- **Vendor:** Microsoft
- **Exam Code:** AZ-305
- **Exam Name:** Designing Microsoft Azure Infrastructure Solutions
- **New Updated Questions from Braindump2go**
- **(Updated in December/2021)**

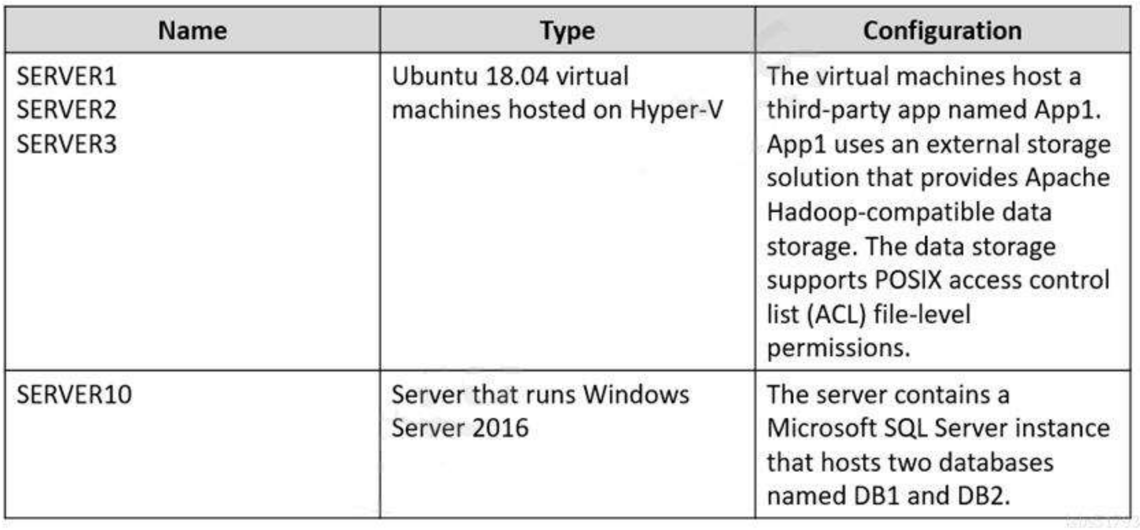
**QUESTION 1**
**Case Study 1 - Litware**
**Existing Environment**
**Azure Environment**

Litware has 10 Azure subscriptions that are linked to the Litware.com tenant and five Azure subscriptions that are linked to the dev.litware.com tenant. All the subscriptions are in an Enterprise Agreement (EA).

The litware.com tenant contains a custom Azure role-based access control (Azure RBAC) role named Role1 that grants the DataActions read permission to the blobs and files in Azure Storage.

**On-Premises Environment**

The on-premises network of Litware contains the resources shown in the following table.



| Name | Type | Configuration |
|---|---|---|
| SERVER1<br>SERVER2<br>SERVER3 | Ubuntu 18.04 virtual machines hosted on Hyper-V | The virtual machines host a third-party app named App1. App1 uses an external storage solution that provides Apache Hadoop-compatible data storage. The data storage supports POSIX access control list (ACL) file-level permissions. |
| SERVER10 | Server that runs Windows Server 2016 | The server contains a Microsoft SQL Server instance that hosts two databases named DB1 and DB2. |

**Network Environment**

Litware has ExpressRoute connectivity to Azure.

**Planned Changes and Requirements**

Litware plans to implement the following changes:

- Migrate DB1 and DB2 to Azure.
- Migrate App1 to Azure virtual machines.
- Migrate the external storage used by App1 to Azure Storage.
- Deploy the Azure virtual machines that will host App1 to Azure dedicated hosts.

**Authentication and Authorization Requirements**

Litware identifies the following authentication and authorization requirements:

- Only users that manage the production environment by using the Azure portal must connect from a hybrid Azure AD-joined device and authenticate by using Azure Multi-Factor Authentication (MFA).

- The Network Contributor built-in RBAC role must be used to grant permissions to the network administrators for all the virtual networks in all the Azure subscriptions.
- To access the resources in Azure, App1 must use the managed identity of the virtual machines that will host the app.
- RBAC roles must be applied at the highest level possible.

**Resiliency Requirements**

Litware identifies the following resiliency requirements:

- Once migrated to Azure, DB1 and DB2 must meet the following requirements:
  - Maintain availability if two availability zones in the local Azure region fail.
  - Fail over automatically.
  - Minimize I/O latency.
- App1 must meet the following requirements:
  - Be hosted in an Azure region that supports availability zones.
  - Be hosted on Azure virtual machines that support automatic scaling.
  - Maintain availability if two availability zones in the local Azure region fail.

**Security and Compliance Requirements**

Litware identifies the following security and compliance requirements:

- Once App1 is migrated to Azure, you must ensure that new data can be written to the app, and the modification of new and existing data is prevented for a period of three years.
- On-premises users and services must be able to access the Azure Storage account that will host the data in App1.
- Access to the public endpoint of the Azure Storage account that will host the App1 data must be prevented.
- All Azure SQL databases in the production environment must have Transparent Data Encryption (TDE) enabled.
- App1 must **NOT** share physical hardware with other workloads.

**Business Requirements**

Litware identifies the following business requirements:

- Minimize administrative effort.
- Minimize costs.

After you migrate App1 to Azure, you need to enforce the data modification requirements to meet the security and compliance requirements.
What should you do?

A. Create an access policy for the blob service.
B. Implement Azure resource locks.
C. Create Azure RBAC assignments.
D. Modify the access level of the blob service.

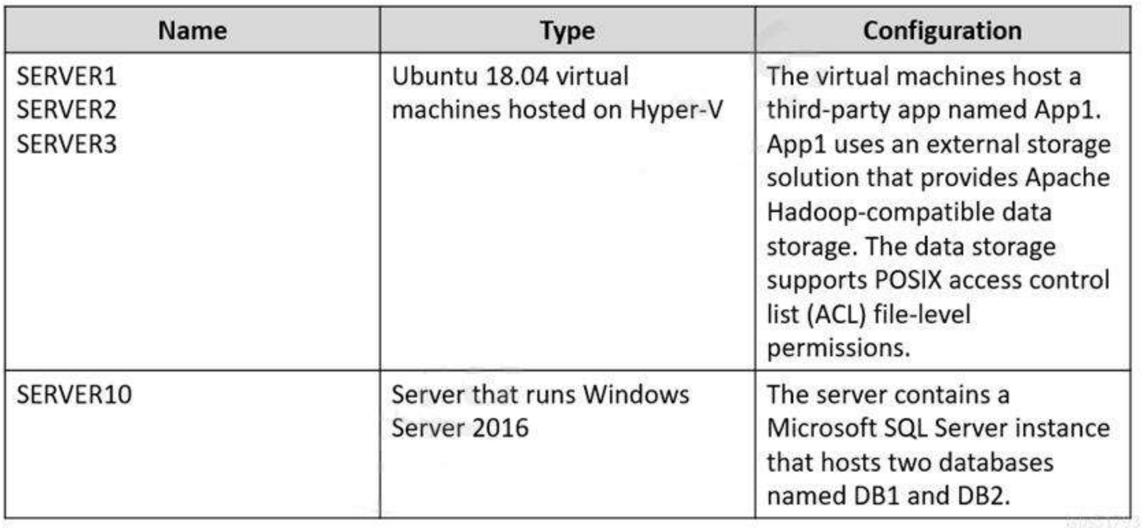
**Answer:** B
**Explanation:**
Scenario: Once App1 is migrated to Azure, you must ensure that new data can be written to the app, and the modification of new and existing data is prevented for a period of three years.
As an administrator, you can lock a subscription, resource group, or resource to prevent other users in your organization from accidentally deleting or modifying critical resources. The lock overrides any permissions the user might have.
Reference:
https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/lock-resources

**QUESTION 2**
**Case Study 1 - Litware**
**Existing Environment**
**Azure Environment**

Litware has 10 Azure subscriptions that are linked to the Litware.com tenant and five Azure subscriptions that are linked to the dev.litware.com tenant. All the subscriptions are in an Enterprise Agreement (EA).
The litware.com tenant contains a custom Azure role-based access control (Azure RBAC) role named Role1 that grants the DataActions read permission to the blobs and files in Azure Storage.

**On-Premises Environment**

The on-premises network of Litware contains the resources shown in the following table.



| Name | Type | Configuration |
|---|---|---|
| SERVER1<br>SERVER2<br>SERVER3 | Ubuntu 18.04 virtual machines hosted on Hyper-V | The virtual machines host a third-party app named App1. App1 uses an external storage solution that provides Apache Hadoop-compatible data storage. The data storage supports POSIX access control list (ACL) file-level permissions. |
| SERVER10 | Server that runs Windows Server 2016 | The server contains a Microsoft SQL Server instance that hosts two databases named DB1 and DB2. |

**Network Environment**

Litware has ExpressRoute connectivity to Azure.

**Planned Changes and Requirements**

Litware plans to implement the following changes:

- Migrate DB1 and DB2 to Azure.
- Migrate App1 to Azure virtual machines.
- Migrate the external storage used by App1 to Azure Storage.
- Deploy the Azure virtual machines that will host App1 to Azure dedicated hosts.

**Authentication and Authorization Requirements**

Litware identifies the following authentication and authorization requirements:

- Only users that manage the production environment by using the Azure portal must connect from a hybrid Azure AD-joined device and authenticate by using Azure Multi-Factor Authentication (MFA).
- The Network Contributor built-in RBAC role must be used to grant permissions to the network administrators for all the virtual networks in all the Azure subscriptions.
- To access the resources in Azure, App1 must use the managed identity of the virtual machines that will host the app.
- RBAC roles must be applied at the highest level possible.

**Resiliency Requirements**

Litware identifies the following resiliency requirements:

- Once migrated to Azure, DB1 and DB2 must meet the following requirements:
  - Maintain availability if two availability zones in the local Azure region fail.
  - Fail over automatically.
  - Minimize I/O latency.
- App1 must meet the following requirements:
  - Be hosted in an Azure region that supports availability zones.
  - Be hosted on Azure virtual machines that support automatic scaling.
  - Maintain availability if two availability zones in the local Azure region fail.

**Security and Compliance Requirements**

Litware identifies the following security and compliance requirements:

- Once App1 is migrated to Azure, you must ensure that new data can be written to the app, and the modification of new and existing data is prevented for a period of three years.
- On-premises users and services must be able to access the Azure Storage account that will host the data in App1.
- Access to the public endpoint of the Azure Storage account that will host the App1 data must be prevented.
- All Azure SQL databases in the production environment must have Transparent Data Encryption (TDE) enabled.
- App1 must **NOT** share physical hardware with other workloads.

