HOTSPOT -

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.

Hot Area:

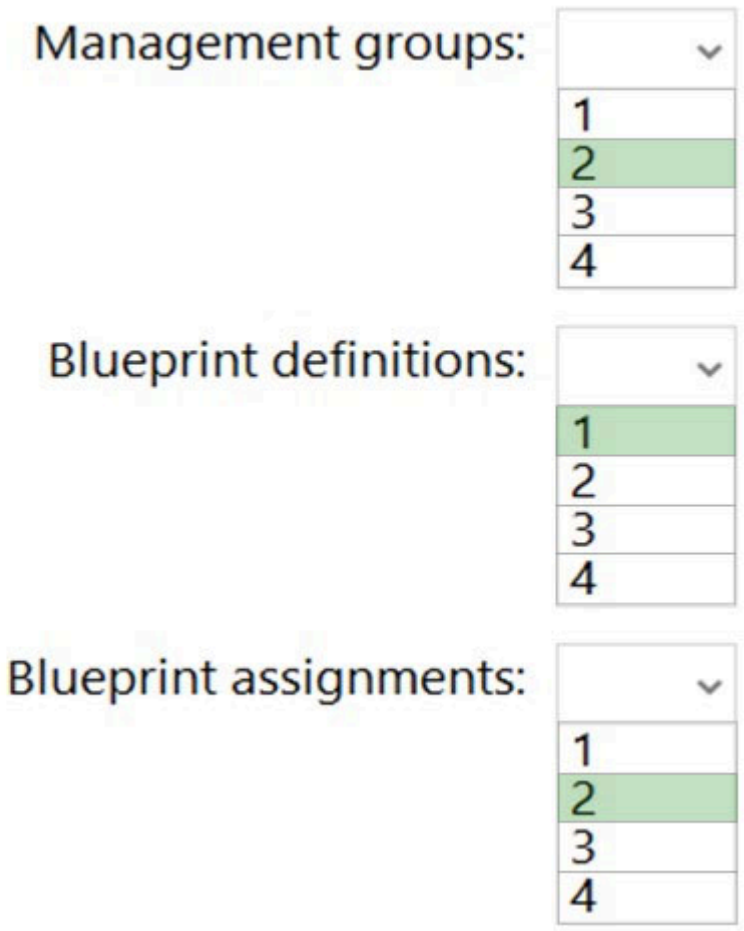
Answer Area

Management groups: 1 / 2 / 3 / 4

Blueprint definitions: 1 / 2 / 3 / 4

Blueprint assignments: 1 / 2 / 3 / 4

Answer Area



Correct Answer:

Box 1: 2 -
One management group for each Azure AD tenant
Azure management groups provide a level of scope above subscriptions.
All subscriptions within a management group automatically inherit the conditions applied to the management group.
All subscriptions within a single management group must trust the same Azure Active Directory tenant.

Box 2: 1 -
One single blueprint definition can be assigned to different existing management groups or subscriptions.
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.

Box 3: 2 -

Blueprint assignment -
Each Published Version of a blueprint can be assigned (with a max name length of 90 characters) to an existing management group or subscription.
Assigning a blueprint definition to a management group means the assignment object exists at the management group. The deployment of artifacts still targets a subscription.
Reference:
https://docs.microsoft.com/en-us/azure/governance/management-groups/overview https://docs.microsoft.com/en-us/azure/governance/blueprints/overview

HOTSPOT -

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.

Hot Area:

Answer Area

Azure Policy effect to use:
- Append
- EnforceOPAConstraint
- EnforceRegoPolicy
- Modify

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
- A managed identity with the User Access Administrator role
- A service principal with the Contributor role
- A service principal with the User Access Administrator role

Correct Answer:

Answer Area

Azure Policy effect to use:
- Append
- EnforceOPAConstraint
- EnforceRegoPolicy
- Modify

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
- A managed identity with the User Access Administrator role
- A service principal with the Contributor role
- A service principal with the User Access Administrator role

Box 1: 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 costCenter. 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.

