Custom View Settings

Topic 6 - Testlet 10

Question #1 *Topic 6*

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.

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.

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.

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
You need to recommend a solution for the App1 maintenance task. The solution must minimize costs.
What should you include in the recommendation?

A. an Azure logic app

B. an Azure function

C. an Azure virtual machine

D. an App Service WebJob

Correct Answer: *A*
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.
App1 will have six instances: three in the East US Azure region and three in the West Europe Azure region.
You can create and manage workflows with Azure PowerShell in Azure Logic Apps.
You can create a Consumption logic app in multi-tenant Azure Logic Apps by using the JSON file for a logic app workflow definition. You can then manage your logic app by running the cmdlets in the Az.LogicApp PowerShell module.
Reference:
https://docs.microsoft.com/en-us/azure/logic-apps/quickstart-logic-apps-azure-powershell

Community vote distribution
B (80%) A (20%)

Question #2 *Topic 6*

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.

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.

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.

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
You need to recommend a solution that meets the application development requirements.
What should you include in the recommendation?

A. the Azure App Configuration service

B. an Azure Container Registry instance

C. deployment slots

D. Continuous Integration/Continuous Deployment (CI/CD) sources

Correct Answer: *C*
When you deploy your web app, web app on Linux, mobile back end, or API app to Azure App Service, you can use a separate deployment slot instead of the default production slot when you're running in the Standard, Premium, or Isolated App Service plan tier. Deployment slots are live apps with their own host names.
App content and configurations elements can be swapped between two deployment slots, including the production slot.
Deploying your application to a non-production slot has the following benefits:
* You can validate app changes in a staging deployment slot before swapping it with the production slot.
* Deploying an app to a slot first and swapping it into production makes sure that all instances of the slot are warmed up before being swapped into production.
This eliminates downtime when you deploy your app.
* After a swap, the slot with previously staged app now has the previous production app. If the changes swapped into the production slot aren't as you expect, you can perform the same swap immediately to get your "last known good site" back.
Note: Application Development Requirements
Application developers will constantly develop new versions of App1 and App2. The development process must meet the following requirements:
ز€¢ A staging instance of a new application version must be deployed to the application host before the new version is used in production.
ز€¢ After testing the new version, the staging version of the application will replace the production version.
ز€¢ The switch to the new application version from staging to production must occur without any downtime of the application.
Reference:
https://docs.microsoft.com/en-us/azure/app-service/deploy-staging-slots

Community vote distribution
C (100%)

Question #3 *Topic 6*

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.

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.

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.

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
You need to recommend an App Service architecture that meets the requirements for App1. The solution must minimize costs.
What should you recommend?

A. one App Service Environment (ASE) per availability zone

B. one App Service Environment (ASE) per region

C. one App Service plan per region

D. one App Service plan per availability zone

Correct Answer: *B*
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.
Note: The Azure App Service Environment v2 is an Azure App Service feature that provides a fully isolated and dedicated environment for securely running App
Service apps at high scale.
Customers can create multiple ASEs within a single Azure region or across multiple Azure regions. This flexibility makes ASEs ideal for horizontally scaling stateless application tiers in support of high requests per second (RPS) workloads.
Reference:
https://docs.microsoft.com/en-us/azure/app-service/environment/intro

Community vote distribution
C (77%) B (23%)

Question #4 *Topic 6*

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.

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.

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.