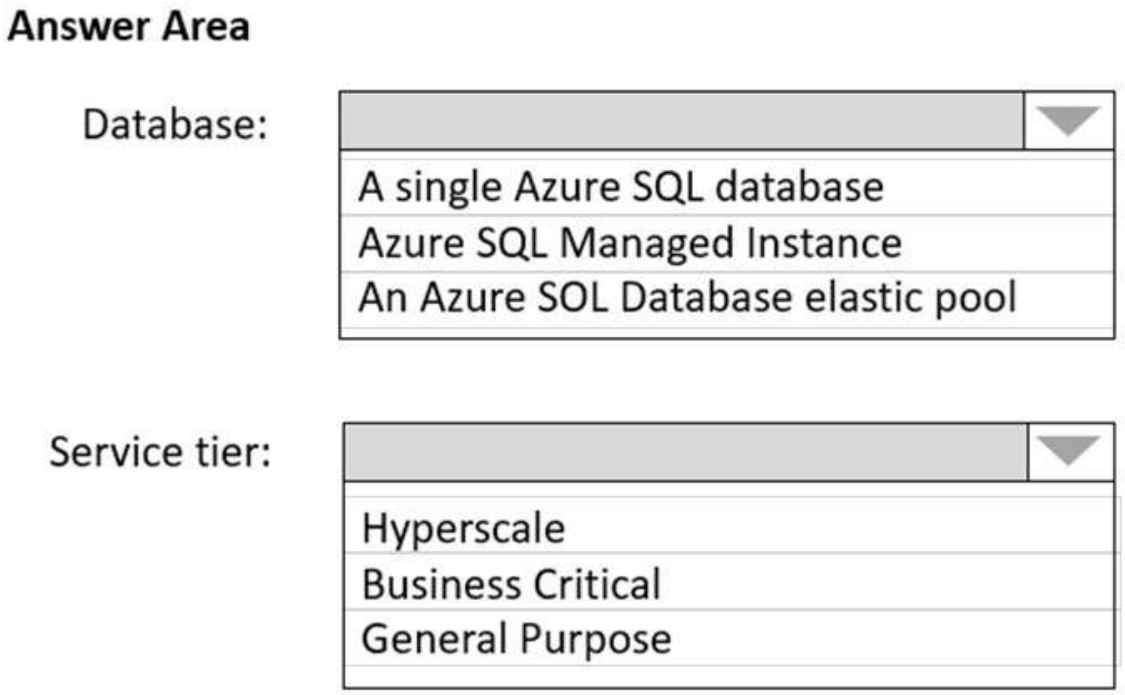
**Business Requirements**

Litware identifies the following business requirements:

- Minimize administrative effort.
- Minimize costs.

Hotspot Question

How should the migrated databases DB1 and DB2 be implemented in Azure?



Answer Area

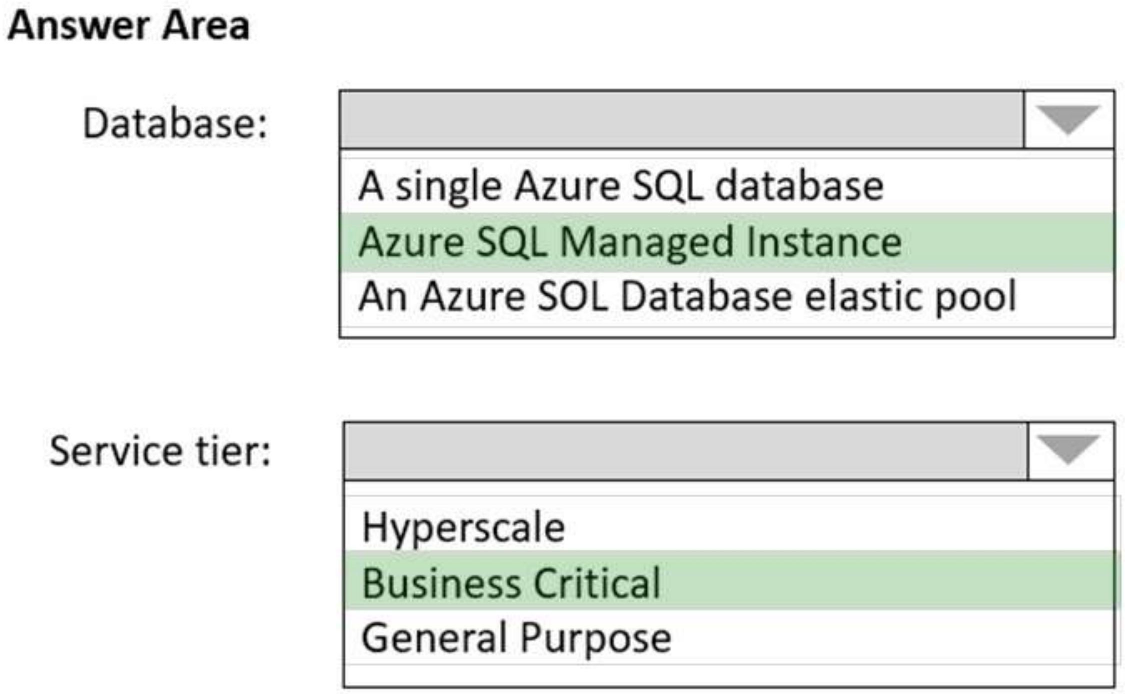
Database:

- A single Azure SQL database
- Azure SQL Managed Instance
- An Azure SOL Database elastic pool

Service tier:

- Hyperscale
- Business Critical
- General Purpose

**Answer:**



Answer Area

Database:

- A single Azure SQL database
- [✓ Azure SQL Managed Instance]
- An Azure SOL Database elastic pool

Service tier:

- Hyperscale
- [✓ Business Critical]
- General Purpose

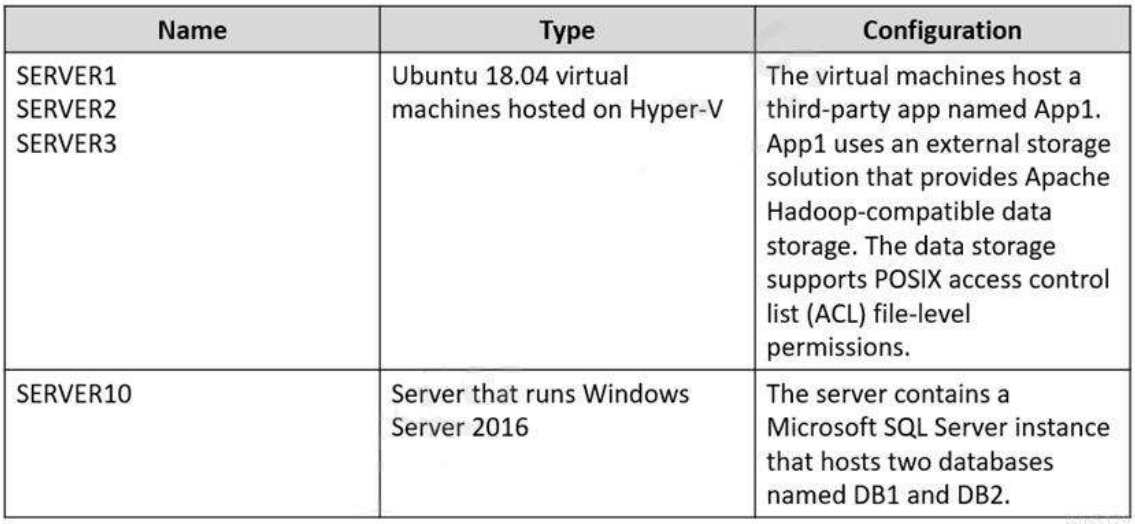
**Explanation:**
Box 1: SQL Managed Instance
Scenario: Once migrated to Azure, DB1 and DB2 must meet the following requirements:

- Maintain availability if two availability zones in the local Azure region fail.
- Fail over automatically.
- Minimize I/O latency.

The auto-failover groups feature allows you to manage the replication and failover of a group of databases on a server or all databases in a managed instance to another region. It is a declarative abstraction on top of the existing active geo-replication feature, designed to simplify deployment and management of geo-replicated databases at scale. You

can initiate a geo-failover manually or you can delegate it to the Azure service based on a user-defined policy. The latter option allows you to automatically recover multiple related databases in a secondary region after a catastrophic failure or other unplanned event that results in full or partial loss of the SQL Database or SQL Managed Instance availability in the primary region.
Box 2: Business critical
SQL Managed Instance is available in two service tiers:
General purpose: Designed for applications with typical performance and I/O latency requirements.
Business critical: Designed for applications with low I/O latency requirements and minimal impact of underlying maintenance operations on the workload.
Reference:
https://docs.microsoft.com/en-us/azure/azure-sql/database/auto-failover-group-overview
https://docs.microsoft.com/en-us/azure/azure-sql/managed-instance/sql-managed-instance-paas-overview

**QUESTION 3**
**Case Study 1 - Litware**
**Existing Environment**
**Azure Environment**
Litware has 10 Azure subscriptions that are linked to the Litware.com tenant and five Azure subscriptions that are linked to the dev.litware.com tenant. All the subscriptions are in an Enterprise Agreement (EA).
The litware.com tenant contains a custom Azure role-based access control (Azure RBAC) role named Role1 that grants the DataActions read permission to the blobs and files in Azure Storage.
**On-Premises Environment**
The on-premises network of Litware contains the resources shown in the following table.



| Name | Type | Configuration |
|---|---|---|
| SERVER1<br>SERVER2<br>SERVER3 | Ubuntu 18.04 virtual machines hosted on Hyper-V | The virtual machines host a third-party app named App1. App1 uses an external storage solution that provides Apache Hadoop-compatible data storage. The data storage supports POSIX access control list (ACL) file-level permissions. |
| SERVER10 | Server that runs Windows Server 2016 | The server contains a Microsoft SQL Server instance that hosts two databases named DB1 and DB2. |

**Network Environment**
Litware has ExpressRoute connectivity to Azure.
**Planned Changes and Requirements**
Litware plans to implement the following changes:

- Migrate DB1 and DB2 to Azure.
- Migrate App1 to Azure virtual machines.
- Migrate the external storage used by App1 to Azure Storage.
- Deploy the Azure virtual machines that will host App1 to Azure dedicated hosts.

**Authentication and Authorization Requirements**
Litware identifies the following authentication and authorization requirements:

- Only users that manage the production environment by using the Azure portal must connect from a hybrid Azure AD-joined device and authenticate by using Azure Multi-Factor Authentication (MFA).
- The Network Contributor built-in RBAC role must be used to grant permissions to the network administrators for all the virtual networks in all the Azure subscriptions.
- To access the resources in Azure, App1 must use the managed identity of the virtual machines that will host the app.
- RBAC roles must be applied at the highest level possible.

**Resiliency Requirements**

Litware identifies the following resiliency requirements:

- Once migrated to Azure, DB1 and DB2 must meet the following requirements:
  - Maintain availability if two availability zones in the local Azure region fail.
  - Fail over automatically.
  - Minimize I/O latency.
- App1 must meet the following requirements:
  - Be hosted in an Azure region that supports availability zones.
  - Be hosted on Azure virtual machines that support automatic scaling.
  - Maintain availability if two availability zones in the local Azure region fail.

