Expert-Level Case Study Questions - Results

Attempt 1

All domains

24 all   0 correct   0 incorrect   **24 skipped**   0 marked

Question 1   Skipped

Introductory Info

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 in 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 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.
- Failover 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 ensure that users managing the production environment are registered for Azure MFA and must authenticate by using Azure MFA when they sign in to the Azure portal. The solution must meet the authentication and authorization requirements.

What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

To register the users for Azure MFA, use:

Azure AD Identity Protection
Security defaults in Azure AD
Azure AD authentication methods policy

To enforce Azure MFA authentication, configure:

Grant control in capolicy1
Session control in capolicy1
Sign-in risk policy in Azure AD Identity Protection for the Litware.com.tenant

---

Correct selection

To register the users for Azure MFA, use:
Azure AD Identity Protection

To register the users for Azure MFA, use:
Security defaults in Azure AD

To register the users for Azure MFA, use:
Azure AD authentication methods policy

Correct selection

To enforce Azure MFA authentication, configure:

Grant control in capolicy1

To enforce Azure MFA authentication, configure:
Session control in capolicy1

To enforce Azure MFA authentication, configure:
Sign-in risk policy in Azure AD Identity Protection for the Litware.com.tenant

Overall explanation

Answer Area

To register the users for Azure MFA, use:

Azure AD Identity Protection
Security defaults in Azure AD
Azure AD authentication methods policy

To enforce Azure MFA authentication, configure:

Grant control in capolicy1
Session control in capolicy1
Sign-in risk policy in Azure AD Identity Protection for the Litware.com.tenant

Azure AD Identity Protection: 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).

Policy configuration:

- Navigate to the Azure portal.
- Browse to Azure Active Directory > Security > Identity Protection > MFA registration policy.
- Under Assignments
- Users - Choose All users or Select individuals and groups if limiting your rollout.
- Optionally you can choose to exclude users from the policy.
- Enforce Policy - On
- Save

Grant control in capolicy1: 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.

Note: We need to configure the policy conditions for capolicy1 that prompt for MFA.

https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-configure-mfa-policy

https://docs.microsoft.com/en-us/azure/active-directory/authentication/tutorial-enable-azure-mfa

---

Question 2   Skipped

Introductory Info

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 in 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 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.
- Failover 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

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

What should you do?

Correct answer

Create an access policy for the blob service.

Implement Azure resource locks.

Create Azure RBAC assignments.

Modify the access level of the blob service.

Overall explanation

Scenario: Once App1 is migrated to Azure, you must ensure that new data can be written to the app, and the modification of new and existing data is prevented for a period of three years.

As an administrator, you can lock a subscription, resource group, or resource to prevent other users in your organization from accidentally deleting or modifying critical resources. The lock overrides any permissions the user might have.

https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/lock-resources

Question 3   Skipped

Introductory Info

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 in 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 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 efforts.

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?

---

an Azure logic app

Correct answer

an Azure function

---

an Azure virtual machine

---

an App Service WebJob

Overall explanation

Azure Functions can run a PowerShell script from a central location. Azure Functions support PowerShell as a language for writing functions, and you can use the timer trigger to run the function every hour as mentioned in the current web page context. The

function can be hosted in one of the regions where App1 is deployed, either East US or West Europe, and can access all the App1 instances to copy the files.

Question 4   Skipped

Introductory Info

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 in 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 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 efforts.

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?

the Azure App Configuration service

an Azure Container Registry instance

Correct answer

deployment slots

Continuous Integration/Continuous Deployment (CI/CD) sources

Overall explanation

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 configuration 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 the 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.

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.

https://docs.microsoft.com/en-us/azure/app-service/deploy-staging-slots

Question 5   Skipped

Introductory Info

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 in 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 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 efforts.

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?

one App Service Environment (ASE) per availability zone

one App Service Environment (ASE) per region

Correct answer

one App Service plan per region

one App Service plan per availability zone

Overall explanation

An App Service Environment (ASE, option B) is a premium Azure App Service hosting offering that provides fully isolated and dedicated environments for securely running App Service apps at a high scale. While it does meet the requirements for App1, it's a costly option compared to the App Service plan (option C).

