QUESTION 16
You have an Azure Active Directory (Azure AD) tenant named contoso.com that has a security group named Group1. Group1 is configured for assigned membership. Group1 has 50 members, including 20 guest users.
You need to recommend a solution for evaluating the membership of Group1. The solution must meet the following requirements:
- The evaluation must be repeated automatically every three months.
- Every member must be able to report whether they need to be in Group1.
- Users who report that they do not need to be in Group1 must be removed from Group1 automatically.
- Users who do not report whether they need to be in Group1 must be removed from Group1 automatically.

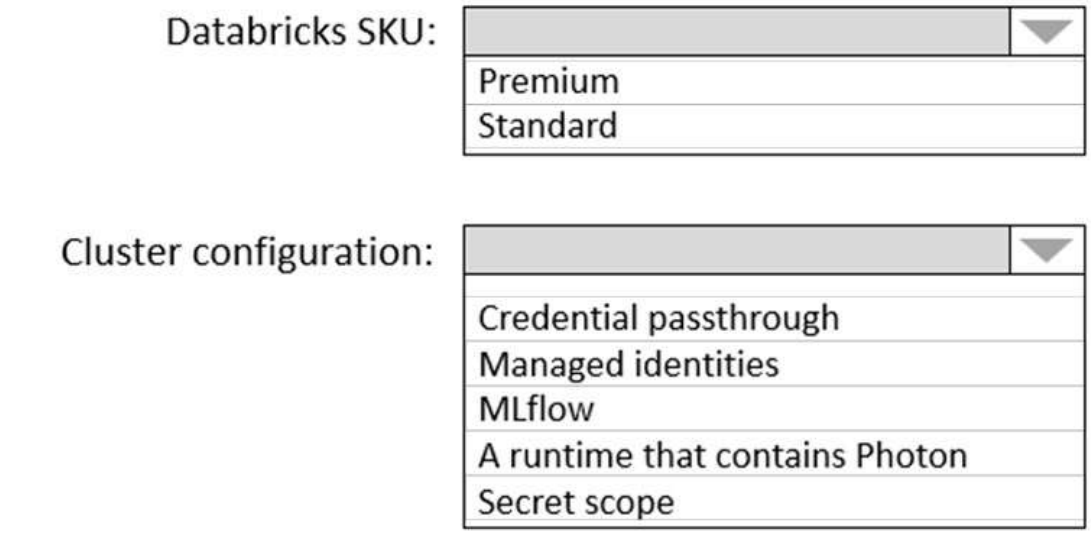
What should you include in the recommendation?

A. Implement Azure AD Identity Protection.
B. Change the Membership type of Group1 to **Dynamic User**.
C. Create an access review.
D. Implement Azure AD Privileged Identity Management (PIM).

