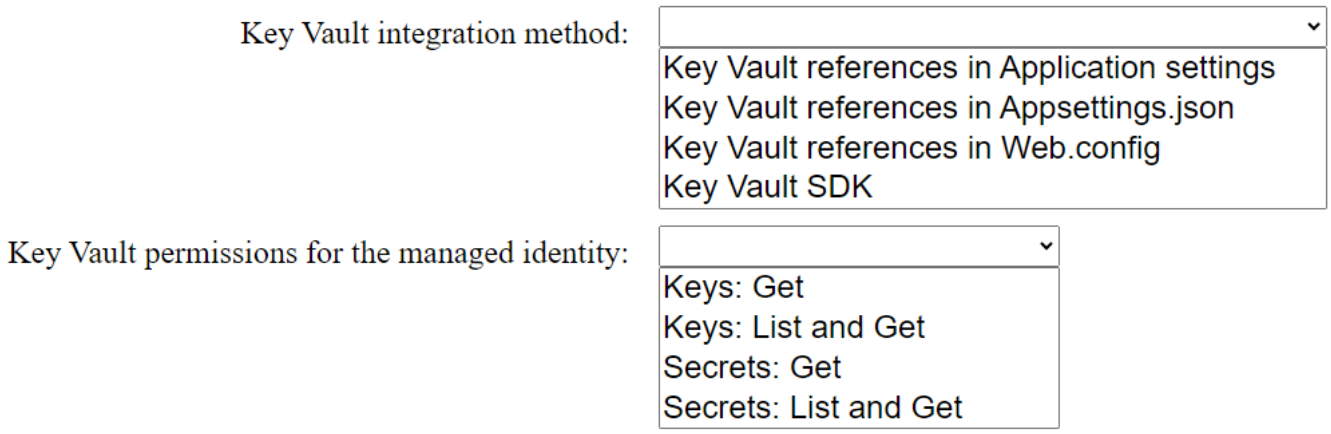
You need to recommend a solution to store the settings of the web app as secrets in an Azure key vault. The solution must meet the following requirements:

- Minimize changes to the app code.
- Use the principle of least privilege.

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

NOTE: Each correct selection is worth one point.

Answer Area



Correct selection

Key Vault integration method:

Key Vault references in Application settings

Key Vault integration method:

Key Vault references in Appsettings.json

Key Vault integration method:

Key Vault references in Web.config

Key Vault integration method:

Key Vault SDK

Key Vault permissions for the managed identity:

Keys: Get

Key Vault permissions for the managed identity:

Keys: List and Get

Correct selection

Key Vault permissions for the managed identity:

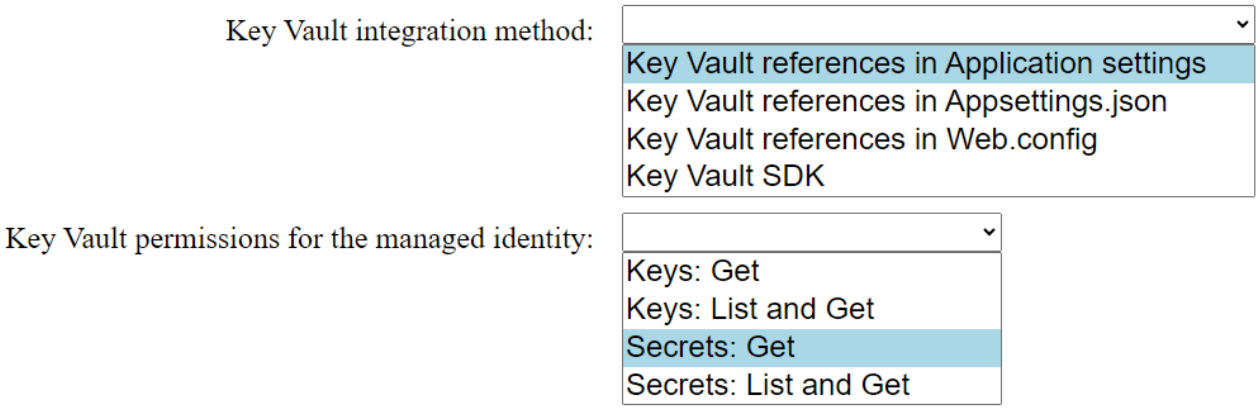
Secrets: Get

Key Vault permissions for the managed identity:

Secrets: List and Get

Overall explanation

Answer Area



Key Vault references in Application settings: Source Application Settings from Key Vault.

Key Vault references can be used as values for Application Settings, allowing you to keep secrets in Key Vault instead of the site config. Application Settings are securely encrypted at rest, but if you need secret management capabilities, they should go into Key Vault.

To use a Key Vault reference for an app setting, set the reference as the value of the setting. Your app can reference the secret through its key as normal. No code changes are required.