On the other hand, an App Service plan (option C) represents a set of compute resources that you allocate to host your apps. You can host multiple apps in the same App Service plan, sharing the resources and thereby reducing costs.

For App1, which is planned to have three instances in each of the two regions, it would be more cost-effective to use a single App Service plan per region. This would allow the

multiple App1 instances in each region to share the resources of the single App Service plan.

Question 6   Skipped

Introductory Info

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 in 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 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 efforts.

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

What should you include in the recommendation? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Authenticate App1 by using:

A Certificate
A system-assigned managed identity
A user-assigned managed identity

Authorize App1 to retrieve Key Vault secrets by using:

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

Authenticate App1 by using:

A Certificate

Authenticate App1 by using:

A system-assigned managed identity

Authenticate App1 by using:

A user-assigned managed identity

Authorize App1 to retrieve Key Vault secrets by using:

An access policy

Authorize App1 to retrieve Key Vault secrets by using:

A connected service

Authorize App1 to retrieve Key Vault secrets by using:

A private link

Authorize App1 to retrieve Key Vault secrets by using:

A role assignment

Overall explanation

Answer Area

Authenticate App1 by using:

A Certificate
A system-assigned managed identity
A user-assigned managed identity

Authorize App1 to retrieve Key Vault secrets by using:

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

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.

An access policy: Set up an access policy for the system-assigned managed identity.

Grant access:

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

- Navigate to your newly created Key Vault
- Select Access Policy from the menu on the left side.
- Select Add Access Policy
- Etc.

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

Question 7   Skipped

Introductory Info

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 in 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 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.

Network Infrastructure

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

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

- An existing application named WebApp1 is hosted in the data center of the London office. WebApp1 is used by customers to place and track orders. WebApp1 has a web tier that uses Microsoft Internet Information Services (IIS)

and a database tier that runs Microsoft SQL Server 2016. The web tier and the database tier are deployed to virtual machines that run on Hyper-V.

- The IT department currently uses a separate Hyper-V environment to test updates to WebApp1.
- Fabrikam purchases all Microsoft licenses through a Microsoft Enterprise Agreement that includes Software Assurance.

Problem 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.

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.

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.

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 to 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 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.

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.	○	○

You must provision an Azure Storage account for the SQL Server database migration.

Yes

You must provision an Azure Storage account for the SQL Server database migration.

No

You must provision an Azure Storage account for the Web site content storage.

Yes

You must provision an Azure Storage account for the Web site content storage.

No

You must provision an Azure Storage account for the Database metric monitoring.

Yes

You must provision an Azure Storage account for the Database metric monitoring.

No

Overall explanation

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.	●	○

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

No - Data for the website can be migrated to the Azure app service.

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

https://azure.microsoft.com/en-au/services/sql-server-stretch-database/

Question 8   Skipped

Introductory Info

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 in 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 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.

Network Infrastructure

- Each office contains at least one domain controller from the corp.fabrikam.com domain. The main office contains all the domain controllers for the rd.fabrikam.com forest.
- All the offices have a high-speed connection to the Internet.
- An existing application named WebApp1 is hosted in the data center of the London office. WebApp1 is used by customers to place and track orders. WebApp1 has a web tier that uses Microsoft Internet Information Services (IIS) and a database tier that runs Microsoft SQL Server 2016. The web tier and the database tier are deployed to virtual machines that run on Hyper-V.
- The IT department currently uses a separate Hyper-V environment to test updates to WebApp1.
- Fabrikam purchases all Microsoft licenses through a Microsoft Enterprise Agreement that includes Software Assurance.

Problem 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.

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.

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.

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 to 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?

Correct answer

Deploy domain controllers for corp.fabrikam.com to virtual networks in Azure.

Move all the domain controllers from corp.fabrikam.com to virtual networks in Azure.

Deploy a new Azure AD tenant for the authentication of new R&D projects.

Deploy domain controllers for the rd.fabrikam.com forest to virtual networks in Azure.

Overall explanation

Directory synchronization between Azure Active Directory (Azure AD) and corp.fabrikam.com must not be affected by a link failure between Azure and the on-premises network. (This requires domain controllers in Azure). Users on the on-premises network must be able to authenticate to corp.fabrikam.com if an Internet link fails. (This requires domain controllers on-premises).

Question 9   Skipped

Introductory Info

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 in 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 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.
- Failover 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 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.