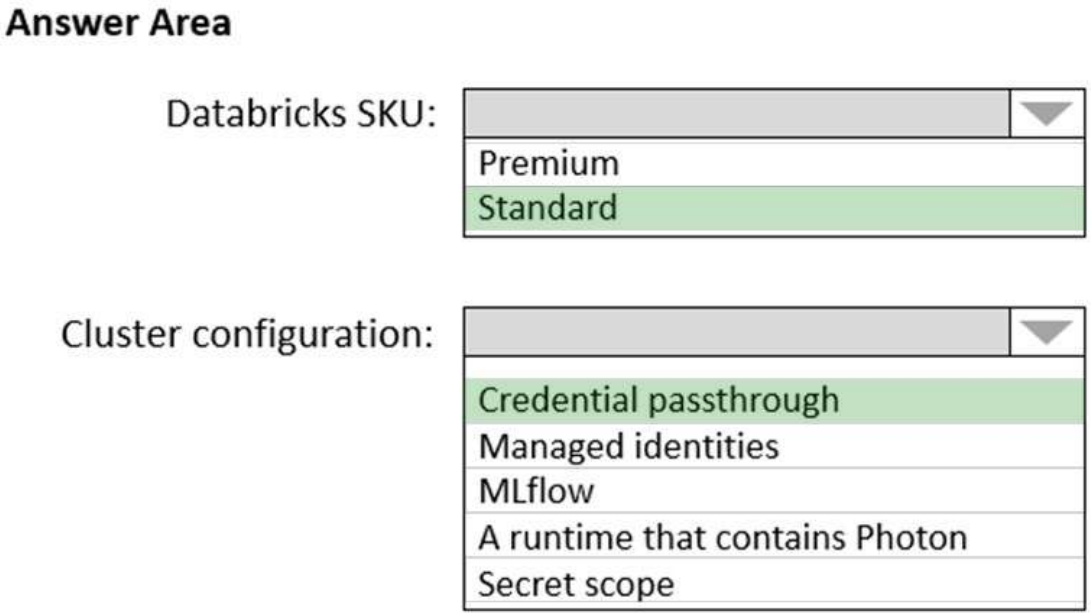
Answer: C
Explanation:
Have reviews recur periodically: You can set up recurring access reviews of users at set frequencies such as weekly, monthly, quarterly or annually, and the reviewers will be notified at the start of each review. Reviewers can approve or deny access with a friendly interface and with the help of smart recommendations.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/governance/access-reviews-overview#learn-about-access-reviews

QUESTION 17
Hotspot Question
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 permissions.
- 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:



Explanation:
Box 1: Standard
Choose Standard to minimize costs.
Box 2: Credential passthrough
Athenticate automatically to Azure Data Lake Storage Gen1 (ADLS Gen1) and Azure Data Lake Storage Gen2 (ADLS Gen2) from Azure Databricks clusters using the same Azure Active Directory (Azure AD) identity that you use to log into Azure Databricks. When you enable Azure Data Lake Storage credential passthrough for your cluster, commands that you run on that cluster can read and write data in Azure Data Lake Storage without requiring you to configure service principal credentials for access to storage.
Reference:
https://docs.microsoft.com/en-us/azure/databricks/security/credential-passthrough/adls-passthrough

QUESTION 18

Hotspot Question
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

Answer:

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

Explanation:
Box 1: 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 azure active directory.
You register your application with Azure active directory tenant.
Box 2: 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.

Reference:
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 19
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your company deploys several virtual machines on-premises and to Azure. ExpressRoute is being deployed and configured for on-premises to Azure connectivity.
Several virtual machines exhibit network connectivity issues.
You need to analyze the network traffic to identify whether packets are being allowed or denied to the virtual machines.
Solution: Use Azure Traffic Analytics in Azure Network Watcher to analyze the network traffic.
Does this meet the goal?

A. Yes
B. No

Answer: B
Explanation:
Instead use Azure Network Watcher IP Flow Verify, which allows you to detect traffic filtering issues at a VM level.
Note: IP flow verify checks if a packet is allowed or denied to or from a virtual machine. The information consists of direction, protocol, local IP, remote IP, local port, and remote port. If the packet is denied by a security group, the name of the rule that denied the packet is returned. While any source or destination IP can be chosen, IP flow verify helps administrators quickly diagnose connectivity issues from or to the internet and from or to the on-premises environment.
Reference:
https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-ip-flow-verify-overview

QUESTION 20
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your company deploys several virtual machines on-premises and to Azure. ExpressRoute is deployed and configured for on-premises to Azure connectivity.
Several virtual machines exhibit network connectivity issues.
You need to analyze the network traffic to identify whether packets are being allowed or denied to the virtual machines.
Solution: Use Azure Advisor to analyze the network traffic.
Does this meet the goal?