**Security and Compliance Requirements**

Litware identifies the following security and compliance requirements:

- Once App1 is migrated to Azure, you must ensure that new data can be written to the app, and the modification of new and existing data is prevented for a period of three years.
- On-premises users and services must be able to access the Azure Storage account that will host the data in App1.
- Access to the public endpoint of the Azure Storage account that will host the App1 data must be prevented.
- All Azure SQL databases in the production environment must have Transparent Data Encryption (TDE) enabled.
- App1 must **NOT** share physical hardware with other workloads.

**Business Requirements**

Litware identifies the following business requirements:

- Minimize administrative effort.
- Minimize costs.

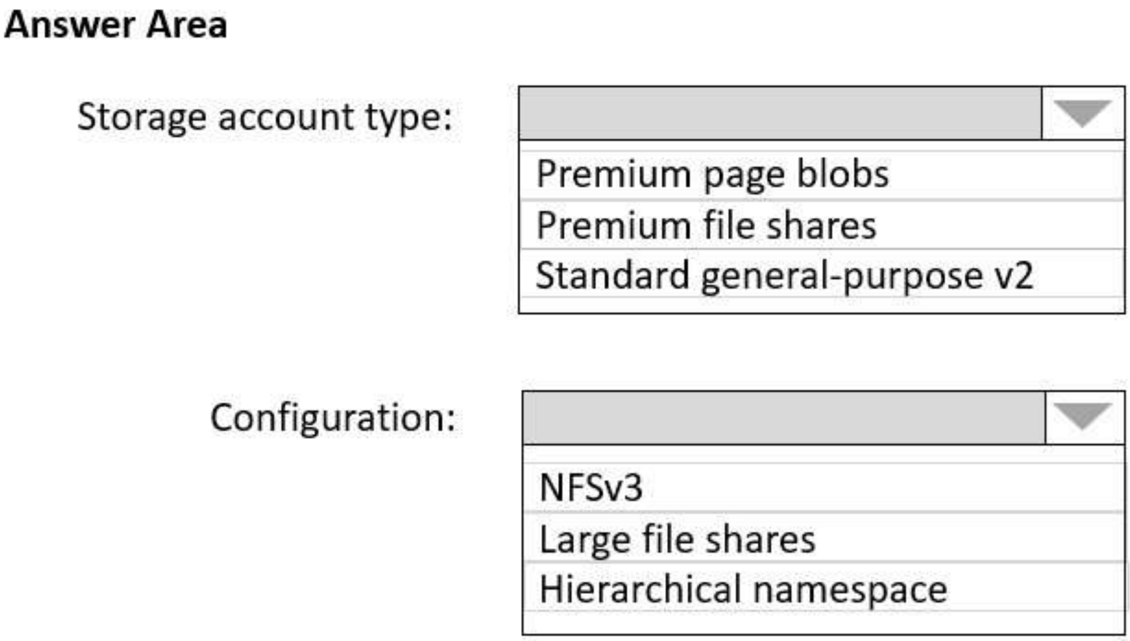
Hotspot Question

You plan to migrate App1 to Azure.

You need to recommend a storage solution for App1 that meets the security and compliance requirements.

Which type of storage should you recommend, and how should you recommend configuring the storage? To answer, select the appropriate options in the answer area.

**NOTE:** Each correct selection is worth one point.

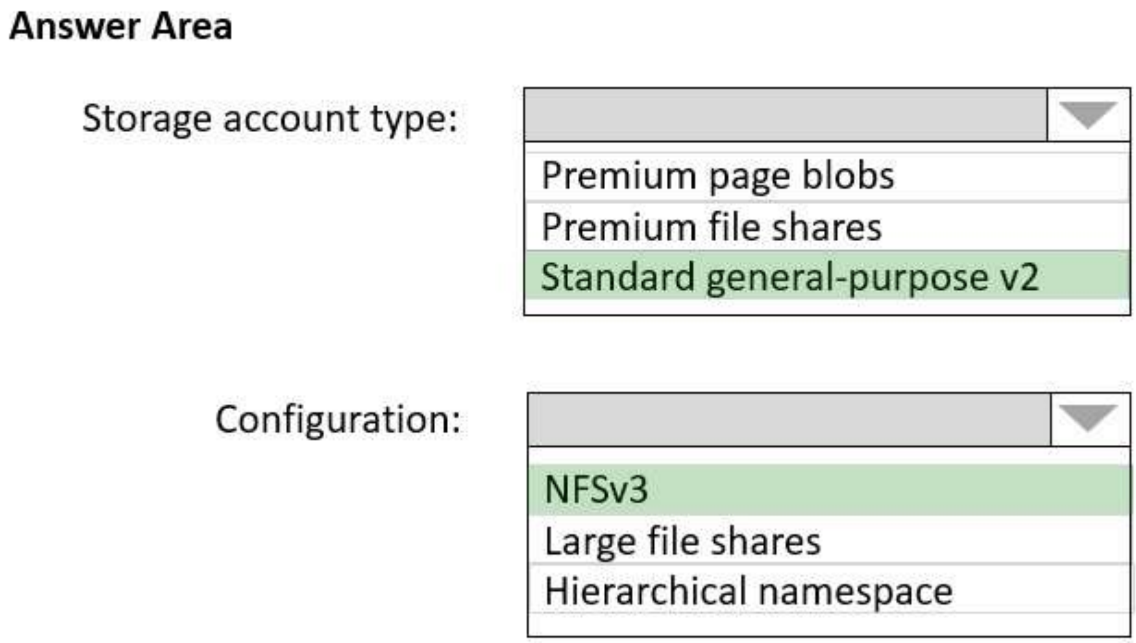


Answer Area

Storage account type:
- Premium page blobs
- Premium file shares
- Standard general-purpose v2

Configuration:
- NFSv3
- Large file shares
- Hierarchical namespace

**Answer:**



Answer Area

Storage account type:

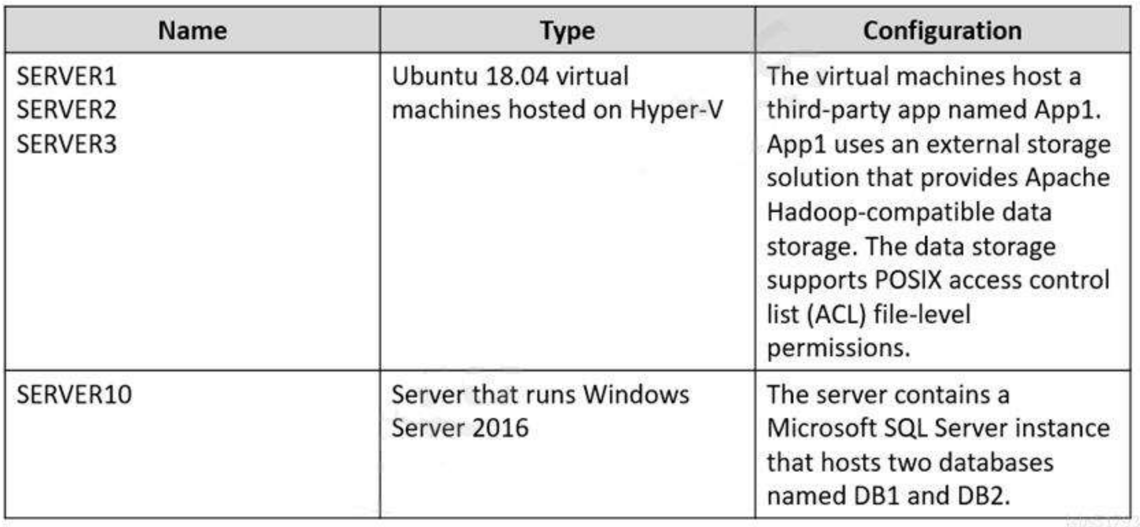
- Premium page blobs
- Premium file shares
- [✓ Standard general-purpose v2]

Configuration:

- [✓ NFSv3]
- Large file shares
- Hierarchical namespace

**Explanation:**
Box 1: Standard general-purpose v2
Standard general-purpose v2 supports Blob Storage.
Azure Storage provides data protection for Blob Storage and Azure Data Lake Storage Gen2.
Scenario:
Litware identifies the following security and compliance requirements:
Once App1 is migrated to Azure, you must ensure that new data can be written to the app, and the modification of new and existing data is prevented for a period of three years.
On-premises users and services must be able to access the Azure Storage account that will host the data in App1.
Access to the public endpoint of the Azure Storage account that will host the App1 data must be prevented.
All Azure SQL databases in the production environment must have Transparent Data Encryption (TDE) enabled.
App1 must NOT share physical hardware with other workloads.
Box 2: NFSv3
Scenario: Plan: Migrate App1 to Azure virtual machines.
Blob storage now supports the Network File System (NFS) 3.0 protocol. This support provides Linux file system compatibility at object storage scale and prices and enables Linux clients to mount a container in Blob storage from an Azure Virtual Machine (VM) or a computer on-premises.
Reference:
https://docs.microsoft.com/en-us/azure/storage/blobs/data-protection-overview

**QUESTION 4**
**Case Study 1 - Litware**
**Existing Environment**
**Azure Environment**
Litware has 10 Azure subscriptions that are linked to the Litware.com tenant and five Azure subscriptions that are linked to the dev.litware.com tenant. All the subscriptions are in an Enterprise Agreement (EA).
The litware.com tenant contains a custom Azure role-based access control (Azure RBAC) role named Role1 that grants the DataActions read permission to the blobs and files in Azure Storage.
**On-Premises Environment**
The on-premises network of Litware contains the resources shown in the following table.



| Name | Type | Configuration |
|---|---|---|
| SERVER1<br>SERVER2<br>SERVER3 | Ubuntu 18.04 virtual machines hosted on Hyper-V | The virtual machines host a third-party app named App1. App1 uses an external storage solution that provides Apache Hadoop-compatible data storage. The data storage supports POSIX access control list (ACL) file-level permissions. |
| SERVER10 | Server that runs Windows Server 2016 | The server contains a Microsoft SQL Server instance that hosts two databases named DB1 and DB2. |

**Network Environment**

Litware has ExpressRoute connectivity to Azure.

**Planned Changes and Requirements**

Litware plans to implement the following changes:

- Migrate DB1 and DB2 to Azure.
- Migrate App1 to Azure virtual machines.
- Migrate the external storage used by App1 to Azure Storage.
- Deploy the Azure virtual machines that will host App1 to Azure dedicated hosts.

**Authentication and Authorization Requirements**

Litware identifies the following authentication and authorization requirements:

- Only users that manage the production environment by using the Azure portal must connect from a hybrid Azure AD-joined device and authenticate by using Azure Multi-Factor Authentication (MFA).
- The Network Contributor built-in RBAC role must be used to grant permissions to the network administrators for all the virtual networks in all the Azure subscriptions.
- To access the resources in Azure, App1 must use the managed identity of the virtual machines that will host the app.
- RBAC roles must be applied at the highest level possible.

**Resiliency Requirements**

Litware identifies the following resiliency requirements:

- Once migrated to Azure, DB1 and DB2 must meet the following requirements:
  - Maintain availability if two availability zones in the local Azure region fail.
  - Fail over automatically.
  - Minimize I/O latency.
- App1 must meet the following requirements:
  - Be hosted in an Azure region that supports availability zones.
  - Be hosted on Azure virtual machines that support automatic scaling.
  - Maintain availability if two availability zones in the local Azure region fail.