Incorrect:

* The following effects are deprecated: EnforceOPAConstraint EnforceRegoPolicy
* Append is used to add additional fields to the requested resource during creation or update. A common example is specifying allowed IPs for a storage resource.

Append is intended for use with non-tag properties. While Append can add tags to a resource during a create or update request, it's recommended to use the

Modify effect for tags instead.

Box 2: 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.

Incorrect:

User Access Administrator: lets you manage user access to Azure resources.

Reference:

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

HOTSPOT -

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

Name	Type	Account Kind	Location
storage1	Azure Storage account	Storage (general purpose v1)	East US
storage2	Azure Storage account	StorageV2 (general purpose v2)	East US
Workspace1	Azure Log Analytics workspace	**Not applicable**	East US
Workspace2	Azure Log Analytics workspace	**Not applicable**	East US
Hub1	Azure event hub	**Not applicable**	East US

You create an Azure SQL database named DB1 that is hosted in the East US Azure region.

To DB1, you add a diagnostic setting named Settings1. Settings1 archive SQLInsights to storage1 and sends SQLInsights to Workspace1.

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

Hot Area:

Answer Area

Statements	Yes	No
You can add a new diagnostic setting that archives SQLInsights logs to storage2.	○	○
You can add a new diagnostic setting that sends SQLInsights logs to Workspace2.	○	○
You can add a new diagnostic setting that sends SQLInsights logs to Hub1.	○	○

Correct Answer:

Answer Area

Statements	Yes	No
You can add a new diagnostic setting that archives SQLInsights logs to storage2.	○	○
You can add a new diagnostic setting that sends SQLInsights logs to Workspace2.	○	○
You can add a new diagnostic setting that sends SQLInsights logs to Hub1.	○	○

Box 1: Yes -

A single diagnostic setting can define no more than one of each of the destinations. If you want to send data to more than one of a particular destination type (for example, two different Log Analytics workspaces), then create multiple settings.

Each resource can have up to 5 diagnostic settings.

Note: This diagnostic telemetry can be streamed to one of the following Azure resources for analysis.

* Log Analytics workspace
* Azure Event Hubs
* Azure Storage

Box 2: Yes -

Box 3: Yes -

Reference:

https://docs.microsoft.com/en-us/azure/azure-monitor/essentials/diagnostic-settings https://docs.microsoft.com/en-us/azure/azure-sql/database/metrics-diagnostic-telemetry-logging-streaming-export-configure?tabs=azure-portal

Question #22 *Topic 1*

You plan to deploy an Azure SQL database that will store Personally Identifiable Information (PII).
You need to ensure that only privileged users can view the PII.
What should you include in the solution?

A. dynamic data masking

B. role-based access control (RBAC)

C. Data Discovery & Classification

D. Transparent Data Encryption (TDE)

Correct Answer: *A*
Dynamic data masking limits sensitive data exposure by masking it to non-privileged users.
Dynamic data masking helps prevent unauthorized access to sensitive data by enabling customers to designate how much of the sensitive data to reveal with minimal impact on the application layer. It's a policy-based security feature that hides the sensitive data in the result set of a query over designated database fields, while the data in the database is not changed.
Reference:
https://docs.microsoft.com/en-us/azure/azure-sql/database/dynamic-data-masking-overview

Community vote distribution

A (100%)

Question #23 *Topic 1*

You plan to deploy an app that will use an Azure Storage account.
You need to deploy the storage account. The storage account must meet the following requirements:
- Store the data for multiple users.
- Encrypt each user's data by using a separate key.
- Encrypt all the data in the storage account by using customer-managed keys.

What should you deploy?