A. Yes
B. No

Answer: B
Explanation:
Instead use Azure Network Watcher IP Flow Verify, which allows you to detect traffic filtering issues at a VM level.
Note: IP flow verify checks if a packet is allowed or denied to or from a virtual machine. The information consists of direction, protocol, local IP, remote IP, local port, and remote port. If the packet is denied by a security group, the name of the rule that denied the packet is returned. While any source or destination IP can be chosen, IP flow verify helps administrators quickly diagnose connectivity issues from or to the internet and from or to the on-premises environment.
Reference:
https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-ip-flow-verify-overview

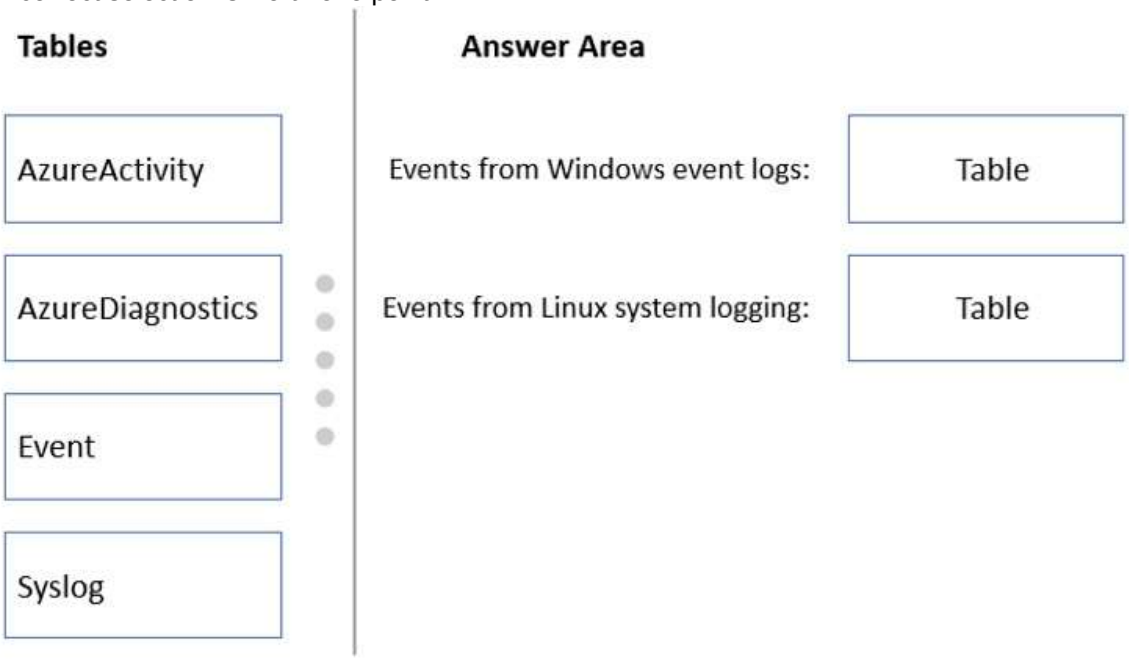
QUESTION 21
Note: This question is part of a series of questions that present the same scenario. Each question in the series

contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your company deploys several virtual machines on-premises and to Azure. ExpressRoute is deployed and configured for on-premises to Azure connectivity.
Several virtual machines exhibit network connectivity issues.
You need to analyze the network traffic to identify whether packets are being allowed or denied to the virtual machines.
Solution: Use Azure Network Watcher to run IP flow verify to analyze the network traffic.
Does this meet the goal?