App2 -

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

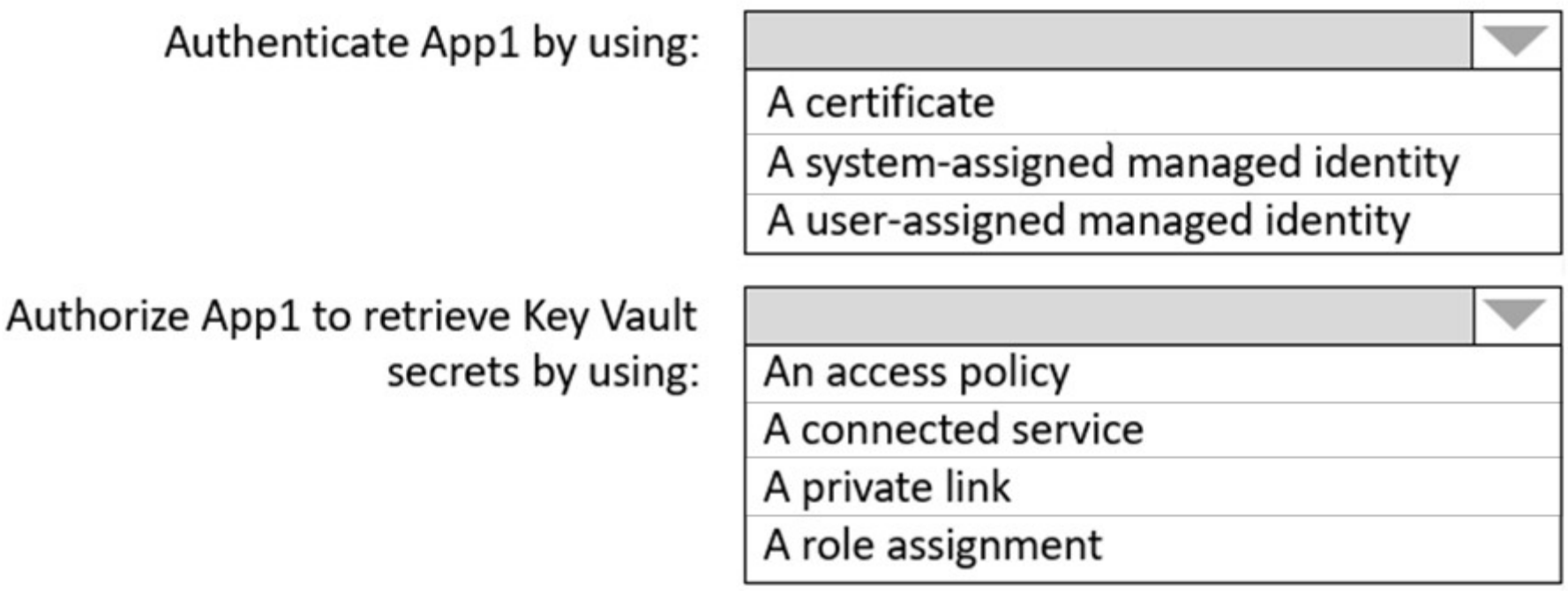
Save files to an Azure Storage account.
Replicate files to an on-premises location.
Ensure that on-premises clients can read the files over the LAN by using the SMB protocol.
You need to monitor App2 to analyze how long it takes to perform different transactions within the application. The solution must 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.