A. files in a premium file share storage account

B. blobs in a general purpose v2 storage account

C. blobs in an Azure Data Lake Storage Gen2 account

D. files in a general purpose v2 storage account

Correct Answer: *B*
You can specify a customer-provided key on Blob storage operations. A client making a read or write request against Blob storage can include an encryption key on the request for granular control over how blob data is encrypted and decrypted.
Reference:
https://docs.microsoft.com/en-us/azure/storage/common/storage-service-encryption

Community vote distribution

B (93%) 7%

HOTSPOT -

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:

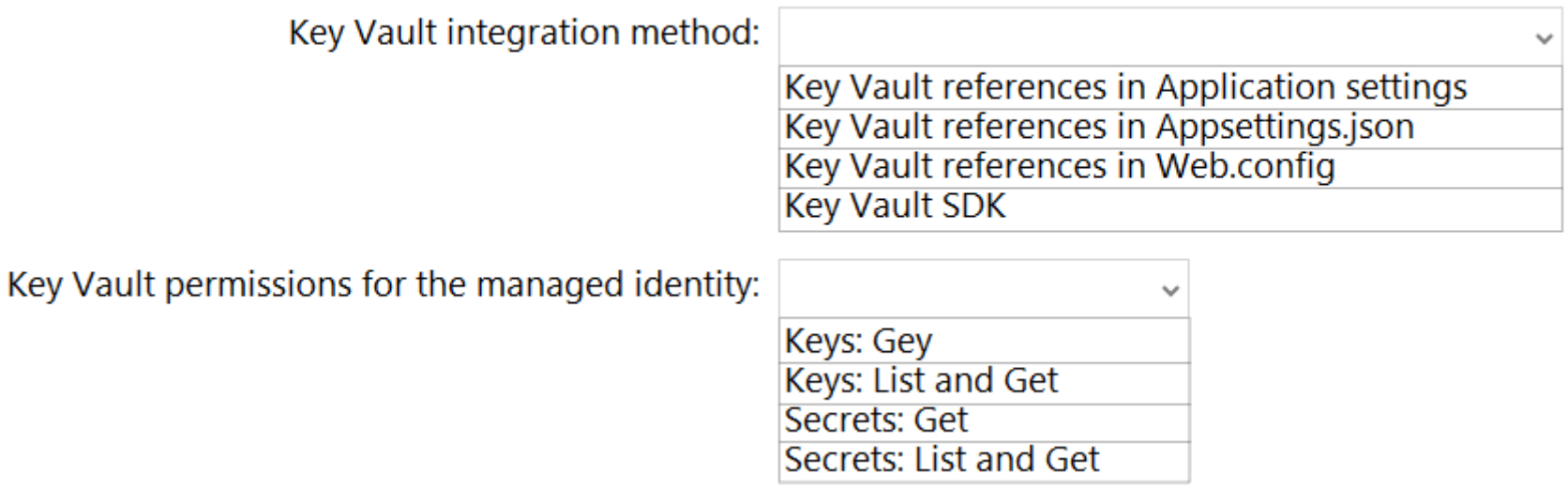
- Minimize changes to the app code.
- Use the principle of least privilege.

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.