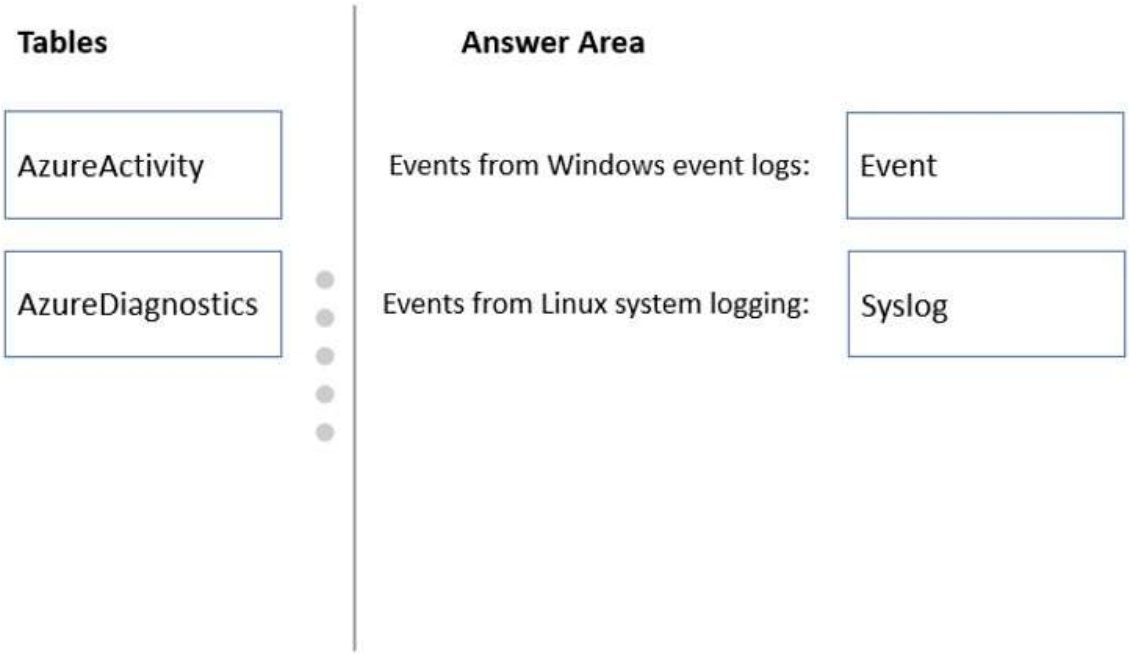
A. Yes
B. No

Answer: A
Explanation:
Azure Network Watcher IP Flow Verify allows you to detect traffic filtering issues at a VM level.
IP flow verify checks if a packet is allowed or denied to or from a virtual machine. The information consists of direction, protocol, local IP, remote IP, local port, and remote port. If the packet is denied by a security group, the name of the rule that denied the packet is returned. While any source or destination IP can be chosen, IP flow verify helps administrators quickly diagnose connectivity issues from or to the internet and from or to the on-premises environment.
Reference:
https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-ip-flow-verify-overview

QUESTION 22
Drag and Drop Question
You have an Azure subscription. The subscription contains Azure virtual machines that run Windows Server 2016 and Linux.
You need to use Azure Monitor to design an alerting strategy for security-related events.
Which Azure Monitor Logs tables should you query? To answer, drag the appropriate tables to the correct log types. Each table may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.
NOTE: Each correct selection is worth one point.



Answer:



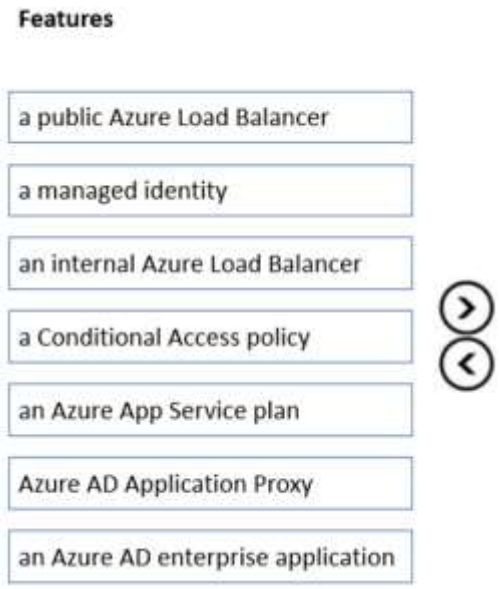
Explanation:
https://docs.microsoft.com/en-us/azure/azure-monitor/platform/data-sources-windows-events
https://docs.microsoft.com/en-us/azure/azure-monitor/agents/data-sources-syslog

QUESTION 23
You are designing a large Azure environment that will contain many subscriptions.
You plan to use Azure Policy as part of a governance solution.
To which three scopes can you assign Azure Policy definitions? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