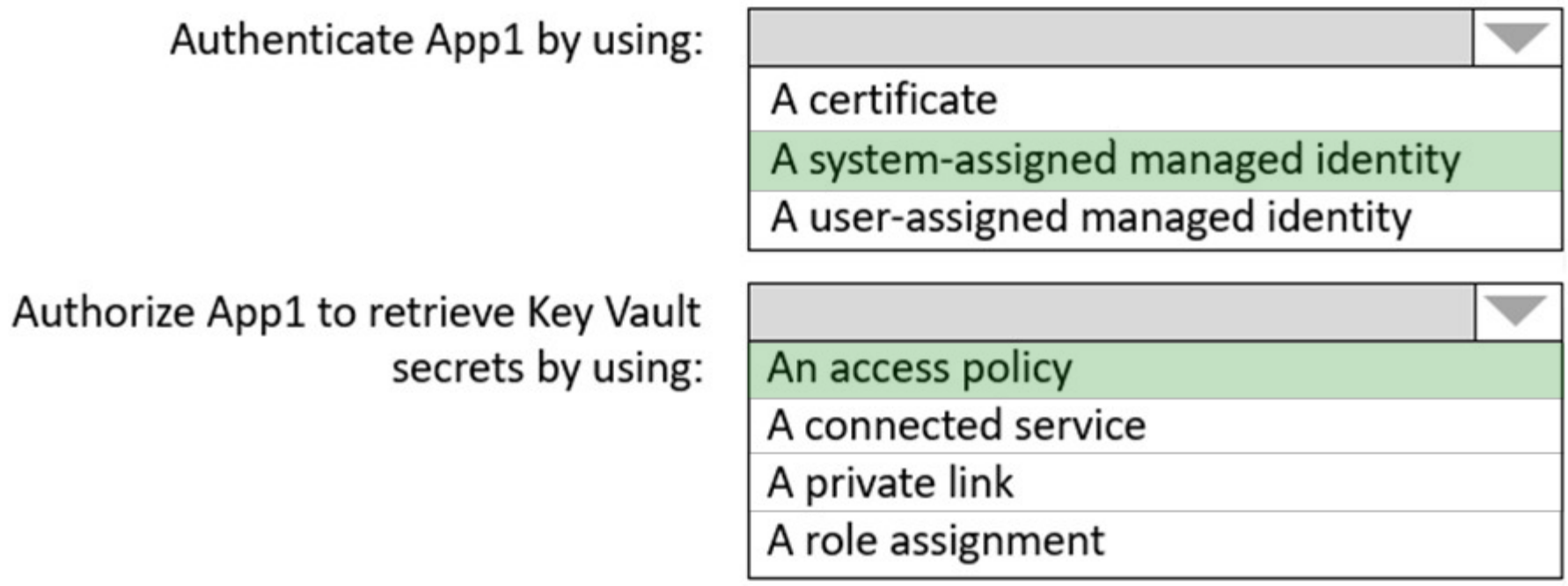
Question
HOTSPOT -
You need to recommend a solution to ensure that App1 can access the third-party credentials and access strings. The solution must meet the security requirements.
What should you include in the recommendation? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Hot Area:

Answer Area



Correct Answer:

Answer Area



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 system-assigned managed identity

No one knows the credentials of managed identities.

Managed Identities exist in two formats:

* System assigned: in this scenario, the identity is linked to a single Azure Resource, eg a Virtual Machine, a Logic App, a Storage Account, Web App, Function,ג€¦ so almost anything. Next, they also ג€liveג€ with the Azure Resource, which means they get deleted when the Azure Resource gets deleted.
* User Assigned Managed Identity (incorrect for this question), which means that you first have to create it as a stand-alone Azure resource by itself, after which it can be linked to multiple Azure Resources.

Box 2: An access policy -

Note: Grant access -

The managed identity needs to be granted access to read the secret that we'll store in the Key Vault.

1. Navigate to your newly created Key Vault
2. Select Access Policy from the menu on the left side.
3. Select Add Access Policy
4. Etc.

Reference:

https://devblogs.microsoft.com/devops/demystifying-service-principals-managed-identities/ https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/tutorial-windows-vm-access-nonaad

Topic 7 - Testlet 11

Question #1 *Topic 7*

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 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.
Hot Area:

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.	○	○

Correct 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.	●	○

Box 1: No -
Online migration will work fine. It does not require an Azure Storage account.

Box 2: No -
Data for the web site can migrated to Azure app service.

Box 3: Yes -
Scenario: Database metrics for the production instance of WebApp1 must be available for analysis so that database administrators can optimize the performance settings.
Reference:
https://azure.microsoft.com/en-au/services/sql-server-stretch-database/

Question #2 *Topic 7*

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

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.

Correct Answer: *A*
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).