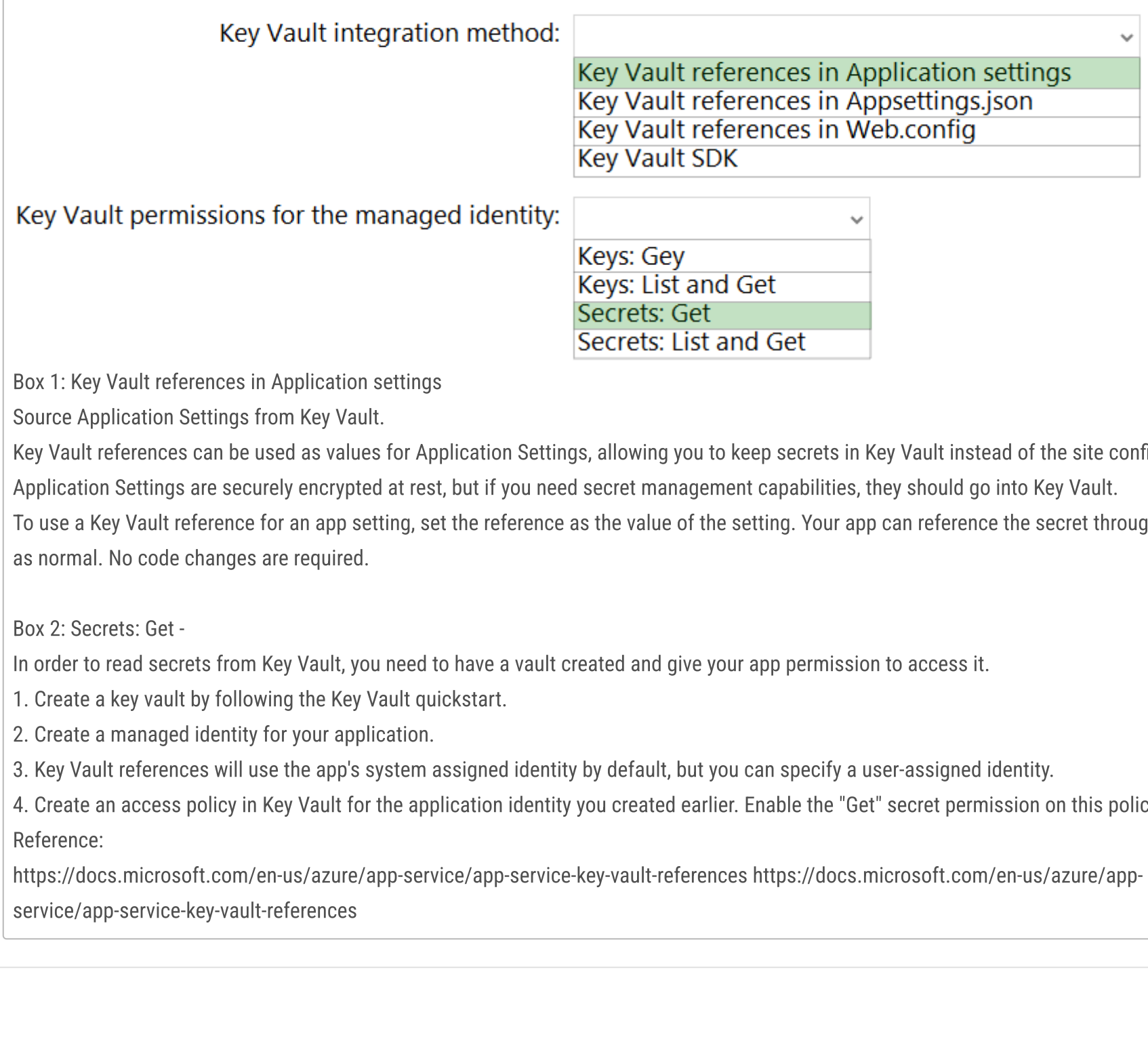
Hot Area:

Answer Area



Correct Answer:

Answer Area



Box 1: 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.

Box 2: 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.

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

Reference:

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

Question #25 *Topic 1*

You plan to deploy an application named App1 that will run on five Azure virtual machines. Additional virtual machines will be deployed later to run App1.
You need to recommend a solution to meet the following requirements for the virtual machines that will run App1:
☞ Ensure that the virtual machines can authenticate to Azure Active Directory (Azure AD) to gain access to an Azure key vault, Azure Logic Apps instances, and an Azure SQL database.
☞ Avoid assigning new roles and permissions for Azure services when you deploy additional virtual machines.
☞ Avoid storing secrets and certificates on the virtual machines.
☞ Minimize administrative effort for managing identities.
Which type of identity should you include in the recommendation?