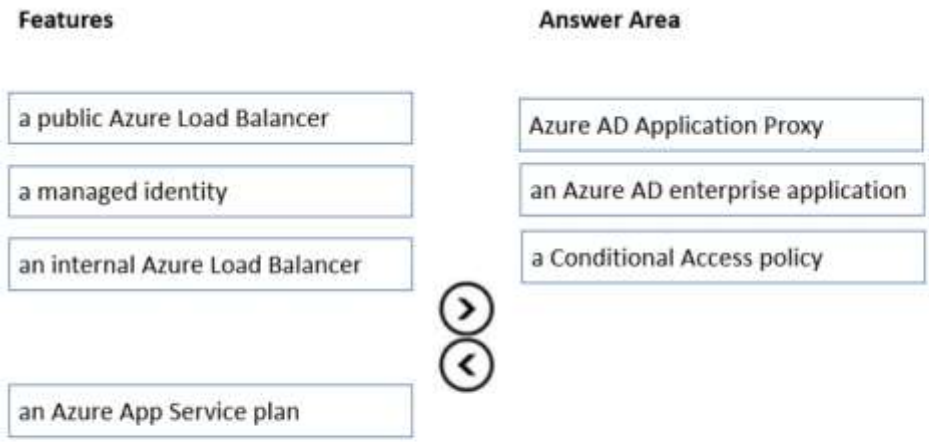
A. Azure Active Directory (Azure AD) administrative units
B. Azure Active Directory (Azure AD) tenants
C. subscriptions
D. compute resources
E. resource groups
F. management groups

Answer: ACF
Explanation:
Azure Policy evaluates resources in Azure by comparing the properties of those resources to business rules. Once your business rules have been formed, the policy definition or initiative is assigned to any scope of resources that Azure supports, such as management groups, subscriptions, resource groups, or individual resources.
Reference:
https://docs.microsoft.com/en-us/azure/governance/policy/overview

QUESTION 24
Drag and Drop Question
Your on-premises network contains a server named Server1 that runs an ASP.NET application named App1.
You have a hybrid deployment of Azure Active Directory (Azure AD).
You need to recommend a solution to ensure that users sign in by using their Azure AD account and Azure Multi-Factor Authentication (MFA) when they connect to App1 from the internet.
Which three features should you recommend be deployed and configured in sequence? To answer, move the appropriate features from the list of features to the answer area and arrange them in the correct order.



Answer:



QUESTION 25
You need to recommend a solution to generate a monthly report of all the new Azure Resource Manager (ARM) resource deployments in your Azure subscription.
What should you include in the recommendation?

A. Azure Activity Log
B. Azure Advisor
C. Azure Analysis Services
D. Azure Monitor action groups

Answer: A
Explanation:
Activity logs are kept for 90 days. You can query for any range of dates, as long as the starting date isn't more than 90 days in the past.
Through activity logs, you can determine:
▪ what operations were taken on the resources in your subscription

- who started the operation
- when the operation occurred
- the status of the operation
- the values of other properties that might help you research the operation

Reference:
https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/view-activity-logs

QUESTION 26
You have 100 servers that run Windows Server 2012 R2 and host Microsoft SQL Server 2014 instances. The instances host databases that have the following characteristics:
- Stored procedures are implemented by using CLR.
- The largest database is currently 3 TB. None of the databases will ever exceed 4 TB.

You plan to move all the data from SQL Server to Azure.
You need to recommend a service to host the databases. The solution must meet the following requirements:
- Whenever possible, minimize management overhead for the migrated databases.
- Ensure that users can authenticate by using Azure Active Directory (Azure AD) credentials.
- Minimize the number of database changes required to facilitate the migration.

What should you include in the recommendation?