Community vote distribution
A (100%)

Topic 8 - Testlet 12

Question #1 *Topic 8*

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

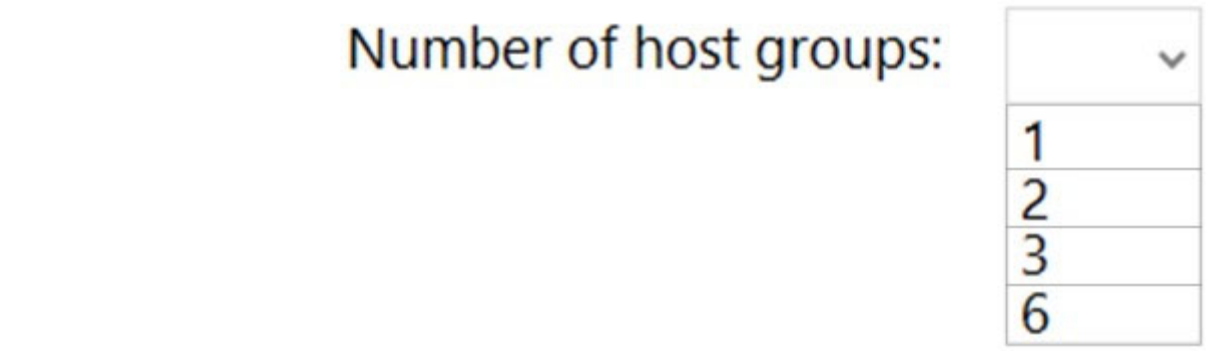
Planned Changes -
Litware plans to implement the following changes:
Migrate DB1 and DB2 to Azure.
Migrate App1 to Azure virtual machines.
Migrate the external storage used by App1 to Azure Storage.
Deploy the Azure virtual machines that will host App1 to Azure dedicated hosts.
▪
Authentication and Authorization 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.

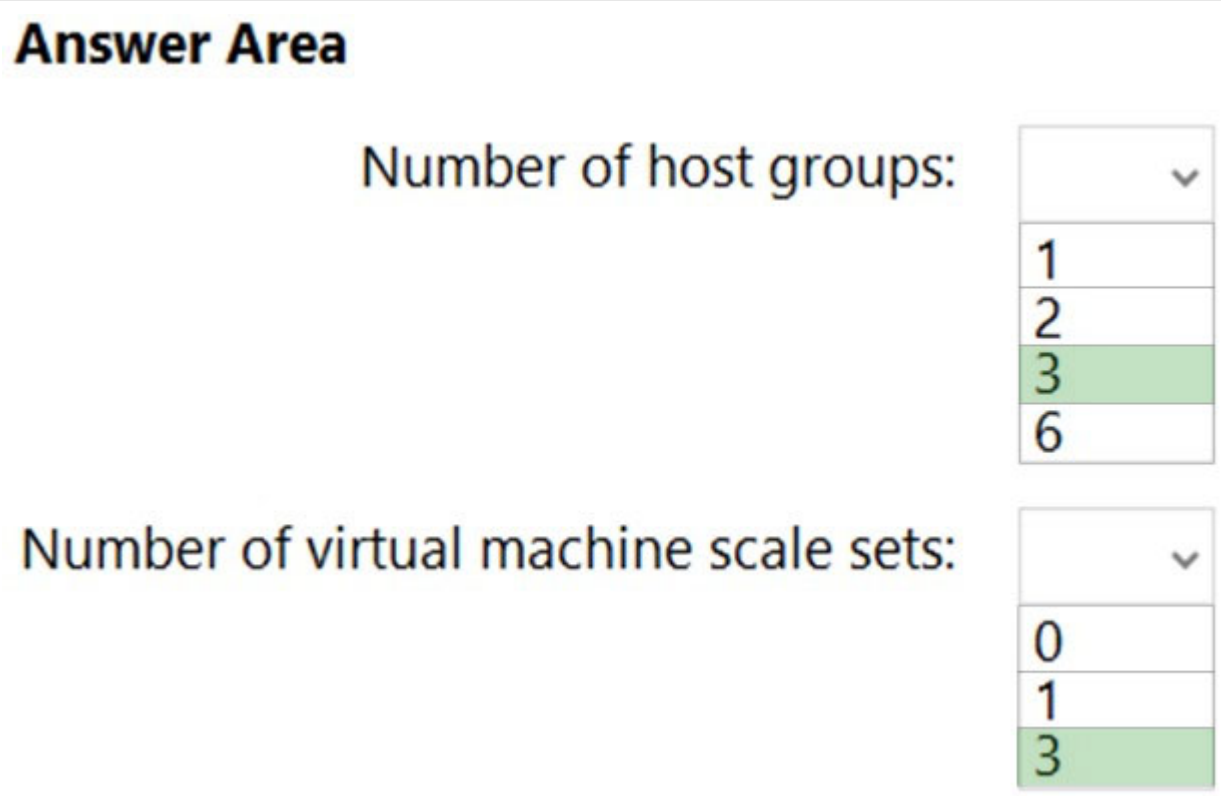
Business Requirements -
Litware identifies the following business requirements:
Minimize administrative effort.
Minimize costs.
▪