A. a system-assigned managed identity

B. a service principal that is configured to use a certificate

C. a service principal that is configured to use a client secret

D. a user-assigned managed identity

Correct Answer: *D*
Managed identities provide an identity for applications to use when connecting to resources that support Azure Active Directory (Azure AD) authentication.
A user-assigned managed identity:
Can be shared.
The same user-assigned managed identity can be associated with more than one Azure resource.
Common usage:
Workloads that run on multiple resources and can share a single identity.
For example, a workload where multiple virtual machines need to access the same resource.
Incorrect:
Not A: A system-assigned managed identity can't be shared. It can only be associated with a single Azure resource.
Typical usage:
Workloads that are contained within a single Azure resource.
Workloads for which you need independent identities.
For example, an application that runs on a single virtual machine.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/overview

Community vote distribution

D (100%)

You have the resources shown in the following table:

Name	Type
AS1	Azure Synapse Analytics instance
CDB1	Azure Cosmos DB SQL API account

CDB1 hosts a container that stores continuously updated operational data.

You are designing a solution that will use AS1 to analyze the operational data daily.

You need to recommend a solution to analyze the data without affecting the performance of the operational data store.

What should you include in the recommendation?

A. Azure Cosmos DB change feed

B. Azure Data Factory with Azure Cosmos DB and Azure Synapse Analytics connectors

C. Azure Synapse Link for Azure Cosmos DB

D. Azure Synapse Analytics with PolyBase data loading

Correct Answer: *C*

Azure Synapse Link for Azure Cosmos DB creates a tight integration between Azure Cosmos DB and Azure Synapse Analytics. It enables customers to run near real-time analytics over their operational data with full performance isolation from their transactional workloads and without an ETL pipeline.

Reference:

https://docs.microsoft.com/en-us/azure/cosmos-db/synapse-link-frequently-asked-questions