**Security and Compliance Requirements**

Litware identifies the following security and compliance requirements:

- Once App1 is migrated to Azure, you must ensure that new data can be written to the app, and the modification of new and existing data is prevented for a period of three years.
- On-premises users and services must be able to access the Azure Storage account that will host the data in App1.
- Access to the public endpoint of the Azure Storage account that will host the App1 data must be prevented.
- All Azure SQL databases in the production environment must have Transparent Data Encryption (TDE) enabled.
- App1 must **NOT** share physical hardware with other workloads.

**Business Requirements**

Litware identifies the following business requirements:

- Minimize administrative effort.
- Minimize costs.

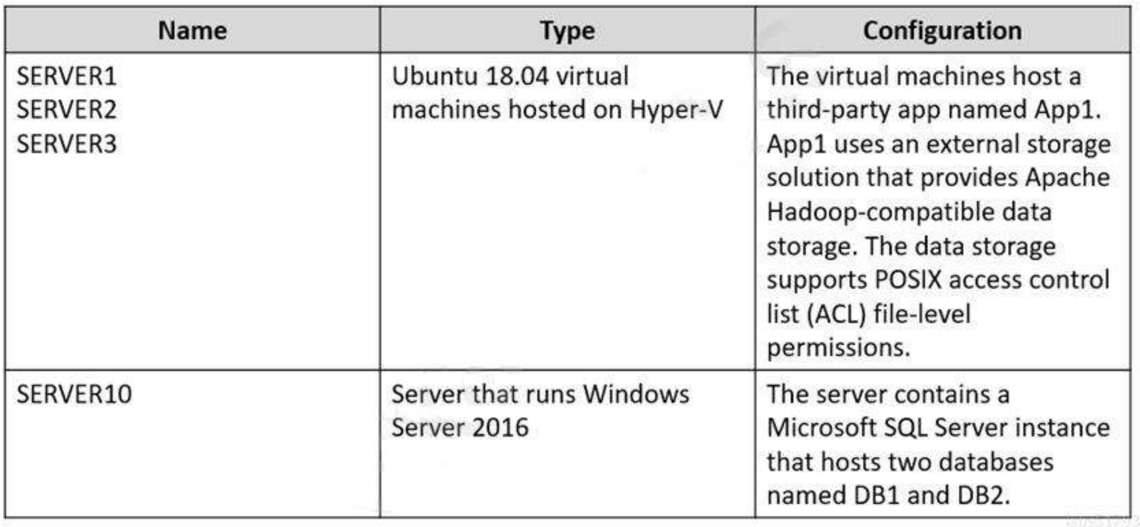
You plan to migrate App1 to Azure.

You need to recommend a network connectivity solution for the Azure Storage account that will host the App1 data.
The solution must meet the security and compliance requirements.
What should you include in the recommendation?

A. Microsoft peering for an ExpressRoute circuit
B. Azure public peering for an ExpressRoute circuit
C. a service endpoint that has a service endpoint policy
D. a private endpoint
E.

**Answer:** D
**Explanation:**
Private Endpoint securely connect to storage accounts from on-premises networks that connect to the VNet using VPN or ExpressRoutes with private-peering.
Private Endpoint also secure your storage account by configuring the storage firewall to block all connections on the public endpoint for the storage service.
Incorrect Answers:
A: Microsoft peering provides access to Azure public services via public endpoints with public IP addresses, which should not be allowed.
B: Azure public peering has been deprecated.
C: By default, Service Endpoints are enabled on subnets configured in Azure virtual networks. Endpoints can't be used for traffic from your premises to Azure services.
Reference:
https://docs.microsoft.com/en-us/azure/expressroute/expressroute-circuit-peerings

**QUESTION 5**
**Case Study 1 - Litware**
**Existing Environment**
**Azure Environment**
Litware has 10 Azure subscriptions that are linked to the Litware.com tenant and five Azure subscriptions that are linked to the dev.litware.com tenant. All the subscriptions are in an Enterprise Agreement (EA).
The litware.com tenant contains a custom Azure role-based access control (Azure RBAC) role named Role1 that grants the DataActions read permission to the blobs and files in Azure Storage.
**On-Premises Environment**
The on-premises network of Litware contains the resources shown in the following table.



| Name | Type | Configuration |
|---|---|---|
| SERVER1<br>SERVER2<br>SERVER3 | Ubuntu 18.04 virtual machines hosted on Hyper-V | The virtual machines host a third-party app named App1. App1 uses an external storage solution that provides Apache Hadoop-compatible data storage. The data storage supports POSIX access control list (ACL) file-level permissions. |
| SERVER10 | Server that runs Windows Server 2016 | The server contains a Microsoft SQL Server instance that hosts two databases named DB1 and DB2. |

**Network Environment**
Litware has ExpressRoute connectivity to Azure.
**Planned Changes and Requirements**
Litware plans to implement the following changes:
・Migrate DB1 and DB2 to Azure.

- Migrate App1 to Azure virtual machines.
- Migrate the external storage used by App1 to Azure Storage.
- Deploy the Azure virtual machines that will host App1 to Azure dedicated hosts.

**Authentication and Authorization Requirements**

Litware identifies the following authentication and authorization requirements:

- Only users that manage the production environment by using the Azure portal must connect from a hybrid Azure AD-joined device and authenticate by using Azure Multi-Factor Authentication (MFA).
- The Network Contributor built-in RBAC role must be used to grant permissions to the network administrators for all the virtual networks in all the Azure subscriptions.
- To access the resources in Azure, App1 must use the managed identity of the virtual machines that will host the app.
- RBAC roles must be applied at the highest level possible.

**Resiliency Requirements**

Litware identifies the following resiliency requirements:

- Once migrated to Azure, DB1 and DB2 must meet the following requirements:
  - Maintain availability if two availability zones in the local Azure region fail.
  - Fail over automatically.
  - Minimize I/O latency.
- App1 must meet the following requirements:
  - Be hosted in an Azure region that supports availability zones.
  - Be hosted on Azure virtual machines that support automatic scaling.
  - Maintain availability if two availability zones in the local Azure region fail.

**Security and Compliance Requirements**

Litware identifies the following security and compliance requirements:

- Once App1 is migrated to Azure, you must ensure that new data can be written to the app, and the modification of new and existing data is prevented for a period of three years.
- On-premises users and services must be able to access the Azure Storage account that will host the data in App1.
- Access to the public endpoint of the Azure Storage account that will host the App1 data must be prevented.
- All Azure SQL databases in the production environment must have Transparent Data Encryption (TDE) enabled.
- App1 must **NOT** share physical hardware with other workloads.

**Business Requirements**

Litware identifies the following business requirements:

- Minimize administrative effort.
- Minimize costs.

You need to implement the Azure RBAC role assignments for the Network Contributor role. The solution must meet the authentication and authorization requirements.
What is the minimum number of assignments that you must use?

A. 1
B. 2
C. 5
D. 10
E. 15

**Answer:** A
**Explanation:**
Scenario: The Network Contributor built-in RBAC role must be used to grant permissions to the network administrators for all the virtual networks in all the Azure subscriptions.
RBAC roles must be applied at the highest level possible.

**QUESTION 6**
**Case Study 2 - Fabrikam, Inc**
**Overview**

Fabrikam, Inc. is an engineering company that has offices throughout Europe. The company has a main office in London and three branch offices in Amsterdam, Berlin, and Rome.

**Existing Environment: Active Directory Environment**

The network contains two Active Directory forests named corp.fabrikam.com and rd.fabrikam.com. There are no trust relationships between the forests.

Corp.fabrikam.com is a production forest that contains identities used for internal user and computer authentication.

Rd.fabrikam.com is used by the research and development (R&D) department only. The R&D department is restricted to using on-premises resources only.

**Existing Environment: Network Infrastructure**

Each office contains at least one domain controller from the corp.fabrikam.com domain. The main office contains all the domain controllers for the rd.fabrikam.com forest.

All the offices have a high-speed connection to the internet.

An existing application named WebApp1 is hosted in the data center of the London office. WebApp1 is used by customers to place and track orders. WebApp1 has a web tier that uses Microsoft Internet information Services (IIS) and a database tier that runs Microsoft SQL Server 2016. The web tier and the database tier are deployed to virtual machines that run on Hyper-V.

The IT department currently uses a separate Hyper-V environment to test updates to WebApp1.

Fabrikam purchases all Microsoft licenses through a Microsoft Enterprise Agreement that includes Software Assurance.

**Existing Environment: Problem Statements**

The use of WebApp1 is unpredictable. At peak times, users often report delays. At other times, many resources for WebApp1 are underutilized.

**Requirements: Planned Changes**

Fabrikam plans to move most of its production workloads to Azure during the next few years, including virtual machines that rely on Active Directory for authentication.

As one of its first projects, the company plans to establish a hybrid identity model, facilitating an upcoming Microsoft 365 deployment.

All R&D operations will remain on-premises.

Fabrikam plans to migrate the production and test instances of WebApp1 to Azure.

**Requirements: Technical Requirements**

Fabrikam identifies the following technical requirements:

- Website content must be easily updated from a single point.
- User input must be minimized when provisioning new web app instances.
- Whenever possible, existing on-premises licenses must be used to reduce cost.
- Users must always authenticate by using their corp.fabrikam.com UPN identity.
- Any new deployments to Azure must be redundant in case an Azure region fails.
- Whenever possible, solutions must be deployed to Azure by using the Standard pricing tier of Azure App Service.
- An email distribution group named IT Support must be notified of any issues relating to the directory synchronization services.
- In the event that a link fails between Azure and the on-premises network, ensure that the virtual machines hosted in Azure can authenticate to Active Directory.
- Directory synchronization between Azure Active Directory (Azure AD) and corp.fabrikam.com must not be affected by a link failure between Azure and the on-premises network.

**Requirements: Database Requirements**

Fabrikam identifies the following database requirements:

- Database metrics for the production instance of WebApp1 must be available for analysis so that database administrators can optimize the performance settings.
- To avoid disrupting customer access, database downtime must be minimized when databases are migrated.
- Database backups must be retained for a minimum of seven years to meet compliance requirements.

**Requirements: Security Requirements**

Fabrikam identifies the following security requirements:

- Company information including policies, templates, and data must be inaccessible to anyone outside the company.
- Users on the on-premises network must be able to authenticate to corp.fabrikam.com if an internet link fails.
- Administrators must be able authenticate to the Azure portal by using their corp.fabrikam.com credentials.
- All administrative access to the Azure portal must be secured by using multi-factor authentication (MFA).
- The testing of WebApp1 updates must not be visible to anyone outside the company.

You need to recommend a solution to meet the database retention requirements.

What should you recommend?

A. Configure a long-term retention policy for the database.
B. Configure Azure Site Recovery.
C. Use automatic Azure SQL Database backups.
D. Configure geo-replication of the database.

**Answer:** A

**QUESTION 7**
**Case Study 2 - Fabrikam, Inc**
**Overview**

Fabrikam, Inc. is an engineering company that has offices throughout Europe. The company has a main office in London and three branch offices in Amsterdam, Berlin, and Rome.