Question
HOTSPOT -
You plan to migrate App1 to Azure.
You need to recommend a high-availability solution for App1. The solution must meet the resiliency 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.
Hot Area:

Answer Area



Correct Answer:



Box 1: 3 -

Need three host groups to meet the third scenario requirement below.

Scenario: 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.

Box 2: 3 -

The availability setting of your host group should match your scale set.

* The host group and the scale set must be using the same availability zone.

* The fault domain count for the host group level should match the fault domain count for your scale set.

Reference:

https://docs.microsoft.com/en-us/azure/virtual-machines/dedicated-hosts

Question #2 *Topic 8*

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 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.
Hot Area:

Answer Area

Storage account type:

- Premium page blobs
- Premium file shares
- Standard general-purpose v2

Configuration:

- NFSv3
- Large file shares
- Hierarchical namespace

Answer Area

Storage account type:

- Premium page blobs
- Premium file shares
- Standard general-purpose v2

Correct Answer:

Configuration:

- NFSv3
- Large file shares
- Hierarchical namespace

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: Hierarchical namespace -

Scenario: Plan: Migrate App1 to Azure virtual machines.

Azure Data Lake Storage Gen2 implements an access control model that supports both Azure role-based access control (Azure RBAC) and POSIX-like access control lists (ACLs).

Data Lake Storage Gen2 and the Network File System (NFS) 3.0 protocol both require a storage account with a hierarchical namespace enabled.

Reference:

https://docs.microsoft.com/en-us/azure/storage/blobs/data-protection-overview https://docs.microsoft.com/en-us/azure/storage/blobs/immutable-storage-overview

Question #3 *Topic 8*

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
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

Correct Answer: *D*

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

Community vote distribution

D (100%)

Question #4 *Topic 8*

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
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

Correct Answer: *B*

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.

Community vote distribution

B (91%) 9%

Question #5 *Topic 8*

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 -

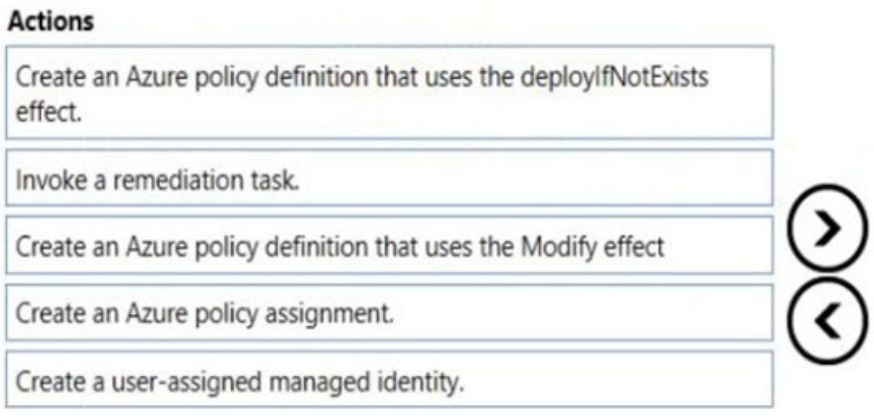
Litware has ExpressRoute connectivity to Azure.
Planned Changes and Requirements

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.