Answer Area

Number of host groups:

	⌄

1
2
3
6

Number of virtual machine scale sets:

	⌄

0
1
3

Number of host groups:

1

Number of host groups:

2

Correct selection

Number of host groups:

3

Number of host groups:

6

Number of virtual machine scale sets:

0

Number of virtual machine scale sets:

1

Overall explanation

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.

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.

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

Question 10   Skipped

Introductory Info

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 in 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 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.
- Failover 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 storage solution for App1 that meets the security and compliance requirements.

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

NOTE: Each correct selection is worth one point.

Answer Area

Storage account type:

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

Configuration:

| NFSv3 |
| Large file shares |
| Hierarchical namespace |

Storage account type:

Premium page blobs

Storage account type:

Premium file shares

Correct selection

Storage account type:

Standard general-purpose v2

Configuration:

NFSv3

Configuration:

Large file shares

Correct selection

Configuration:

Overall explanation

Answer Area

Storage account type:

Premium page blobs
Premium file shares
Standard general-purpose v2

Configuration:

NFSv3
Large file shares
Hierarchical namespace

Standard general-purpose v2 supports Blob Storage. Azure Storage provides data protection for Blob Storage and Azure Data Lake Storage Gen2.

Hierarchical namespace

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.

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 11   Skipped

Introductory Info

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 in 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 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.

- Failover 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?

Microsoft peering for an ExpressRoute circuit

Azure public peering for an ExpressRoute circuit

a service endpoint that has a service endpoint policy

Correct answer

a private endpoint

Overall explanation

Private Endpoint securely connects to storage accounts from on-premises networks that connect to the VNet using VPN or ExpressRoutes with private peering.

Private Endpoint also secures your storage account by configuring the storage firewall to block all connections on the public endpoint for the storage service.

https://docs.microsoft.com/en-us/azure/expressroute/expressroute-circuit-peerings

Question 12   Skipped

Introductory Info

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 in 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 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.
- Failover 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?

1

Correct answer

2

5

10

15

Overall explanation

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

Question 13   Skipped

Introductory Info

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 in 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 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.
- Failover 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 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.

Actions

Create an Azure policy definition that uses the deployIfNotExists effect.

Invoke a remediation task.

Create an Azure policy definition that uses the Modify effect.

Create an Azure policy assignment.

Create a user-assigned managed identity.

Answer Area

Action 1 - Create an Azure policy definition that uses the Modify effect.

Action 2 - Create a user-assigned managed identity.

Action 3 - Invoke a remediation task.

Action 1 - Create an Azure policy assignment.

Action 2 - Create a user-assigned managed identity.

Action 3 - Create an Azure policy definition that uses the Modify effect.

Action 1 - Create an Azure policy assignment.

Action 2 - Create an Azure policy definition that uses the deployIfNotExists effect.

Action 3 - Invoke a remediation task.

Correct answer

Action 1 - Create an Azure policy definition that uses the deployIfNotExists effect.

Action 2 - Create an Azure policy assignment.

Action 3 - Invoke a remediation task.

Overall explanation

<table>
<tr><th colspan="2">Actions</th><th colspan="2">Answer Area</th></tr>
<tr>
<td>Create an Azure policy definition that uses the deployIfNotExists effect.</td>
<td></td>
<td>Create an Azure policy definition that uses the deployIfNotExists effect.</td>
<td></td>
</tr>
<tr>
<td>Invoke a remediation task.</td>
<td></td>
<td>Create an Azure policy assignment.</td>
<td></td>
</tr>
<tr>
<td>Create an Azure policy definition that uses the Modify effect.</td>
<td></td>
<td>Invoke a remediation task.</td>
<td></td>
</tr>
<tr>
<td>Create an Azure policy assignment.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create a user-assigned managed identity.</td>
<td></td>
<td></td>
<td></td>
</tr>
</table>

- **Create an Azure policy definition that uses the deployIfNotExists effect.**

  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.

- **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.

- **Invoke a remediation task.**

  Resources that are non-compliant with 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. During the evaluation, the policy assignment with deployIfNotExists or modify effects determines if there are non-compliant resources or subscriptions. When non-compliant resources or subscriptions are found, the details are provided on the Remediation page.

https://docs.microsoft.com/en-us/azure/governance/policy/how-to/remediate-resources

Question 14 Skipped

Introductory Info

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 in 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 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.