**Existing Environment: Active Directory Environment**

The network contains two Active Directory forests named corp.fabrikam.com and rd.fabrikam.com. There are no trust relationships between the forests.

Corp.fabrikam.com is a production forest that contains identities used for internal user and computer authentication.

Rd.fabrikam.com is used by the research and development (R&D) department only. The R&D department is restricted to using on-premises resources only.

**Existing Environment: Network Infrastructure**

Each office contains at least one domain controller from the corp.fabrikam.com domain. The main office contains all the domain controllers for the rd.fabrikam.com forest.

All the offices have a high-speed connection to the internet.

An existing application named WebApp1 is hosted in the data center of the London office. WebApp1 is used by customers to place and track orders. WebApp1 has a web tier that uses Microsoft Internet information Services (IIS) and a database tier that runs Microsoft SQL Server 2016. The web tier and the database tier are deployed to virtual machines that run on Hyper-V.

The IT department currently uses a separate Hyper-V environment to test updates to WebApp1.

Fabrikam purchases all Microsoft licenses through a Microsoft Enterprise Agreement that includes Software Assurance.

**Existing Environment: Problem Statements**

The use of WebApp1 is unpredictable. At peak times, users often report delays. At other times, many resources for WebApp1 are underutilized.

**Requirements: Planned Changes**

Fabrikam plans to move most of its production workloads to Azure during the next few years, including virtual machines that rely on Active Directory for authentication.

As one of its first projects, the company plans to establish a hybrid identity model, facilitating an upcoming Microsoft 365 deployment.

All R&D operations will remain on-premises.

Fabrikam plans to migrate the production and test instances of WebApp1 to Azure.

**Requirements: Technical Requirements**

Fabrikam identifies the following technical requirements:

- Website content must be easily updated from a single point.
- User input must be minimized when provisioning new web app instances.
- Whenever possible, existing on-premises licenses must be used to reduce cost.
- Users must always authenticate by using their corp.fabrikam.com UPN identity.
- Any new deployments to Azure must be redundant in case an Azure region fails.
- Whenever possible, solutions must be deployed to Azure by using the Standard pricing tier of Azure App Service.
- An email distribution group named IT Support must be notified of any issues relating to the directory synchronization services.
- In the event that a link fails between Azure and the on-premises network, ensure that the virtual machines hosted in Azure can authenticate to Active Directory.
- Directory synchronization between Azure Active Directory (Azure AD) and corp.fabrikam.com must not be affected by a link failure between Azure and the on-premises network.

**Requirements: Database Requirements**

Fabrikam identifies the following database requirements:

- Database metrics for the production instance of WebApp1 must be available for analysis so that database administrators can optimize the performance settings.

- To avoid disrupting customer access, database downtime must be minimized when databases are migrated.
- Database backups must be retained for a minimum of seven years to meet compliance requirements.

**Requirements: Security Requirements**

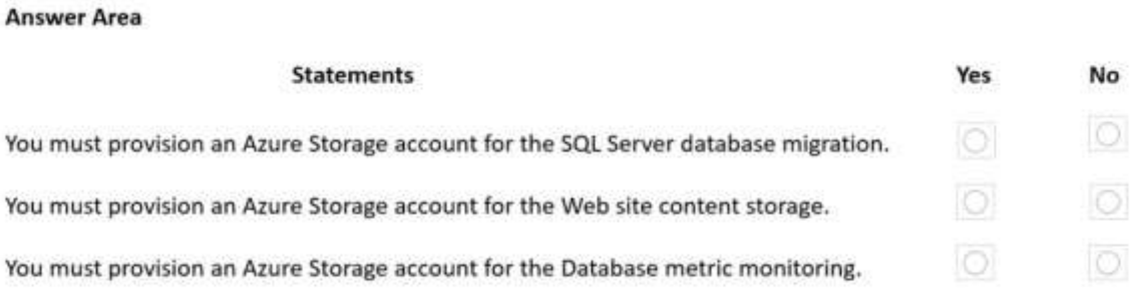
Fabrikam identifies the following security requirements:

- Company information including policies, templates, and data must be inaccessible to anyone outside the company.
- Users on the on-premises network must be able to authenticate to corp.fabrikam.com if an internet link fails.
- Administrators must be able authenticate to the Azure portal by using their corp.fabrikam.com credentials.
- All administrative access to the Azure portal must be secured by using multi-factor authentication (MFA).
- The testing of WebApp1 updates must not be visible to anyone outside the company.

Hotspot Question

You are evaluating the components of the migration to Azure that require you to provision an Azure Storage account.
For each of the following statements, select Yes if the statement is true. Otherwise, select No.

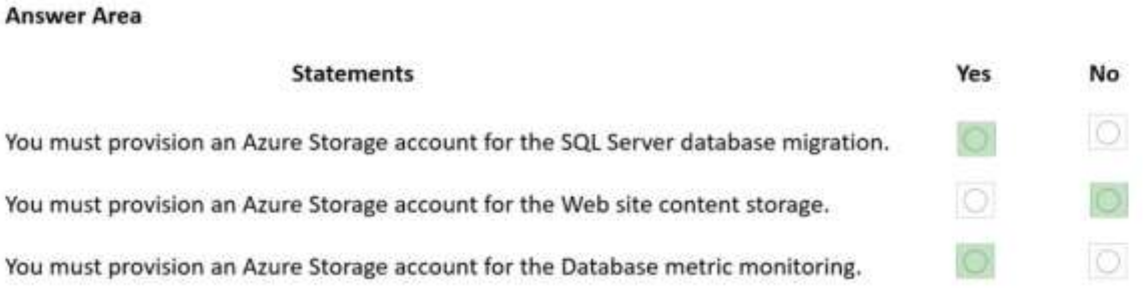
**NOTE:** Each correct selection is worth one point.



Answer Area

| Statements | Yes | No |
|---|---|---|
| You must provision an Azure Storage account for the SQL Server database migration. | ○ | ○ |
| You must provision an Azure Storage account for the Web site content storage. | ○ | ○ |
| You must provision an Azure Storage account for the Database metric monitoring. | ○ | ○ |

**Answer:**



Answer Area

| Statements | Yes | No |
|---|---|---|
| You must provision an Azure Storage account for the SQL Server database migration. | ● | ○ |
| You must provision an Azure Storage account for the Web site content storage. | ○ | ● |
| You must provision an Azure Storage account for the Database metric monitoring. | ● | ○ |

**QUESTION 8**

**Case Study 2 - Fabrikam, Inc**

**Overview**

Fabrikam, Inc. is an engineering company that has offices throughout Europe. The company has a main office in London and three branch offices in Amsterdam, Berlin, and Rome.

**Existing Environment: Active Directory Environment**

The network contains two Active Directory forests named corp.fabrikam.com and rd.fabrikam.com. There are no trust relationships between the forests.

Corp.fabrikam.com is a production forest that contains identities used for internal user and computer authentication.

Rd.fabrikam.com is used by the research and development (R&D) department only. The R&D department is restricted to using on-premises resources only.

**Existing Environment: Network Infrastructure**

Each office contains at least one domain controller from the corp.fabrikam.com domain. The main office contains all the domain controllers for the rd.fabrikam.com forest.

All the offices have a high-speed connection to the internet.

An existing application named WebApp1 is hosted in the data center of the London office. WebApp1 is used by customers to place and track orders. WebApp1 has a web tier that uses Microsoft Internet information Services (IIS) and a database tier that runs Microsoft SQL Server 2016. The web tier and the database tier are deployed to virtual machines that run on Hyper-V.

The IT department currently uses a separate Hyper-V environment to test updates to WebApp1.

Fabrikam purchases all Microsoft licenses through a Microsoft Enterprise Agreement that includes Software Assurance.

**Existing Environment: Problem Statements**

The use of WebApp1 is unpredictable. At peak times, users often report delays. At other times, many resources for

WebApp1 are underutilized.

**Requirements: Planned Changes**

Fabrikam plans to move most of its production workloads to Azure during the next few years, including virtual machines that rely on Active Directory for authentication.

As one of its first projects, the company plans to establish a hybrid identity model, facilitating an upcoming Microsoft 365 deployment.

All R&D operations will remain on-premises.

Fabrikam plans to migrate the production and test instances of WebApp1 to Azure.

**Requirements: Technical Requirements**

Fabrikam identifies the following technical requirements:

- Website content must be easily updated from a single point.
- User input must be minimized when provisioning new web app instances.
- Whenever possible, existing on-premises licenses must be used to reduce cost.
- Users must always authenticate by using their corp.fabrikam.com UPN identity.
- Any new deployments to Azure must be redundant in case an Azure region fails.
- Whenever possible, solutions must be deployed to Azure by using the Standard pricing tier of Azure App Service.
- An email distribution group named IT Support must be notified of any issues relating to the directory synchronization services.
- In the event that a link fails between Azure and the on-premises network, ensure that the virtual machines hosted in Azure can authenticate to Active Directory.
- Directory synchronization between Azure Active Directory (Azure AD) and corp.fabrikam.com must not be affected by a link failure between Azure and the on-premises network.

**Requirements: Database Requirements**

Fabrikam identifies the following database requirements:

- Database metrics for the production instance of WebApp1 must be available for analysis so that database administrators can optimize the performance settings.
- To avoid disrupting customer access, database downtime must be minimized when databases are migrated.
- Database backups must be retained for a minimum of seven years to meet compliance requirements.

**Requirements: Security Requirements**

Fabrikam identifies the following security requirements:

- Company information including policies, templates, and data must be inaccessible to anyone outside the company.
- Users on the on-premises network must be able to authenticate to corp.fabrikam.com if an internet link fails.
- Administrators must be able authenticate to the Azure portal by using their corp.fabrikam.com credentials.
- All administrative access to the Azure portal must be secured by using multi-factor authentication (MFA).
- The testing of WebApp1 updates must not be visible to anyone outside the company.

What should you include in the identity management strategy to support the planned changes?

A. Deploy domain controllers for corp.fabrikam.com to virtual networks in Azure.
B. Move all the domain controllers from corp.fabrikam.com to virtual networks in Azure.
C. Deploy a new Azure AD tenant for the authentication of new R&D projects.
D. Deploy domain controllers for the rd.fabrikam.com forest to virtual networks in Azure.

**Answer:** A

**Explanation:**

Directory synchronization between Azure Active Directory (Azure AD) and corp.fabrikam.com must not be affected by a link failure between Azure and the on-premises network. (This requires domain controllers in Azure).

Users on the on-premises network must be able to authenticate to corp.fabrikam.com if an Internet link fails. (This requires domain controllers on-premises).

**QUESTION 9**

**Case Study 3 - Contoso**

**Existing Environment: Technical Environment**

The on-premises network contains a single Active Directory domain named contoso.com.

Contoso has a single Azure subscription.

**Existing Environment: Business Partnerships**

Contoso has a business partnership with Fabrikam, Inc. Fabrikam users access some Contoso applications over the internet by using Azure Active Directory (Azure AD) guest accounts.

**Requirements: Planned Changes**

Contoso plans to deploy two applications named App1 and App2 to Azure.

