

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.

Question

HOTSPOT -

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.

Hot Area:

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 Area

Service:

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

Correct Answer:

Feature:

	▼
Access packages	
Access reviews	
Approvals	
Runbooks	

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: Azure AD Identity Governance

Incorrect:

Not PIM: Life Cycle Requirements must be met.

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>

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 -

Contoso, Ltd. is a research company that has a main office in Montreal.

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.

Question

What should you recommend to meet the monitoring requirements for App2?

- A. VM insights
- B. Azure Application Insights
- C. Microsoft Sentinel
- D. Container insights

Correct Answer: B

Scenario: 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.

Unified cross-component transaction diagnostics.

The unified diagnostics experience automatically correlates server-side telemetry from across all your Application Insights monitored components into a single view. It doesn't matter if you have multiple resources. Application Insights detects the underlying relationship and allows you to easily diagnose the application component, dependency, or exception that caused a transaction slowdown or failure.

Note: Components are independently deployable parts of your distributed/microservices application. Developers and operations teams have code-level visibility or access to telemetry generated by these application components.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-monitor/app/transaction-diagnostics>

Community vote distribution

B (100%)

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

You need to recommend a data storage strategy for WebApp1.

What should you include in the recommendation?

- A. an Azure virtual machine that runs SQL Server
- B. a fixed-size DTU Azure SQL database
- C. an Azure SQL Database elastic pool
- D. a vCore-based Azure SQL database

Correct Answer: D

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

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

Note: A virtual core (vCore) represents a logical CPU and offers you the option to choose between generations of hardware and the physical characteristics of the hardware (for example, the number of cores, the memory, and the storage size). The vCore-based purchasing model gives you flexibility, control, transparency of individual resource consumption, and a straightforward way to translate on-premises workload requirements to the cloud. This model optimizes price, and allows you to choose compute, memory, and storage resources based on your workload needs.

Incorrect:

Not C: Azure SQL Database elastic pools are a simple, cost-effective solution for managing and scaling multiple databases, not for a single database.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-sql/database/service-tiers-sql-database-vcore>

Community vote distribution

D (79%) C (16%) 5%

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 -

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.

Hot Area:

Answer Area

Database:

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

Service tier:

Hyperscale
Business Critical
General Purpose

Correct Answer:

Answer Area

Database:

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

Service tier:

Hyperscale
Business Critical
General Purpose

Box 1: An Azure SQL Database elastic pool

Scenario:

* 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.

* Litware identifies the following business requirements:

Minimize administrative effort.

Minimize costs.

Box 2: Business Critical

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 -

Contoso, Ltd. is a research company that has a main office in Montreal.

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