Network Infrastructure

- Each office contains at least one domain controller from the corp.fabrikam.com domain. The main office contains all the domain controllers for the rd.fabrikam.com forest.
- All the offices have a high-speed connection to the Internet.
- An existing application named WebApp1 is hosted in the data center of the London office. WebApp1 is used by customers to place and track orders. WebApp1 has a web tier that uses Microsoft Internet Information Services (IIS) and a database tier that runs Microsoft SQL Server 2016. The web tier and the database tier are deployed to virtual machines that run on Hyper-V.
- The IT department currently uses a separate Hyper-V environment to test updates to WebApp1.
- Fabrikam purchases all Microsoft licenses through a Microsoft Enterprise Agreement that includes Software Assurance.

Problem 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.

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.

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.

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 to 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

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.

Answer Area

Minimum number of Azure AD tenants:

0
1
2
3
4

Minimum number of custom domains to add:

0
1
2
3
4

Minimum number of conditional access policies to create:

0
1
2
3
4

Minimum number of Azure AD tenants:

0

Correct selection

Minimum number of Azure AD tenants:

1

Minimum number of Azure AD tenants:

2

Minimum number of Azure AD tenants:

3

Minimum number of Azure AD tenants:

4

Minimum number of custom domains to add:

0

Correct selection

Minimum number of custom domains to add:

1

Minimum number of custom domains to add:

2

Minimum number of custom domains to add:

3

Minimum number of custom domains to add:

4

Minimum number of conditional access policies to create:

0

Minimum number of conditional access policies to create:

1

Minimum number of conditional access policies to create:

2

Minimum number of conditional access policies to create:

3

Minimum number of conditional access policies to create:

4

Overall explanation

Answer Area

Minimum number of Azure AD tenants:

0
1
2
3
4

Minimum number of custom domains to add:

0
1
2
3
4

Minimum number of conditional access policies to create:

0
1
2
3
4

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

1 - Need to add custom domain due to default .onmicrosoft.com domain on tenant creation.

2 - One conditional access policy for Multi-Factor Authentication (MFA) will be used for administrative access, and a second conditional access policy in order to prevent external access.

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

Question 15   Skipped

Introductory Info

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 in 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 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.

Network Infrastructure

- Each office contains at least one domain controller from the corp.fabrikam.com domain. The main office contains all the domain controllers for the rd.fabrikam.com forest.
- All the offices have a high-speed connection to the Internet.

- An existing application named WebApp1 is hosted in the data center of the London office. WebApp1 is used by customers to place and track orders. WebApp1 has a web tier that uses Microsoft Internet Information Services (IIS) and a database tier that runs Microsoft SQL Server 2016. The web tier and the database tier are deployed to virtual machines that run on Hyper-V.
- The IT department currently uses a separate Hyper-V environment to test updates to WebApp1.
- Fabrikam purchases all Microsoft licenses through a Microsoft Enterprise Agreement that includes Software Assurance.

Problem 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.

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.

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.

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 to 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 notification solution for the IT Support distribution group.

What should you include in the recommendation?

---

a SendGrid account with advanced reporting

---

an action group

Azure Network Watcher

Azure AD Connect Health

Overall explanation

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

Note: You can configure the Azure AD Connect Health service to send email notifications when alerts indicate that your identity infrastructure is not healthy. his occurs when an alert is generated, and when it is resolved.

https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-health-operations

Question 16   Skipped

Introductory Info

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 in 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 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.

Network Infrastructure

- Each office contains at least one domain controller from the corp.fabrikam.com domain. The main office contains all the domain controllers for the rd.fabrikam.com forest.
- All the offices have a high-speed connection to the Internet.
- An existing application named WebApp1 is hosted in the data center of the London office. WebApp1 is used by customers to place and track orders. WebApp1 has a web tier that uses Microsoft Internet Information Services (IIS) and a database tier that runs Microsoft SQL Server 2016. The web tier and the database tier are deployed to virtual machines that run on Hyper-V.
- The IT department currently uses a separate Hyper-V environment to test updates to WebApp1.
- Fabrikam purchases all Microsoft licenses through a Microsoft Enterprise Agreement that includes Software Assurance.