**Requirements: App1**

App1 will be a Python web app hosted in Azure App Service that requires a Linux runtime. Users from Contoso and Fabrikam will access App1.

App1 will access several services that require third-party credentials and access strings. The credentials and access strings are stored in Azure Key Vault.

App1 will have six instances: three in the East US Azure region and three in the West Europe Azure region.

App1 has the following data requirements:

- Each instance will write data to a data store in the same availability zone as the instance.
- Data written by any App1 instance must be visible to all App1 instances.

App1 will only be accessible from the internet. App1 has the following connection requirements:

- Connections to App1 must pass through a web application firewall (WAF).
- Connections to App1 must be active-active load balanced between instances.
- All connections to App1 from North America must be directed to the East US region. All other connections must be directed to the West Europe region.

Every hour, you will run a maintenance task by invoking a PowerShell script that copies files from all the App1 instances. The PowerShell script will run from a central location.

**Requirements: App2**

App2 will be a NET app hosted in App Service that requires a Windows runtime. App2 has the following file storage requirements:

- Save files to an Azure Storage account.
- Replicate files to an on-premises location.
- Ensure that on-premises clients can read the files over the LAN by using the SMB protocol.

You need to monitor App2 to analyze how long it takes to perform different transactions within the application. The solution must not require changes to the application code.

**Application Development Requirements**

Application developers will constantly develop new versions of App1 and App2. The development process must meet the following requirements:

- A staging instance of a new application version must be deployed to the application host before the new version is used in production.
- After testing the new version, the staging version of the application will replace the production version.
- The switch to the new application version from staging to production must occur without any downtime of the application.

**Identity Requirements**

Contoso identifies the following requirements for managing Fabrikam access to resources:

- Every month, an account manager at Fabrikam must review which Fabrikam users have access permissions to App1. Accounts that no longer need permissions must be removed as guests.
- The solution must minimize development effort.

**Security Requirement**

All secrets used by Azure services must be stored in Azure Key Vault.

Services that require credentials must have the credentials tied to the service instance. The credentials must **NOT** be shared between services.

You need to recommend a solution that meets the data requirements for App1.

What should you recommend deploying to each availability zone that contains an instance of App1?

A. an Azure Cosmos DB that uses multi-region writes  
B. an Azure Data Lake store that uses geo-zone-redundant storage (GZRS)  
C. an Azure SQL database that uses active geo-replication  
D. an Azure Storage account that uses geo-zone-redundant storage (GZRS)

**Answer:** A

**Explanation:**

Scenario: App1 has the following data requirements:

Each instance will write data to a data store in the same availability zone as the instance.
Data written by any App1 instance must be visible to all App1 instances.
Azure Cosmos DB: Each partition across all the regions is replicated. Each region contains all the data partitions of an Azure Cosmos container and can serve reads as well as serve writes when multi-region writes is enabled.
Incorrect Answers:
B, D: GZRS protects against failures. Geo-redundant storage (with GRS or GZRS) replicates your data to another physical location in the secondary region to protect against regional outages. However, that data is available to be read only if the customer or Microsoft initiates a failover from the primary to secondary region.
C: Active geo-replication is designed as a business continuity solution that lets you perform quick disaster recovery of individual databases in case of a regional disaster or a large scale outage. Once geo-replication is set up, you can initiate a geo-failover to a geo-secondary in a different Azure region. The geo-failover is initiated programmatically by the application or manually by the user.
Reference:
https://docs.microsoft.com/en-us/azure/cosmos-db/high-availability

**QUESTION 10**
**Case Study 3 - Contoso**
**Existing Environment: Technical Environment**
The on-premises network contains a single Active Directory domain named contoso.com.
Contoso has a single Azure subscription.
**Existing Environment: Business Partnerships**
Contoso has a business partnership with Fabrikam, Inc. Fabrikam users access some Contoso applications over the internet by using Azure Active Directory (Azure AD) guest accounts.
**Requirements: Planned Changes**
Contoso plans to deploy two applications named App1 and App2 to Azure.
**Requirements: App1**
App1 will be a Python web app hosted in Azure App Service that requires a Linux runtime. Users from Contoso and Fabrikam will access App1.
App1 will access several services that require third-party credentials and access strings. The credentials and access strings are stored in Azure Key Vault.
App1 will have six instances: three in the East US Azure region and three in the West Europe Azure region.
App1 has the following data requirements:

- Each instance will write data to a data store in the same availability zone as the instance.
- Data written by any App1 instance must be visible to all App1 instances.

App1 will only be accessible from the internet. App1 has the following connection requirements:

- Connections to App1 must pass through a web application firewall (WAF).
- Connections to App1 must be active-active load balanced between instances.
- All connections to App1 from North America must be directed to the East US region. All other connections must be directed to the West Europe region.

Every hour, you will run a maintenance task by invoking a PowerShell script that copies files from all the App1 instances. The PowerShell script will run from a central location.
**Requirements: App2**
App2 will be a NET app hosted in App Service that requires a Windows runtime. App2 has the following file storage requirements:

- Save files to an Azure Storage account.
- Replicate files to an on-premises location.
- Ensure that on-premises clients can read the files over the LAN by using the SMB protocol.

You need to monitor App2 to analyze how long it takes to perform different transactions within the application. The solution must not require changes to the application code.
**Application Development Requirements**
Application developers will constantly develop new versions of App1 and App2. The development process must meet the following requirements:

- A staging instance of a new application version must be deployed to the application host before the new version is used in production.
- After testing the new version, the staging version of the application will replace the production version.
- The switch to the new application version from staging to production must occur without any downtime of the application.

**Identity Requirements**

Contoso identifies the following requirements for managing Fabrikam access to resources:

- Every month, an account manager at Fabrikam must review which Fabrikam users have access permissions to App1. Accounts that no longer need permissions must be removed as guests.
- The solution must minimize development effort.

**Security Requirement**

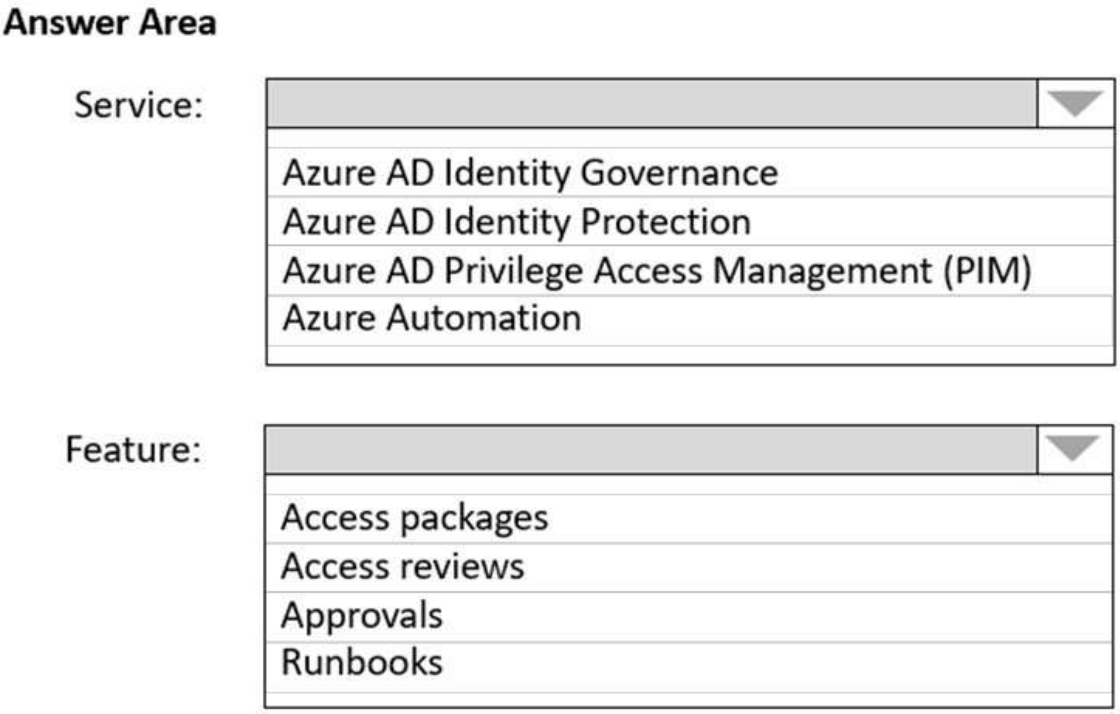
All secrets used by Azure services must be stored in Azure Key Vault.

Services that require credentials must have the credentials tied to the service instance. The credentials must **NOT** be shared between services.

Hotspot Question

What should you implement to meet the identity requirements? To answer, select the appropriate options in the answer area.

**NOTE:** Each correct selection is worth one point.



Answer Area

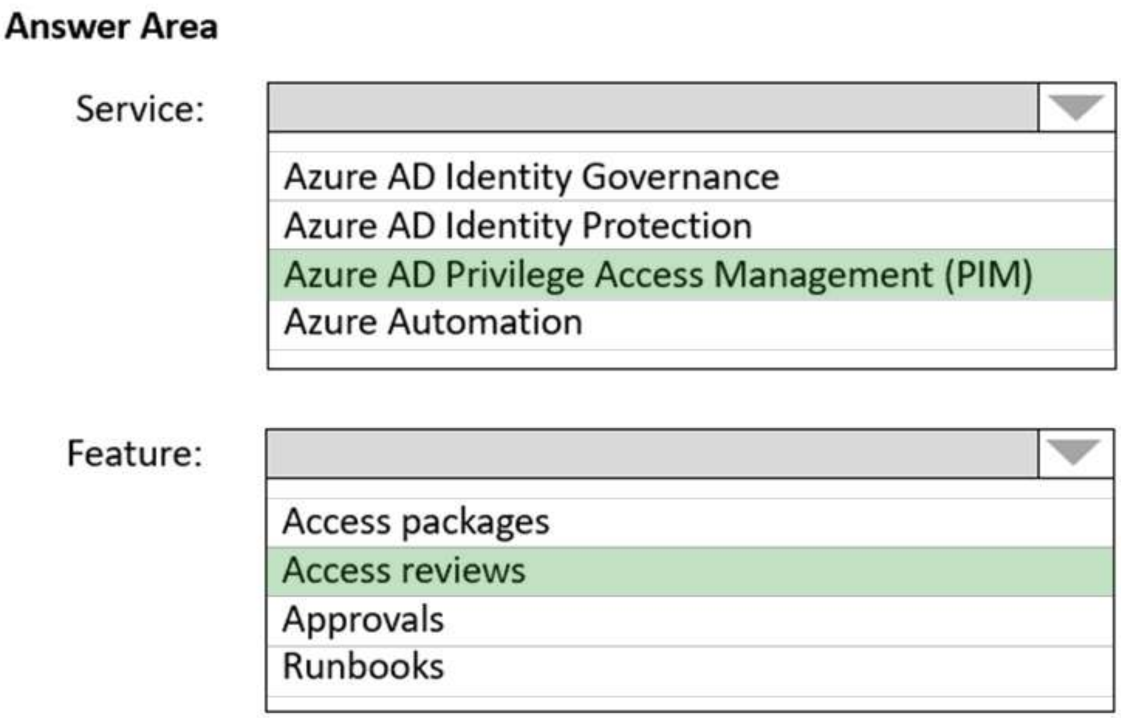
Service:

- Azure AD Identity Governance
- Azure AD Identity Protection
- Azure AD Privilege Access Management (PIM)
- Azure Automation

Feature:

- Access packages
- Access reviews
- Approvals
- Runbooks

**Answer:**



Answer Area

Service:

- Azure AD Identity Governance
- Azure AD Identity Protection
- [✓ Azure AD Privilege Access Management (PIM)]
- Azure Automation

Feature:

- Access packages
- [✓ Access reviews]
- Approvals
- Runbooks

**Explanation:**
Requirements: Identity Requirements
Contoso identifies the following requirements for managing Fabrikam access to resources:

- Every month, an account manager at Fabrikam must review which Fabrikam users have access permissions to App1. Accounts that no longer need permissions must be removed as guests.
- The solution must minimize development effort.

