Custom View Settings

Topic 15 - Testlet 8

Question #1 *Topic 15*

Introductory Info

Case Study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs When you are ready to answer a question, click the Question button to return to the question.

Overview -

Litware, Inc. is a medium-sized finance company that has a main office in Boston.

Existing Environment -

Identity Environment -

The network contains an Active Directory forest named litware.com that is linked to an Azure Active Directory (Azure AD) tenant named litware.com. All users have Azure Active Directory Premium P2 licenses.

Litware has a second Azure AD tenant named dev.litware.com that is used as a development environment.

The litware.com tenant has a Conditional Access policy named Capolicy1. Capolicy1 requires that when users manage the Azure subscription for a production environment by using the Azure portal, they must connect from a hybrid Azure AD-joined device.

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 SERVER2 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

Planned Changes -
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 to management groups.

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.
▪

Question
HOTSPOT -
How should the migrated databases DB1 and DB2 be implemented in Azure?
Hot Area:

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 Area

Database:

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

Correct Answer:

Service tier:

- Hyperscale
- Business Critical
- General Purpose

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

Topic 16 - Testlet 9

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 #1 *Topic 16*

Introductory Info

Case Study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

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.

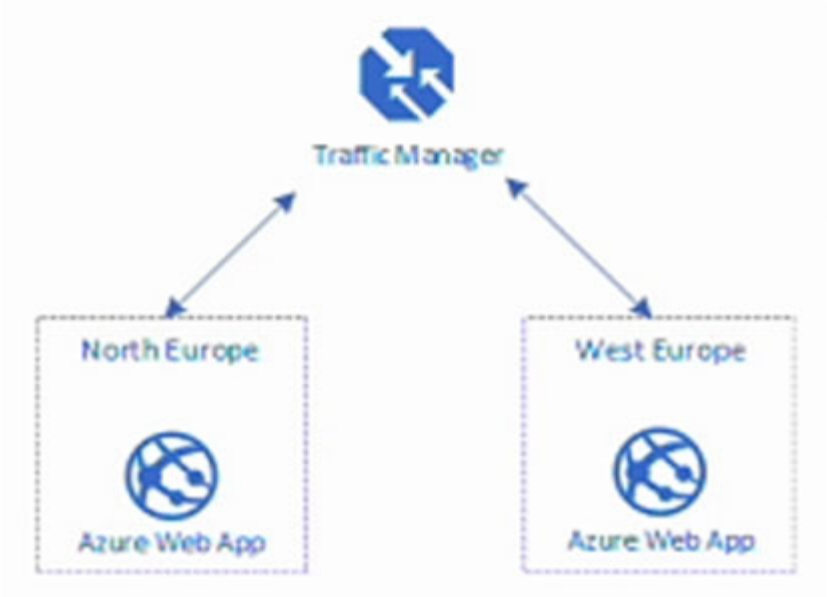
An email distribution group named IT Support must be notified of any issues relating to the directory synchronization services.

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.

Question

HOTSPOT -

You design a solution for the web tier of WebApp1 as shown in the exhibit.



For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.
Hot Area:

Statements	Yes	No
The design supports the technical requirements for redundancy.	○	○
The design supports autoscaling.	○	○
The design requires a manual configuration if an Azure region fails.	○	○

Correct Answer:
Box 1: Yes -
Any new deployments to Azure must be redundant in case an Azure region fails.
Traffic Manager is resilient to failure, including the failure of an entire Azure region.

Box 2: No -
Traffic Manager provides load balancing, but not auto-scaling.

Box 3: No -
Automatic failover using Azure Traffic Manager: when you have complex architectures and multiple sets of resources capable of performing the same function, you can configure Azure Traffic Manager (based on DNS) to check the health of your resources and route the traffic from the non-healthy resource to the healthy resource.
Reference:
https://docs.microsoft.com/en-us/azure/traffic-manager/traffic-manager-overview https://docs.microsoft.com/en-us/azure/networking/disaster-recovery-dns-traffic-manager
Social Media