Problem 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.

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.

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.

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 to 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 solution to meet the database retention requirements.

What should you recommend?

Correct answer

Configure a long-term retention policy for the database.

Configure Azure Site Recovery.

Use automatic Azure SQL Database backups.

Configure geo-replication of the database.

Overall explanation

Scenario: Database backups must be retained for a minimum of seven years to meet compliance requirements.

Many applications have regulatory, compliance, or other business purposes that require you to retain database backups beyond the 7-35 days provided by Azure SQL Database and Azure SQL Managed Instance automatic backups. By using the long-term retention (LTR) feature, you can store specified SQL Database and SQL Managed Instance full backups in Azure Blob storage with configured redundancy for up to 10 years. LTR backups can then be restored as a new database.

Question 17   Skipped

Introductory Info

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 in 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 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 efforts.

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

NOTE: Each correct selection is worth one point.

Answer Area

Service:

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

Feature:

Access packages
Access reviews
Approvals
Runbooks

Service:

Azure AD Identity Governance

Service:

Azure AD Identity Protection

Service:

Azure AD Privilege Access Management (PIM)

Service:

Azure Automation

Feature:

Access packages

Feature:

Access reviews

Feature:

Approvals

Feature:

Runbooks

Overall explanation

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

Azure AD Identity Governance service allows organizations to manage, control, and monitor access to resources, which is necessary for the management of Fabrikam users' access to resources.

Access reviews is a feature of Azure AD Identity Governance that allows for periodic review of access permissions, fulfilling the requirement for the monthly review of Fabrikam users' access permissions to App1.

https://docs.microsoft.com/en-us/azure/active-directory/governance/access-reviews-overview

---

Question 18   Skipped

Introductory Info

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 in 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 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 efforts.

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?

VM insights

Correct answer

Azure Application Insights

Microsoft Sentinel

Container insights

Overall explanation

Azure Application Insights is an extensible Application Performance Management (APM) service for web developers. It provides real-time, detailed insights into application performance and failures, making it a suitable choice for analyzing the performance of different transactions within App2, as required. Plus, it doesn't require changes to the application code. Other options are either not relevant or not specifically geared toward application performance monitoring.

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

Question 19   Skipped

Introductory Info

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 in 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 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.

Network Infrastructure

- Each office contains at least one domain controller from the corp.fabrikam.com domain. The main office contains all the domain controllers for the rd.fabrikam.com forest.
- All the offices have a high-speed connection to the Internet.
- An existing application named WebApp1 is hosted in the data center of the London office. WebApp1 is used by customers to place and track orders. WebApp1 has a web tier that uses Microsoft Internet Information Services (IIS) and a database tier that runs Microsoft SQL Server 2016. The web tier and the database tier are deployed to virtual machines that run on Hyper-V.
- The IT department currently uses a separate Hyper-V environment to test updates to WebApp1.
- Fabrikam purchases all Microsoft licenses through a Microsoft Enterprise Agreement that includes Software Assurance.

Problem 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.

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.

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.

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 to 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?

an Azure virtual machine that runs SQL Server

a fixed-size DTU Azure SQL database

an Azure SQL Database elastic pool

Correct answer

a vCore-based Azure SQL database

Overall explanation

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.

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

---

Question 20   Skipped

Introductory Info

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 in 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 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.
- Failover 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 DB1 and DB2 to Azure.

You need to ensure that the Azure database and the service tier meet the resiliency and business requirements.

What should you configure? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Database:

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

Service tier:

| Hyperscale |
| Business Critical |
| General Purpose |

Database:

A single Azure SQL database

Database:

Azure SQL Managed Instance

Service tier:

Hyperscale

Service tier:

General Purpose

Overall explanation

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

An Azure SQL Database Elastic Pool is a shared resource model that enables higher resource utilization efficiency. It allows multiple databases to share the same resources,

which will be beneficial in this case where there are two databases, DB1 and DB2, to be migrated.

Business Critical service tier provides high availability and low latency, and it is fully managed, which aligns with the business requirement to minimize administrative effort and the technical requirement to maintain availability if two availability zones fail. As you pointed out, the zone redundancy is still in preview for Managed Instances which can't guarantee the desired level of stability and reliability.

