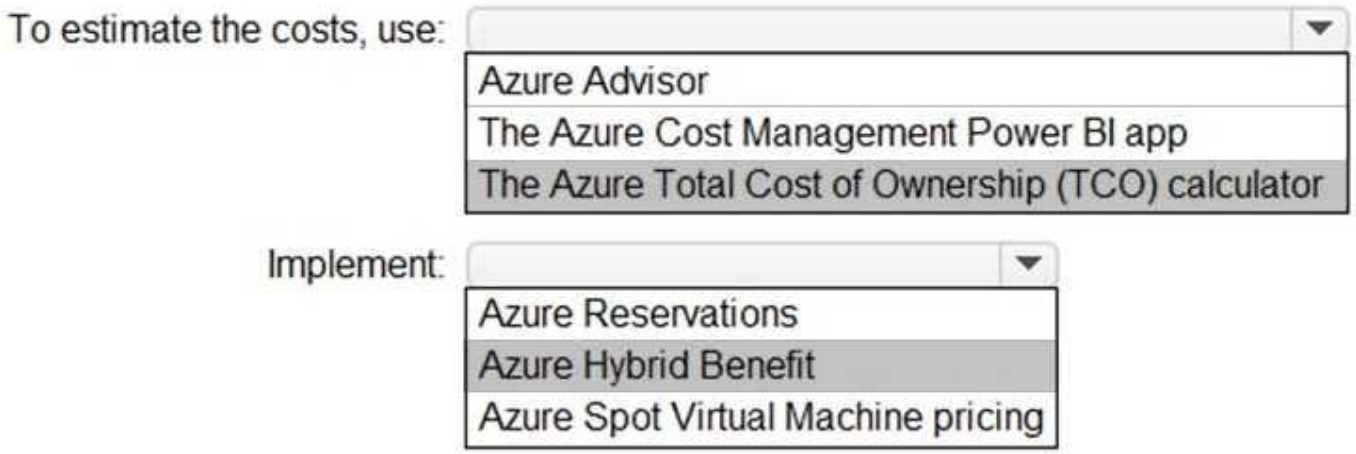
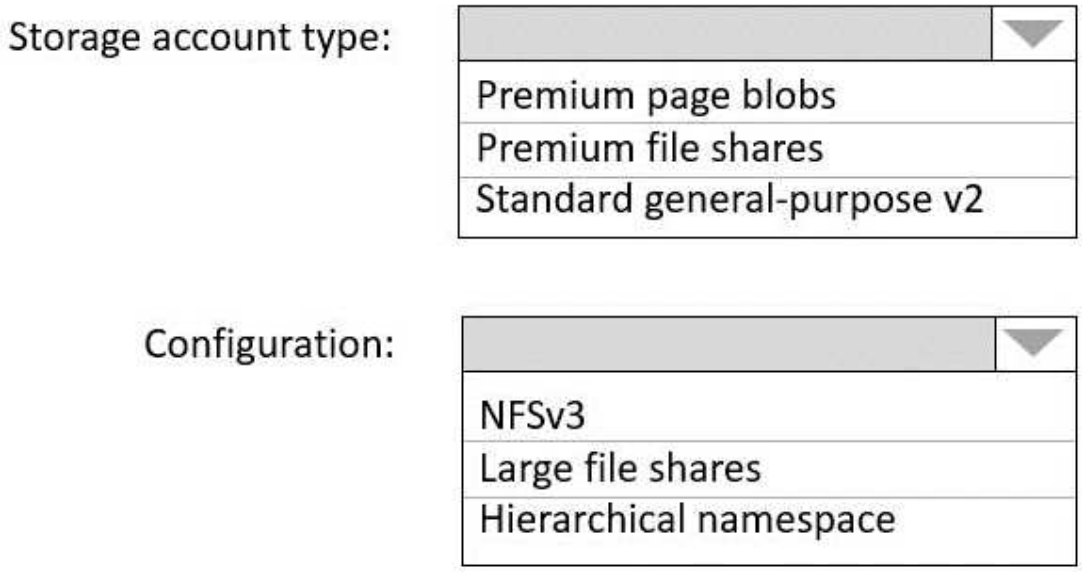