Box 1: The Azure AD Privileged Identity Management (PIM)
When should you use access reviews?

- Too many users in privileged roles: It's a good idea to check how many users have administrative access, how many of them are Global Administrators, and if there are any invited guests or partners that have not been removed after being assigned to do an administrative task. You can recertify the role assignment users in Azure AD roles such as Global Administrators, or Azure resources roles such as User Access Administrator in the Azure AD Privileged Identity Management (PIM) experience.

Box 2: Access reviews
Azure Active Directory (Azure AD) access reviews enable organizations to efficiently manage group memberships, access to enterprise applications, and role assignments. User's access can be reviewed on a regular basis to make sure only the right people have continued access.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/governance/access-reviews-overview

**QUESTION 11**
**Case Study 3 - Contoso**
**Existing Environment: Technical Environment**
The on-premises network contains a single Active Directory domain named contoso.com.
Contoso has a single Azure subscription.
**Existing Environment: Business Partnerships**
Contoso has a business partnership with Fabrikam, Inc. Fabrikam users access some Contoso applications over the internet by using Azure Active Directory (Azure AD) guest accounts.
**Requirements: Planned Changes**
Contoso plans to deploy two applications named App1 and App2 to Azure.
**Requirements: App1**
App1 will be a Python web app hosted in Azure App Service that requires a Linux runtime. Users from Contoso and Fabrikam will access App1.
App1 will access several services that require third-party credentials and access strings. The credentials and access

strings are stored in Azure Key Vault.
App1 will have six instances: three in the East US Azure region and three in the West Europe Azure region.
App1 has the following data requirements:

- Each instance will write data to a data store in the same availability zone as the instance.
- Data written by any App1 instance must be visible to all App1 instances.

App1 will only be accessible from the internet. App1 has the following connection requirements:

- Connections to App1 must pass through a web application firewall (WAF).
- Connections to App1 must be active-active load balanced between instances.
- All connections to App1 from North America must be directed to the East US region. All other connections must be directed to the West Europe region.

Every hour, you will run a maintenance task by invoking a PowerShell script that copies files from all the App1 instances. The PowerShell script will run from a central location.

**Requirements: App2**

App2 will be a NET app hosted in App Service that requires a Windows runtime. App2 has the following file storage requirements:

- Save files to an Azure Storage account.
- Replicate files to an on-premises location.
- Ensure that on-premises clients can read the files over the LAN by using the SMB protocol.

You need to monitor App2 to analyze how long it takes to perform different transactions within the application. The solution must not require changes to the application code.

**Application Development Requirements**

Application developers will constantly develop new versions of App1 and App2. The development process must meet the following requirements:

- A staging instance of a new application version must be deployed to the application host before the new version is used in production.
- After testing the new version, the staging version of the application will replace the production version.
- The switch to the new application version from staging to production must occur without any downtime of the application.

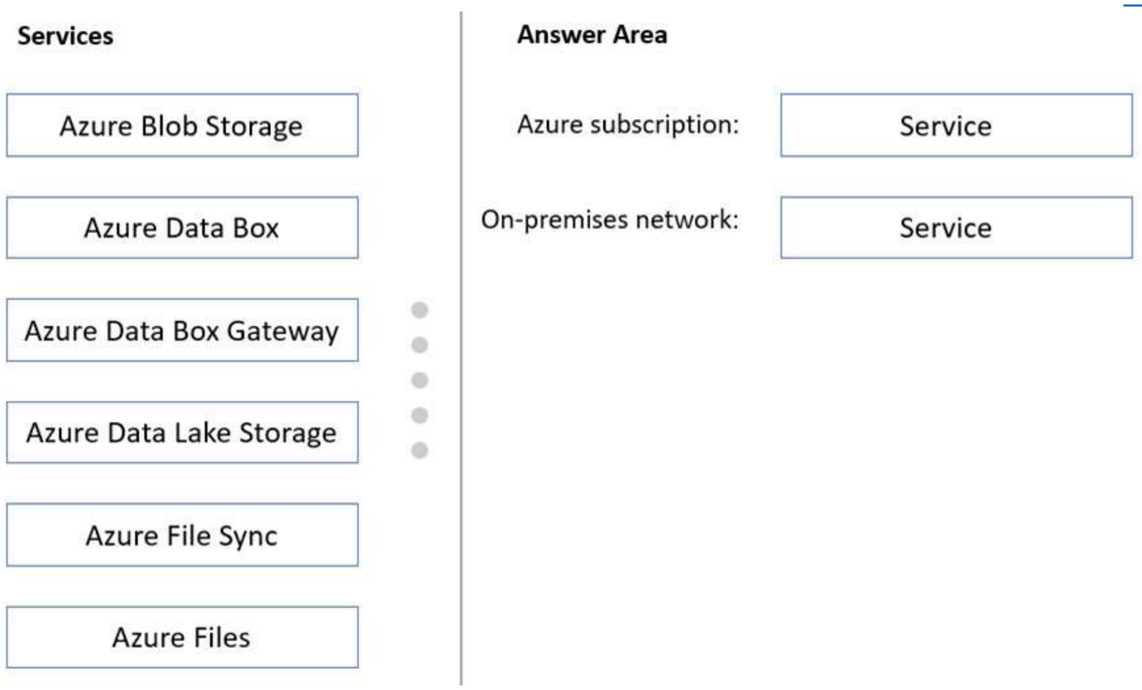
**Identity Requirements**

Contoso identifies the following requirements for managing Fabrikam access to resources:

- Every month, an account manager at Fabrikam must review which Fabrikam users have access permissions to App1. Accounts that no longer need permissions must be removed as guests.
- The solution must minimize development effort.

**Security Requirement**

All secrets used by Azure services must be stored in Azure Key Vault.
Services that require credentials must have the credentials tied to the service instance. The credentials must **NOT** be shared between services.
Drag and Drop Question
You need to recommend a solution that meets the file storage requirements for App2.
What should you deploy to the Azure subscription and the on-premises network? To answer, drag the appropriate services to the correct locations. Each service 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.



Services

Azure Blob Storage

Azure Data Box

Azure Data Box Gateway

Azure Data Lake Storage

Azure File Sync

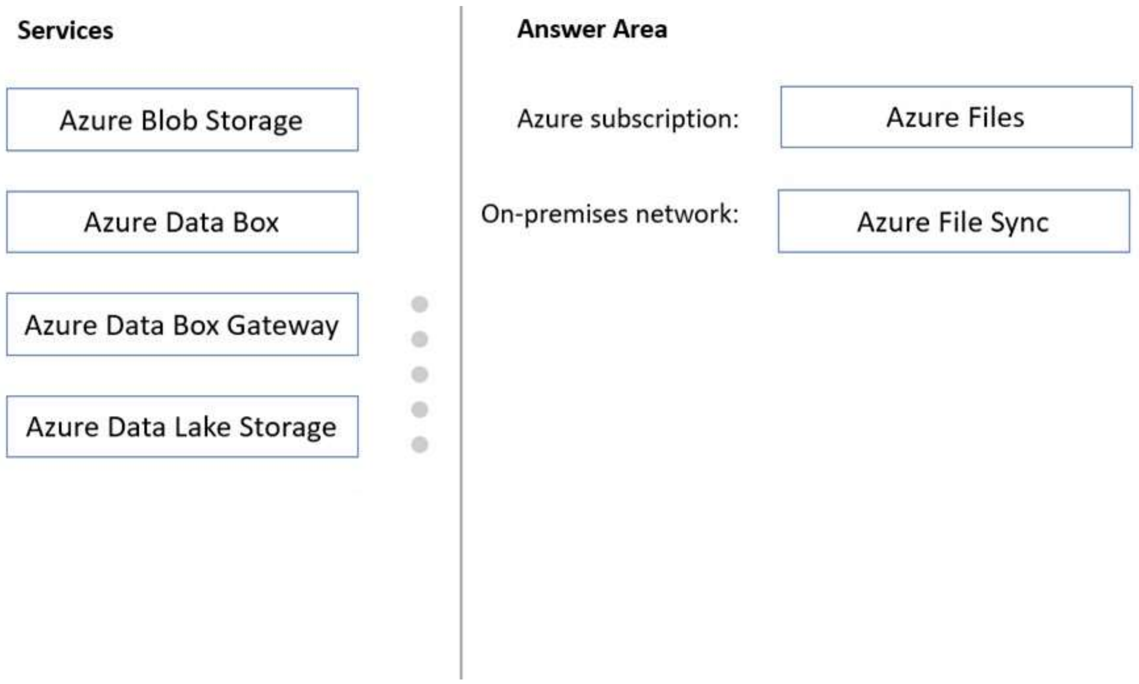
Azure Files

Answer Area

Azure subscription: Service

On-premises network: Service

**Answer:**



Services

Azure Blob Storage

Azure Data Box

Azure Data Box Gateway

Azure Data Lake Storage

Answer Area

Azure subscription: Azure Files

On-premises network: Azure File Sync

**Explanation:**
Box 1: Azure Files
Scenario: App2 has the following file storage requirements:

- Save files to an Azure Storage account.
- Replicate files to an on-premises location.
- Ensure that on-premises clients can read the files over the LAN by using the SMB protocol.

Box 2: Azure File Sync
Use Azure File Sync to centralize your organization's file shares in Azure Files, while keeping the flexibility, performance, and compatibility of an on-premises file server. Azure File Sync transforms Windows Server into a quick cache of your Azure file share. You can use any protocol that's available on Windows Server to access your data locally, including SMB, NFS, and FTPS. You can have as many caches as you need across the world.
Reference:
https://docs.microsoft.com/en-us/azure/storage/file-sync/file-sync-deployment-guide

**QUESTION 12**
**Case Study 3 - Contoso**
**Existing Environment: Technical Environment**
The on-premises network contains a single Active Directory domain named contoso.com.
Contoso has a single Azure subscription.
**Existing Environment: Business Partnerships**
Contoso has a business partnership with Fabrikam, Inc. Fabrikam users access some Contoso applications over the internet by using Azure Active Directory (Azure AD) guest accounts.
**Requirements: Planned Changes**
Contoso plans to deploy two applications named App1 and App2 to Azure.
**Requirements: App1**
App1 will be a Python web app hosted in Azure App Service that requires a Linux runtime. Users from Contoso and Fabrikam will access App1.
App1 will access several services that require third-party credentials and access strings. The credentials and access strings are stored in Azure Key Vault.
App1 will have six instances: three in the East US Azure region and three in the West Europe Azure region.
App1 has the following data requirements:
- Each instance will write data to a data store in the same availability zone as the instance.
- Data written by any App1 instance must be visible to all App1 instances.