Secrets: Get: In order to read secrets from Key Vault, you need to have a vault created and give your app permission to access it.

- Create a key vault by following the Key Vault quickstart.
- Create a managed identity for your application.
- Key Vault references will use the app's system-assigned identity by default, but you can specify a user-assigned identity.
- Create an access policy in Key Vault for the application identity you created earlier. Enable the "Get" secret permission on this policy.

https://docs.microsoft.com/en-us/azure/app-service/app-service-key-vault-references

Question 36 Skipped

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

Name	Type	Description
App1	Azure App Service	None
Workspace1	Log Analytics Workspace	Configured to use a pay-as-you-go pricing tier
App1Logs	Log Analytics Table	Hosted in Workspace1, configured to use the Analytics Logs data plan

Log files from App1 are registered to App1Logs. An average of 120 GB of log data is ingested per day.

You configure an Azure Monitor alert that will be triggered if the App1 logs contain error messages.

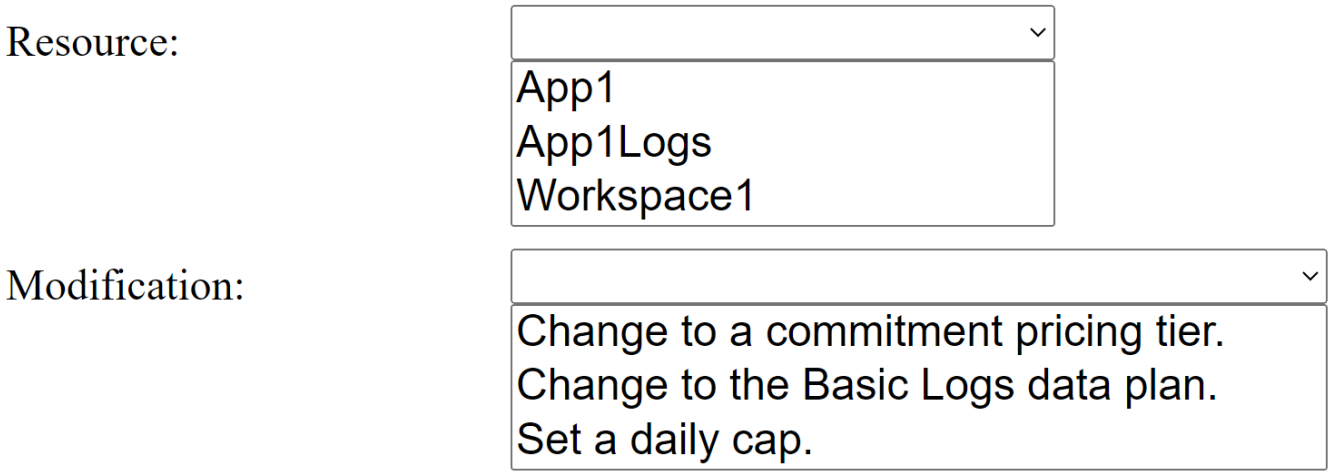
You need to minimize the Log Analytics costs associated with App1. The solution must meet the following requirements:

- Ensure that all the log files from App1 are ingested into App1Logs.
- Minimize the impact on the Azure Monitor alert.

Which resource should you modify, and which modification should you perform? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area



Resource:

App1

Resource:

App1Logs

Correct selection

Resource:

Workspace1

Correct selection

Modification:

Change to a commitment pricing tier.

Modification:

Change to the Basic Logs data plan.

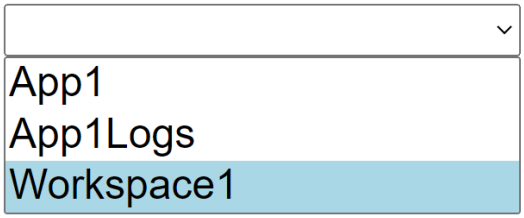
Modification:

Set a daily cap.

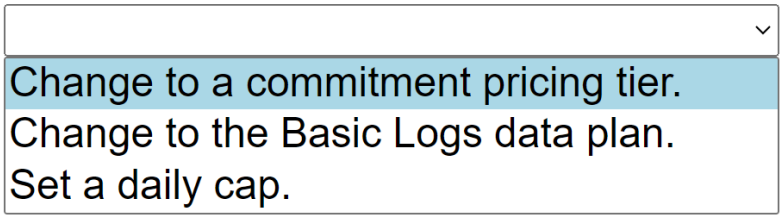
Overall explanation

Answer Area

Resource:



Modification:



- **Workspace1:** This is the Log Analytics workspace where the logs are ingested. Modifying this resource helps manage costs associated with log ingestion.
- **Change to a commitment pricing tier:** Commitment tiers offer discounted rates for log ingestion based on a fixed commitment, which can significantly reduce costs compared to the pay-as-you-go pricing tier, especially when dealing with large volumes of data like 120 GB per day. This change ensures that all log files are ingested while minimizing costs and impact on the Azure Monitor alert.