A. Azure SQL Database elastic pools
B. Azure SQL Managed Instance
C. Azure SQL Database single databases
D. SQL Server 2016 on Azure virtual machines

Answer: B
Explanation:
SQL Managed Instance allows existing SQL Server customers to lift and shift their on-premises applications to the cloud with minimal application and database changes. At the same time, SQL Managed Instance preserves all PaaS capabilities (automatic patching and version updates, automated backups, high availability) that drastically reduce management overhead and TCO.
Reference:
https://docs.microsoft.com/en-us/azure/sql-database/sql-database-managed-instance

QUESTION 27
You have an Azure subscription that contains an Azure Blob Storage account named store1.
You have an on-premises file server named Server1 that runs Windows Server 2016. Server1 stores 500 GB of company files.
You need to store a copy of the company files from Server1 in store1.
Which two possible Azure services achieve this goal? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

A. an Azure Logic Apps integration account
B. an Azure Import/Export job
C. Azure Data Factory
D. an Azure Analysis services On-premises data gateway
E. an Azure Batch account

Answer: BC
Explanation:
https://docs.microsoft.com/en-us/azure/data-factory/introduction

QUESTION 28
You have an Azure subscription that contains two applications named App1 and App2. App1 is a sales processing application. When a transaction in App1 requires shipping, a message is added to an Azure Storage account queue, and then App2 listens to the queue for relevant transactions.
In the future, additional applications will be added that will process some of the shipping requests based on the specific

details of the transactions.
You need to recommend a replacement for the storage account queue to ensure that each additional application will be able to read the relevant transactions.
What should you recommend?

A. one Azure Data Factory pipeline
B. multiple storage account queues
C. one Azure Service Bus queue
D. one Azure Service Bus topic

Answer: D
Explanation:
A queue allows processing of a message by a single consumer. In contrast to queues, topics and subscriptions provide a one-to-many form of communication in a publish and subscribe pattern. It's useful for scaling to large numbers of recipients. Each published message is made available to each subscription registered with the topic. Publisher sends a message to a topic and one or more subscribers receive a copy of the message, depending on filter rules set on these subscriptions.
Reference:
https://docs.microsoft.com/en-us/azure/service-bus-messaging/service-bus-queues-topics-subscriptions

QUESTION 29
Hotspot Question
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

Answer:

Answer Area

Storage account type:

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

Storage service:

- **Blob**
- File
- Table

Explanation:
Box 1: BlockBlobStorage
Block Blob is a premium storage account type for block blobs and append blobs. Recommended for scenarios with high transactions rates, or scenarios that use smaller objects or require consistently low storage latency.
Box 2: 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.
Reference:
https://docs.microsoft.com/en-us/azure/storage/blobs/archive-blob

QUESTION 30
Hotspot Question
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

Answer:

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

Explanation:
Box 1: Storage1 and storage3 only
Azure Blob Storage lifecycle management offers a rich, rule-based policy for GPv2 and blob storage accounts. Storage 2 does not support access tiers.
Box 2: Storage1 and storage4 only

FileStorage storage accounts allow you to deploy Azure file shares on premium/solid-state disk-based (SSD-based) hardware.
Reference:
https://docs.microsoft.com/en-us/azure/storage/blobs/storage-lifecycle-management-concepts
https://docs.microsoft.com/ja-jp/azure/storage/common/storage-account-overview

QUESTION 31
You are designing an application that will be hosted in Azure.
The application will host video files that range from 50 MB to 12 GB. The application will use certificate-based authentication and will be available to users on the internet.
You need to recommend a storage option for the video files. The solution must provide the fastest read performance and must minimize storage costs.
What should you recommend?

A. Azure Files
B. Azure Data Lake Storage Gen2
C. Azure Blob Storage
D. Azure SQL Database

Answer: C
Explanation:
Blob Storage: Stores large amounts of unstructured data, such as text or binary data, that can be accessed from anywhere in the world via HTTP or HTTPS. You can use Blob storage to expose data publicly to the world, or to store application data privately.
Max file in Blob Storage. 4.77 TB.
Reference:
https://docs.microsoft.com/en-us/azure/architecture/solution-ideas/articles/digital-media-video