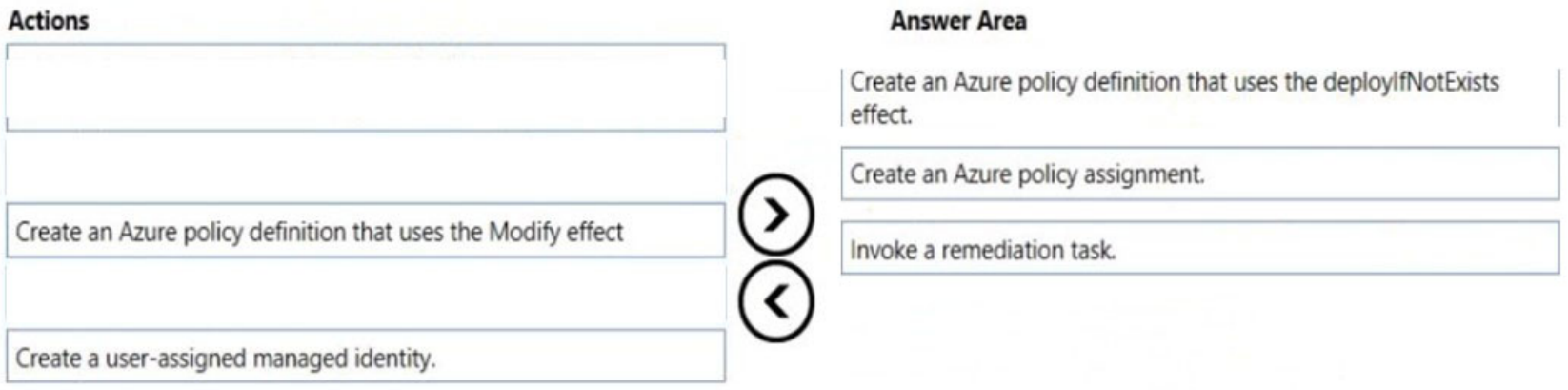
Resiliency Requirements -
Litware identifies the following resiliency requirements:
Once migrated to Azure, DB1 and DB2 must meet the following requirements:
- Maintain availability if two availability zones in the local Azure region fail.
- Fail over automatically.
- Minimize I/O latency.
App1 must 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
DRAG DROP -
You need to configure an Azure policy to ensure that the Azure SQL databases have Transparent Data Encryption (TDE) enabled. The solution must meet the security and compliance requirements.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.
Select and Place:



Correct Answer:



Step 1: Create an Azure policy definition that uses the deployIfNotExists
The first step is to define the roles that deployIfNotExists and modify needs in the policy definition to successfully deploy the content of your included template.
Step 2: Create an Azure policy assignment
When creating an assignment using the portal, Azure Policy both generates the managed identity and grants it the roles defined in roleDefinitionIds.
Step 3: Invoke a remediation task.
Resources that are non-compliant to a deployIfNotExists or modify policy can be put into a compliant state through Remediation. Remediation is accomplished by instructing Azure Policy to run the deployIfNotExists effect or the modify operations of the assigned policy on your existing resources and subscriptions, whether that assignment is to a management group, a subscription, a resource group, or an individual resource. When non- compliant resources or subscriptions are found, the details are provided on the Remediation page.
Reference:
https://docs.microsoft.com/en-us/azure/governance/policy/how-to/remediate-resources

Topic 9 - Testlet 2

Question #1 *Topic 9*

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.