Question 37 Skipped

You have an Azure subscription that contains multiple storage accounts.

You assign Azure Policy definitions to the storage accounts.

You need to recommend a solution to meet the following requirements:

- Trigger on-demand Azure Policy compliance scans.
- Raise Azure Monitor non-compliance alerts by querying logs collected by Log Analytics.

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

NOTE: Each correct selection is worth one point.

Answer Area

To trigger the compliance scans, use:

An Azure Template
The Azure Command-Line Interface (CLI)
The Azure Portal

To generate the non-compliance alerts, configure diagnostic settings for the:

Azure activity logs
Log Analytics workspace
Storage accounts

To trigger the compliance scans, use:
An Azure Template

Correct selection

To trigger the compliance scans, use:
The Azure Command-Line Interface (CLI)

To trigger the compliance scans, use:
The Azure Portal

To generate the non-compliance alerts, configure diagnostic settings for the:
Azure activity logs

Correct selection

To generate the non-compliance alerts, configure diagnostic settings for the:
Log Analytics workspace

To generate the non-compliance alerts, configure diagnostic settings for the:
Storage accounts

Overall explanation

Answer Area

To trigger the compliance scans, use:

- An Azure Template
- The Azure Command-Line Interface (CLI)
- The Azure Portal

To generate the non-compliance alerts, configure diagnostic settings for the:

- Azure activity logs
- Log Analytics workspace
- Storage accounts

- **The Azure Command-Line Interface (CLI):** The Azure CLI allows you to run compliance scans on-demand using the `az policy state trigger-scan` command.
- **Log Analytics workspace:** By configuring diagnostic settings to send the compliance data to a Log Analytics workspace, you can create queries and set up alerts based on the non-compliance logs.

Question 38 Skipped

You have an Azure subscription.

You plan to deploy five storage accounts that will store block blobs and five storage accounts that will host file shares. The file shares will be accessed by using the SMB protocol.

You need to recommend an access authorization solution for the storage accounts. The solution must meet the following requirements:

- Maximize security.
- Prevent the use of shared keys.
- Whenever possible, support time-limited access.

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

NOTE: Each correct selection is worth one point.

Answer Area

For the blobs:

- A user delegation shared access signature (SAS) only
- A shared access signature (SAS) and a stored access policy
- A user delegation shared access signature (SAS) and a stored access policy

For the file shares:

- Azure AD credentials
- A user delegation shared access signature (SAS) only
- A user delegation shared access signature (SAS) and a stored access policy

Correct selection

For the blobs:

A user delegation shared access signature (SAS) only

For the blobs:

A shared access signature (SAS) and a stored access policy

For the blobs:

A user delegation shared access signature (SAS) and a stored access policy

Correct selection

For the file shares:

Azure AD credentials

For the file shares:

A user delegation shared access signature (SAS) only

For the file shares:

A user delegation shared access signature (SAS) and a stored access policy

Overall explanation

Answer Area

For the blobs:

- A user delegation shared access signature (SAS) only
- A shared access signature (SAS) and a stored access policy
- A user delegation shared access signature (SAS) and a stored access policy

For the file shares:

- Azure AD credentials
- A user delegation shared access signature (SAS) only
- A user delegation shared access signature (SAS) and a stored access policy

1. **For the blobs: A user delegation shared access signature (SAS) only**

   To enhance security, it is advisable to use a user delegation SAS (Shared Access Signature). According to Azure documentation, it is recommended to use Azure AD credentials whenever possible instead of account keys, as account keys are more susceptible to compromise. If your application needs shared access signatures, leveraging Azure AD credentials to create a user delegation SAS ensures improved security. This approach also eliminates the use of shared keys and supports time-limited access. However, note that user delegation SAS does not support stored access policies.

2. **For the file shares: Azure AD credentials**

   The solution maximizes security according to Microsoft's highest recommendations. While it does not support time-limited access, this feature is optional and of lower priority compared to security.

Question 39 Skipped

You have an Azure subscription. The subscription contains 100 virtual machines that run Windows Server 2022 and have the Azure Monitor Agent installed.

You need to recommend a solution that meets the following requirements:

- Forwards JSON-formatted logs from the virtual machines to a Log Analytics workspace
- Transforms the logs and stores the data in a table in the Log Analytics workspace

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

NOTE: Each correct selection is worth one point.