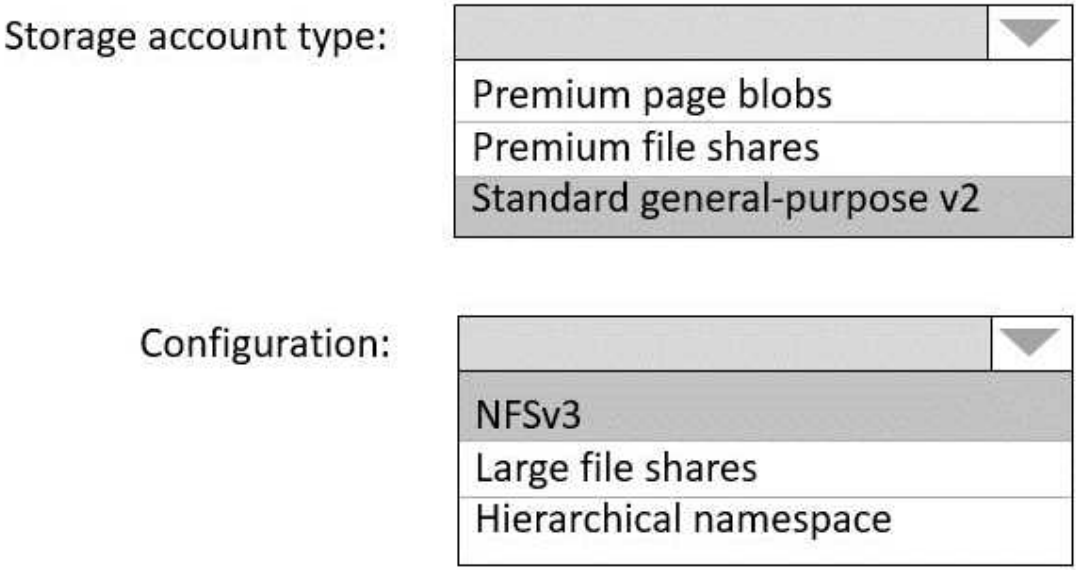
Explanation:
Box 1: The Azure Total Cost of Ownership (TCO) Calculator
The Total Cost of Ownership (TCO) Calculator estimates the cost savings you can realize by migrating your workloads to Azure.
Note: The TCO Calculator recommends a set of equivalent services in Azure that will support your applications. Our analysis will show each cost area with an estimate of your on-premises spend versus your spend in Azure. There are several cost categories that either decrease or go away completely when you move workloads to the cloud.
Box 2: Azure Hybrid Benefit
Azure Hybrid Benefit is a licensing benefit that helps you to significantly reduce the costs of running your workloads in the cloud. It works by letting you use your on-premises Software Assuranceenabled Windows Server and SQL Server licenses on Azure. And now, this benefit applies to RedHat and SUSE Linux subscriptions, too.
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.
Reference:
https://azure.microsoft.com/en-us/pricing/tco/
https://azure.microsoft.com/en-us/pricing/hybrid-benefit/

QUESTION 7
HOTSPOT
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:



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 8
You migrate App1 to Azure. You need to ensure that the data storage for App1 meets the security and compliance requirement
What should you do?

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

Answer: A

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 9
HOTSPOT
How should the migrated databases DB1 and DB2 be implemented in Azure?

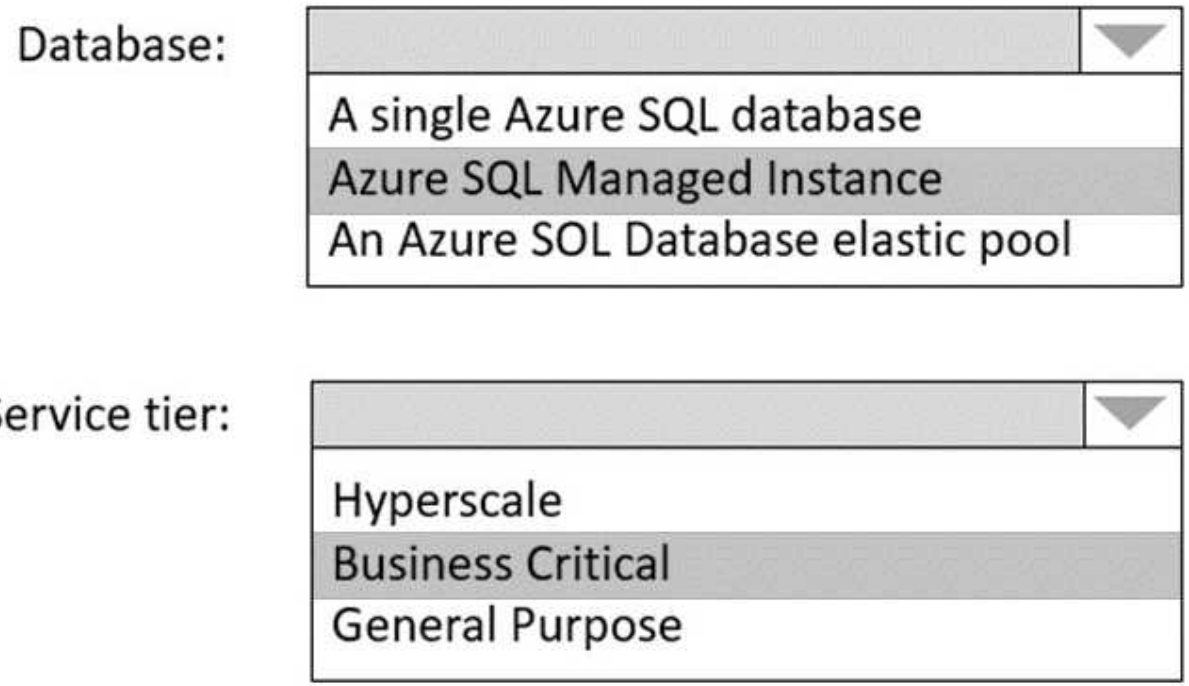
Database:

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

Service tier:

- Hyperscale
- Business Critical
- General Purpose

Answer:



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-paasoverview

---

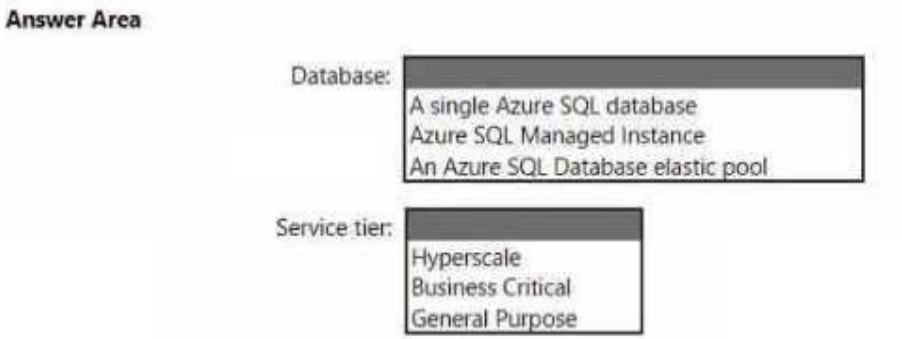
QUESTION 10
You need to implement the Azure RBAC role assignments for the Network Contributor role. The solution must meet the authentication and authorization requirements.
What is the minimum number of assignments that you must use?

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

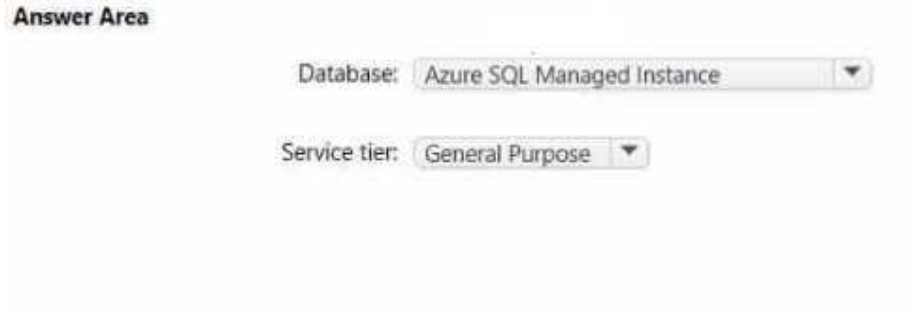
Answer: A

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 11
HOTSPOT
You plan to migrate DB1 and DB2 to Azure.
You need to ensure that the Azure database and the service tier meet the resiliency and business requirements.
What should you configure? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:



Explanation:

New Topic: Topic 2, Fabrikam, inc Case Study A

Overview:

Existing Environment

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.

Active Directory Environment:

The network contains two Active Directory forests named corp.fabnkam.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.

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.
Problem Statement:
The use of Web App1 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.
As one of its first projects, the company plans to establish a hybrid identity model, facilitating an upcoming Microsoft Office 365 deployment
All R&D operations will remain on-premises.
Fabrikam plans to migrate the production and test instances of WebApp1 to Azure.
Technical Requirements:
Fabrikam identifies the following technical requirements:
Web site content must be easily updated from a single point.
User input must be minimized when provisioning new 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 platform as a service (PaaS).
An email distribution group named IT Support must be notified of any issues relating to the directory synchronization services.
Directory synchronization between Azure Active Directory (Azure AD) and corp.fabhkam.com must not be affected by a link failure between Azure and the on premises network.
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 requirement
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.
*The testing of WebApp1 updates must not be visible to anyone outside the company.

QUESTION 12
HOTSPOT
To meet the authentication requirements of Fabrikam, what should you include in the solution? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.