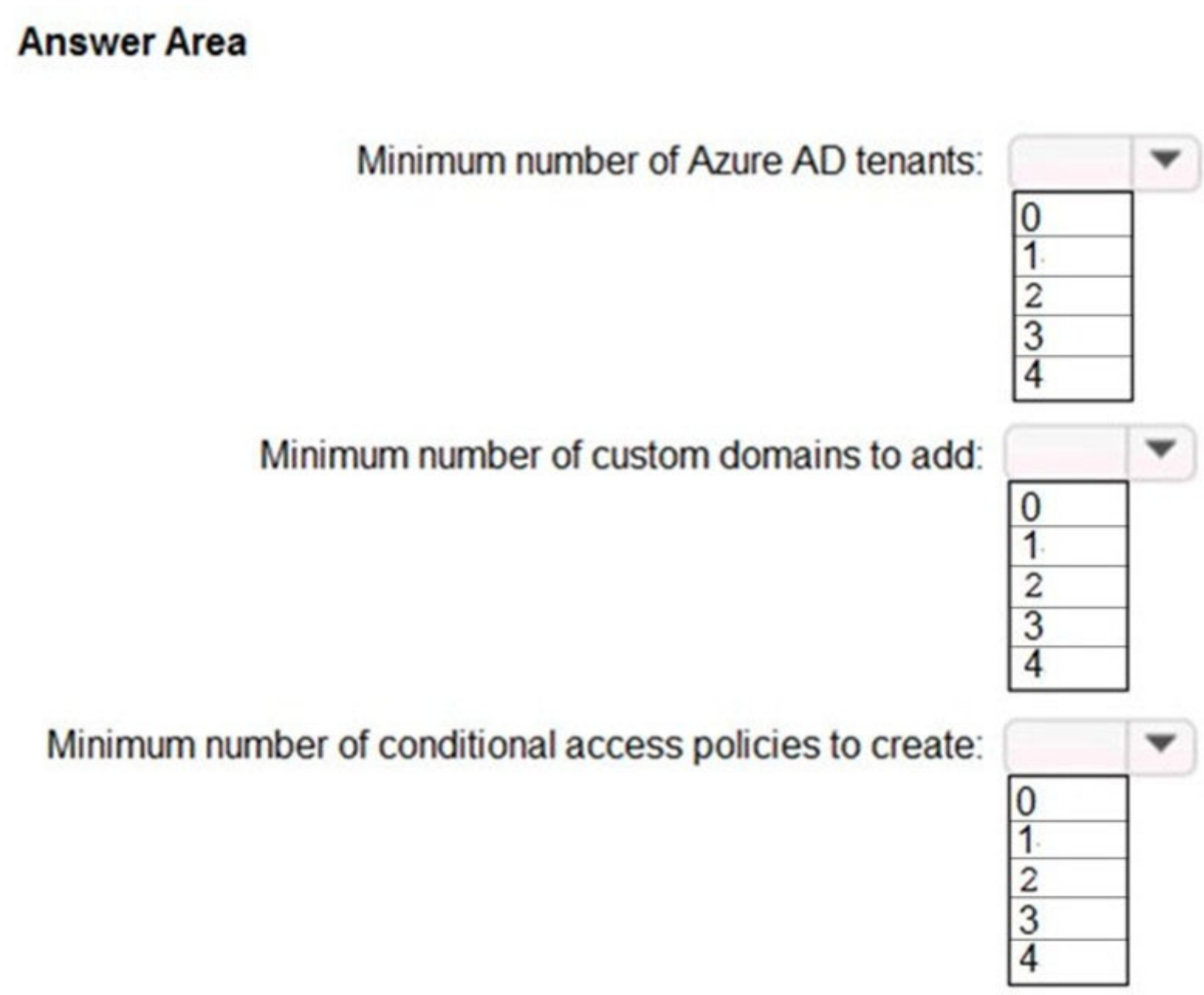
Whenever possible, solutions must be deployed to Azure by using the Standard pricing tier of Azure App Service.

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.