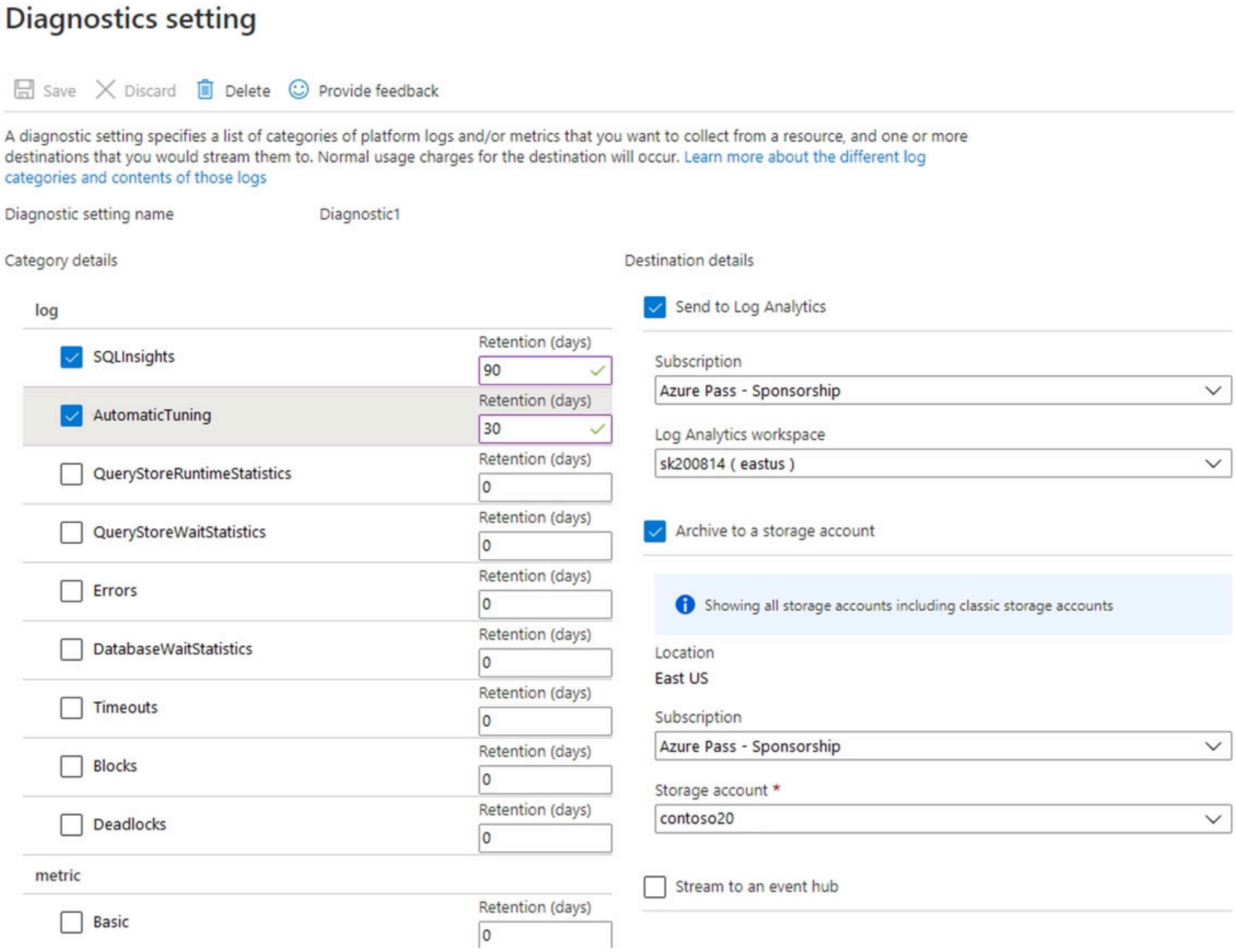
Community vote distribution

C (100%)

HOTSPOT -

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.

Hot Area:

Answer Area

The amount of time that SQLInsights data will be stored in blob storage is **[answer choice]**.

- 30 days
- 90 days
- 730 days
- indefinite

The maximum amount of time that SQLInsights data can be stored in Azure Log Analytics is **[answer choice]**.

- 30 days
- 90 days
- 730 days
- indefinite

Answer Area

The amount of time that SQLInsights data will be stored in blob storage is **[answer choice]**.

- 30 days
- 90 days
- 730 days
- indefinite

Correct Answer:

The maximum amount of time that SQLInsights data can be stored in Azure Log Analytics is **[answer choice]**.

- 30 days
- 90 days
- 730 days
- indefinite

Box 1: 90 days -

As per exhibit.

Box 2: 730 days -

How long is the data kept?

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

Reference:

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

Question #28 *Topic 1*

You have an application that is used by 6,000 users to validate their vacation requests. The application manages its own credential store. Users must enter a username and password to access the application. The application does NOT support identity providers.

You plan to upgrade the application to use single sign-on (SSO) authentication by using an Azure Active Directory (Azure AD) application registration.

Which SSO method should you use?

A. header-based

B. SAML

C. password-based

D. OpenID Connect

Correct Answer: *C*

Password - On-premises applications can use a password-based method for SSO. This choice works when applications are configured for Application Proxy.

With password-based SSO, users sign in to the application with a username and password the first time they access it. After the first sign-on, Azure AD provides the username and password to the application. Password-based SSO enables secure application password storage and replay using a web browser extension or mobile app. This option uses the existing sign-in process provided by the application, enables an administrator to manage the passwords, and doesn't require the user to know the password.

Incorrect:

Choosing an SSO method depends on how the application is configured for authentication. Cloud applications can use federation-based options, such as OpenID

Connect, OAuth, and SAML.

Federation - When you set up SSO to work between multiple identity providers, it's called federation.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/what-is-single-sign-on

Community vote distribution

C (100%)