App1 will only be accessible from the internet. App1 has the following connection requirements:
- Connections to App1 must pass through a web application firewall (WAF).
- Connections to App1 must be active-active load balanced between instances.
- All connections to App1 from North America must be directed to the East US region. All other connections must be directed to the West Europe region.

Every hour, you will run a maintenance task by invoking a PowerShell script that copies files from all the App1 instances. The PowerShell script will run from a central location.
**Requirements: App2**
App2 will be a NET app hosted in App Service that requires a Windows runtime. App2 has the following file storage requirements:
- Save files to an Azure Storage account.
- Replicate files to an on-premises location.
- Ensure that on-premises clients can read the files over the LAN by using the SMB protocol.

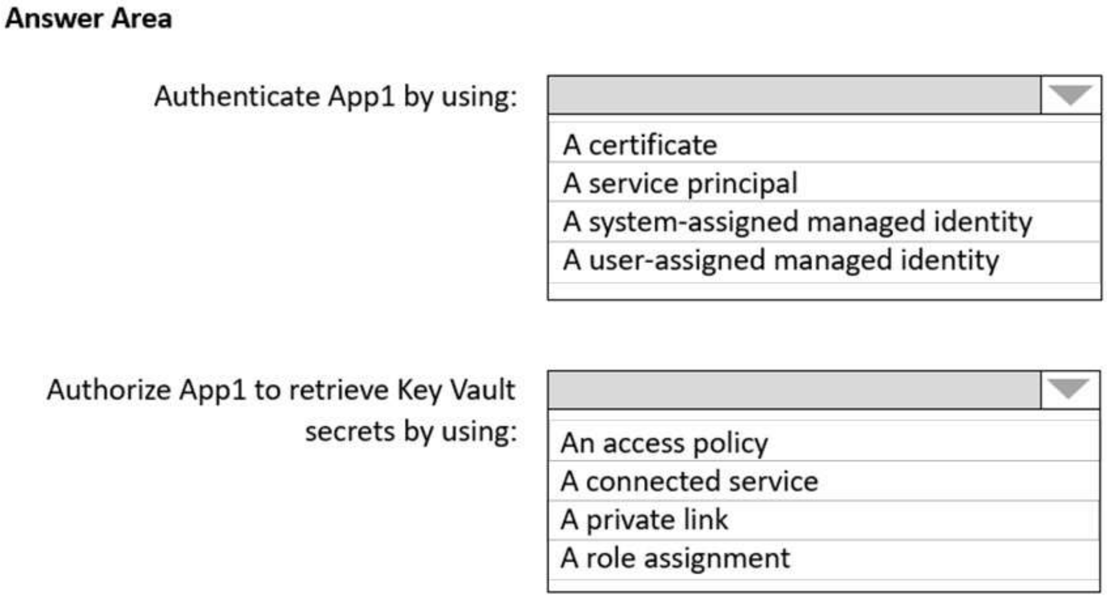
You need to monitor App2 to analyze how long it takes to perform different transactions within the application. The solution must not require changes to the application code.
**Application Development Requirements**
Application developers will constantly develop new versions of App1 and App2. The development process must meet the following requirements:
- A staging instance of a new application version must be deployed to the application host before the new version is used in production.
- After testing the new version, the staging version of the application will replace the production version.
- The switch to the new application version from staging to production must occur without any downtime of the application.

**Identity Requirements**
Contoso identifies the following requirements for managing Fabrikam access to resources:
- Every month, an account manager at Fabrikam must review which Fabrikam users have access permissions to App1. Accounts that no longer need permissions must be removed as guests.
- The solution must minimize development effort.

**Security Requirement**
All secrets used by Azure services must be stored in Azure Key Vault.
Services that require credentials must have the credentials tied to the service instance. The credentials must **NOT** be shared between services.
Hotspot Question

You need to recommend a solution to ensure that App1 can access the third-party credentials and access strings. The solution must meet the security requirements.
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

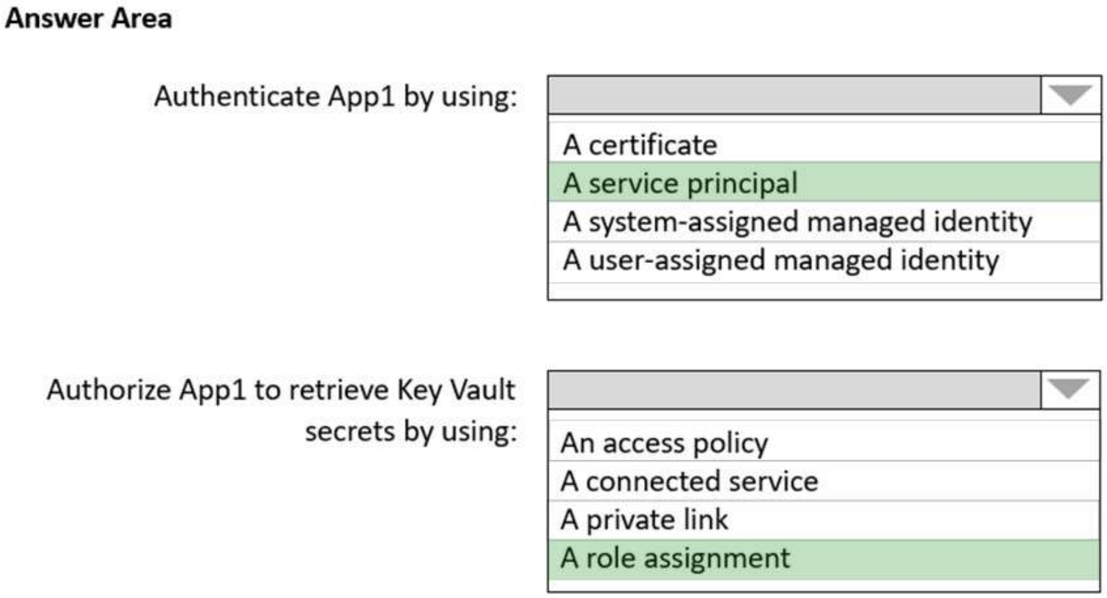
Authenticate App1 by using:

- A certificate
- A service principal
- A system-assigned managed identity
- A user-assigned managed identity

Authorize App1 to retrieve Key Vault secrets by using:

- An access policy
- A connected service
- A private link
- A role assignment

**Answer:**



Answer Area

Authenticate App1 by using:

- A certificate
- [✓ A service principal]
- A system-assigned managed identity
- A user-assigned managed identity

Authorize App1 to retrieve Key Vault secrets by using:

- An access policy
- A connected service
- A private link
- [✓ A role assignment]

**Explanation:**
Scenario: Security Requirement
All secrets used by Azure services must be stored in Azure Key Vault.
Services that require credentials must have the credentials tied to the service instance. The credentials must NOT be shared between services.
Box 1: A service principal
A service principal is a type of security principal that identifies an application or service, which is to say, a piece of code rather than a user or group. A service principal's object ID is known as its client ID and acts like its username. The service principal's client secret acts like its password.
Note: Authentication with Key Vault works in conjunction with Azure Active Directory (Azure AD), which is responsible for authenticating the identity of any given security principal.
A security principal is an object that represents a user, group, service, or application that's requesting access to Azure resources. Azure assigns a unique object ID to every security principal.
Box 2: A role assignment
You can provide access to Key Vault keys, certificates, and secrets with an Azure role-based access control.
Reference:

https://docs.microsoft.com/en-us/azure/key-vault/general/authentication

**QUESTION 13**
You have an Azure subscription that contains a custom application named Application1. Application1 was developed by an external company named Fabrikam, Ltd. Developers at Fabrikam were assigned role-based access control (RBAC) permissions to the Application1 components. All users are licensed for the Microsoft 365 E5 plan.
You need to recommend a solution to verify whether the Fabrikam developers still require permissions to Application1. The solution must meet the following requirements:
・To the manager of the developers, send a monthly email message that lists the access permissions to Application1.
・If the manager does not verify an access permission, automatically revoke that permission.
・Minimize development effort.
What should you recommend?

A. In Azure Active Directory (Azure AD), create an access review of Application1.
B. Create an Azure Automation runbook that runs the `Get-AzRoleAssignment` cmdlet.
C. In Azure Active Directory (Azure AD) Privileged Identity Management, create a custom role assignment for the Application1 resources.
D. Create an Azure Automation runbook that runs the `Get-AzureADUserAppRoleAssignment` cmdlet.

**Answer:** A
**Explanation:**
https://docs.microsoft.com/en-us/azure/active-directory/governance/manage-user-access-with-access-reviews

**QUESTION 14**
You have an Azure subscription. The subscription has a blob container that contains multiple blobs.
Ten users in the finance department of your company plan to access the blobs during the month of April.
You need to recommend a solution to enable access to the blobs during the month of April only.
Which security solution should you include in the recommendation?

A. shared access signatures (SAS)
B. Conditional Access policies
C. certificates
D. access keys

**Answer:** A
**Explanation:**
Shared Access Signatures (SAS) allows for limited-time fine grained access control to resources. So you can generate URL, specify duration (for month of April) and disseminate URL to 10 team members. On May 1, the SAS token is automatically invalidated, denying team members continued access.
Reference:
https://docs.microsoft.com/en-us/azure/storage/common/storage-sas-overview

**QUESTION 15**
You have an Azure Active Directory (Azure AD) tenant that syncs with an on-premises Active Directory domain.
You have an internal web app named WebApp1 that is hosted on-premises. WebApp1 uses Integrated Windows authentication.
Some users work remotely and do **NOT** have VPN access to the on-premises network.
You need to provide the remote users with single sign-on (SSO) access to WebApp1.
Which two features should you include in the solution? Each correct answer presents part of the solution.
**NOTE:** Each correct selection is worth one point.

A. Azure AD Application Proxy
B. Azure AD Privileged Identity Management (PIM)
C. Conditional Access policies
D. Azure Arc

E. Azure AD enterprise applications
F. Azure Application Gateway

**Answer:** AC
**Explanation:**
A: Application Proxy is a feature of Azure AD that enables users to access on-premises web applications from a remote client. Application Proxy includes both the Application Proxy service which runs in the cloud, and the Application Proxy connector which runs on an on-premises server.
You can configure single sign-on to an Application Proxy application.
C: Microsoft recommends using Application Proxy with pre-authentication and Conditional Access policies for remote access from the internet. An approach to provide Conditional Access for intranet use is to modernize applications so they can directly authenticate with AAD.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy-config-sso-how-to
https://docs.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy-deployment-plan