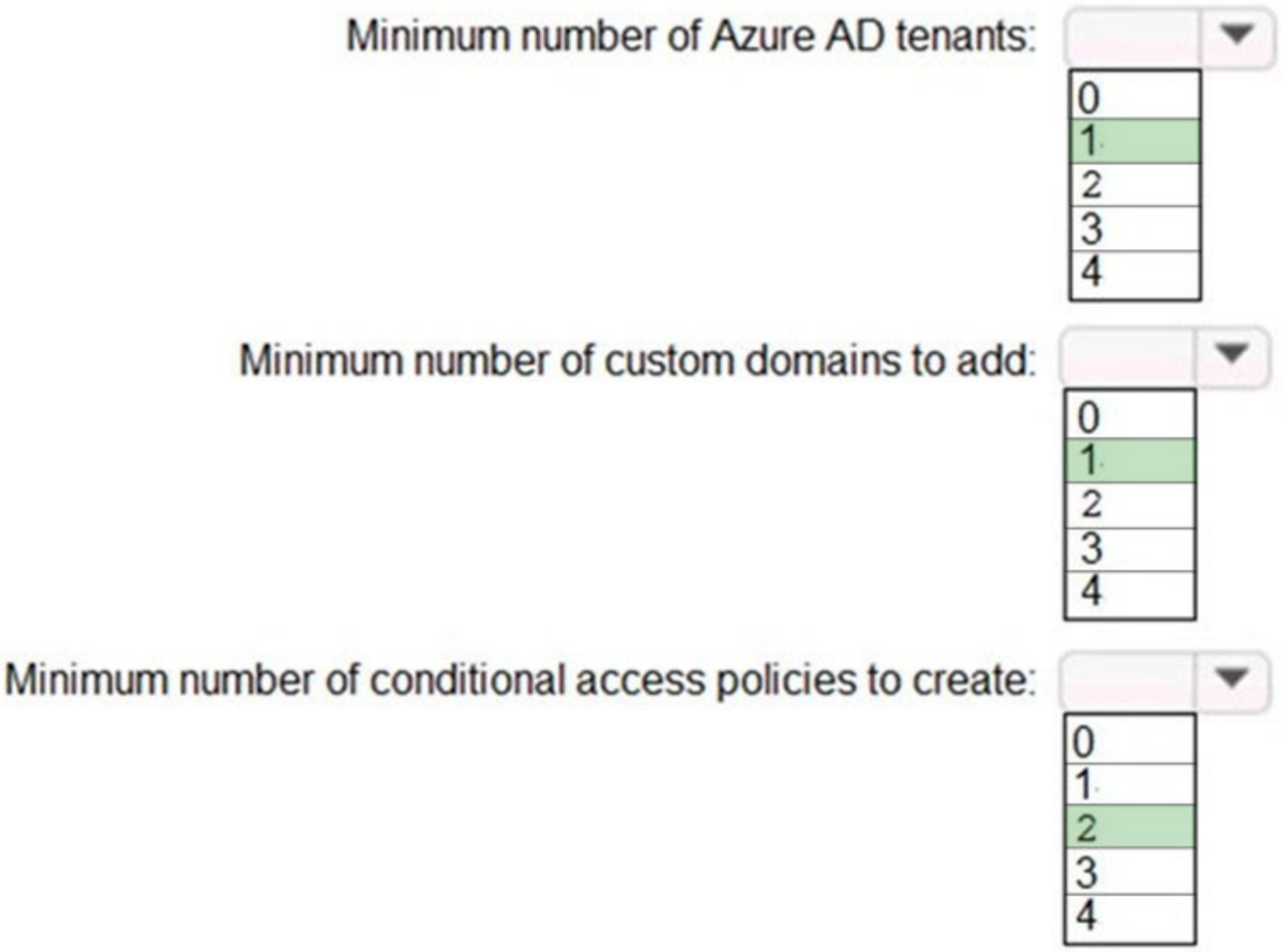
Question

HOTSPOT -
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.
Hot Area:



Correct Answer:

Answer Area



Box 1: 1 -
One single Azure AD tenant is needed as only the Corp tenant is migrated.

Box 2: 1 -

Box 3: 2 -
One conditional access policy for Multi-Factor Authentication (MFA) will be used for administative access, and a second conditional access policy in order to prevent external access.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-location
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-admin-mfa