Answer Area

To forward the logs:

- A linked storage account for the Log Analytics workspace
- An Azure Monitor data collection endpoint
- A service endpoint

To transform the logs and store the data:

- A KQL query
- A WQL query
- An XPath query

To forward the logs:

A linked storage account for the Log Analytics workspace

Correct selection

To forward the logs:

An Azure Monitor data collection endpoint

To forward the logs:

A service endpoint

Correct selection

To transform the logs and store the data:

A KQL query

To transform the logs and store the data:

A WQL query

To transform the logs and store the data:

An XPath query

Overall explanation

Answer Area

To forward the logs:

- A linked storage account for the Log Analytics workspace
- An Azure Monitor data collection endpoint
- A service endpoint

To transform the logs and store the data:

- A KQL query
- A WQL query
- An XPath query

1. **To forward the logs: An Azure Monitor data collection endpoint**

   This endpoint allows you to ingest data directly into a Log Analytics workspace from various sources, including virtual machines with the Azure Monitor Agent installed.

2. **To transform the logs and store the data: A KQL query**

   Kusto Query Language (KQL) is used within Azure Monitor to transform and query log data, making it suitable for storing and analyzing the logs in a Log Analytics workspace.

Question 40 Skipped

You have five Azure subscriptions. Each subscription is linked to a separate Azure AD tenant and contains virtual machines that run Windows Server 2022.

You plan to collect Windows security events from the virtual machines and send them to a single Log Analytics workspace.

You need to recommend a solution that meets the following requirements:

- Collects event logs from multiple subscriptions
- Supports the use of data collection rules (DCRs) to define which events to collect

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

NOTE: Each correct selection is worth one point.

Answer Area

To collect the event logs:

- Azure Event Grid
- Azure Lighthouse
- Azure Purview

To support the DCRs:

- The Log Analytics agent
- The Azure Monitor agent
- The Azure Connected Machine agent

To collect the event logs:

Azure Event Grid

Correct selection

To collect the event logs:

Azure Lighthouse

To collect the event logs:

Azure Purview

To support the DCRs:

The Log Analytics agent

Correct selection

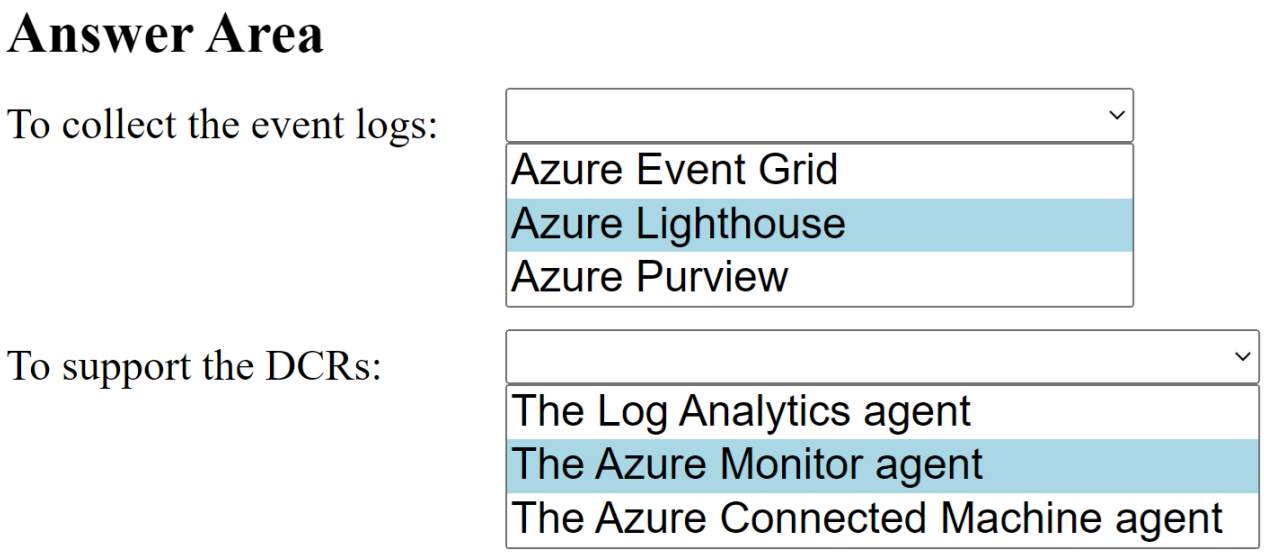
To support the DCRs:

The Azure Monitor agent

To support the DCRs:

The Azure Connected Machine agent

Overall explanation



1. **To collect the event logs: Azure Lighthouse**

   Azure Lighthouse allows you to manage multiple Azure subscriptions and tenants from a single control plane. It provides the capability to deploy and manage resources at scale across multiple subscriptions, making it suitable for this requirement.

2. **To support the DCRs: The Azure Monitor agent**

   The Azure Monitor agent supports data collection rules (DCRs) which can be used to define which events to collect from the virtual machines. This agent is designed to work with Log Analytics and provides a more flexible and scalable approach to data collection compared to the older Log Analytics agent.

Back to result overview

Scroll back to top