Question 21   Skipped

Introductory Info

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 in 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 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 efforts.

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 file storage requirements for App2.

What should you deploy to the Azure subscription and the on-premises network? To answer, drag the appropriate services to the correct locations. Each service may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Services

Azure Blob Storage
Azure Data Box
Azure Data Box Gateway
Azure Data Lake Storage
Azure File Sync
Azure Files

Answer Area

Azure subscription:

On-premises network:

Azure subscription:

Azure Blob Storage

Azure subscription:

Azure Data Box

Azure subscription:

Azure Data Box Gateway

Azure subscription:

Azure Data Lake Storage

Azure subscription:

Azure File Sync

Correct selection

Azure subscription:

Azure Files

On-premises network:

Azure Blob Storage

On-premises network:

Azure Data Box

On-premises network:

Azure Data Box Gateway

On-premises network:

Azure Data Lake Storage

Correct selection

On-premises network:

Azure File Sync

On-premises network:

Azure Files

Overall explanation

Services	Answer Area	
Azure Blob Storage	Azure subscription:	Azure Files
Azure Data Box	On-premises network:	Azure File Sync
Azure Data Box Gateway		
Azure Data Lake Storage		
Azure File Sync		
Azure Files		

Azure Files

Scenario: App2 has the following file storage requirements:

- Save files to an Azure Storage account.

- Replicate files to an on-premises location.

- Ensure that on-premises clients can read the files over the LAN by using the SMB protocol.

Azure File Sync

Use Azure File Sync to centralize your organization's file shares in Azure Files, while keeping the flexibility, performance, and compatibility of an on-premises file server. Azure File Sync transforms Windows Server into a quick cache of your Azure file share. You can use any protocol that's available on Windows Server to access your data locally, including SMB, NFS, and FTPS. You can have as many caches as you need across the world.

https://docs.microsoft.com/en-us/azure/storage/file-sync/file-sync-deployment-guide

---

Question 22   Skipped

Introductory Info

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 in 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 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 efforts.

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 data requirements for App1.

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

Correct answer

an Azure Cosmos DB that uses multi-region writes

an Azure Data Lake store that uses geo-zone-redundant storage (GZRS)

an Azure Storage account that uses geo-zone-redundant storage (GZRS)

Overall explanation

App1 has the following data requirements:

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

Azure Cosmos DB: Each partition across all the regions is replicated. Each region contains all the data partitions of an Azure Cosmos container and can serve reads as well as serve writes when multi-region writes are enabled.

https://docs.microsoft.com/en-us/azure/cosmos-db/high-availability

Question 23   Skipped

Introductory Info

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 in 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 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 efforts.

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 are evaluating whether to use Azure Traffic Manager and Azure Application Gateway to meet the connection requirements for App1.

What is the minimum number of instances required for each service? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Azure Traffic Manager:

1
2
3
6

Azure Application Gateway:

1
2
3
6

Correct selection

Azure Traffic Manager:

1

Azure Traffic Manager:

2

Azure Traffic Manager:

3

Azure Traffic Manager:

6

Azure Application Gateway:

1

Correct selection

Azure Application Gateway:

2

Azure Application Gateway:

3

Azure Application Gateway:

6

Overall explanation

Answer Area

Azure Traffic Manager: [▾]

1
2
3
6

Azure Application Gateway: [▾]

1
2
3
6

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

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

Note: Azure Traffic Manager is a DNS-based traffic load balancer. This service allows you to distribute traffic to your public-facing applications across the global Azure regions.

2 - For production workloads, run at least two gateway instances.

A single Application Gateway deployment can run multiple instances of the gateway.

Use one Application Gateway in East US Region, and one in the West Europe region.

https://docs.microsoft.com/en-us/azure/architecture/high-availability/reference-architecture-traffic-manager-application-gateway

Question 24   Skipped

Introductory Info

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 in 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 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.

Network Infrastructure

- Each office contains at least one domain controller from the corp.fabrikam.com domain. The main office contains all the domain controllers for the rd.fabrikam.com forest.
- All the offices have a high-speed connection to the Internet.
- An existing application named WebApp1 is hosted in the data center of the London office. WebApp1 is used by customers to place and track orders. WebApp1 has a web tier that uses Microsoft Internet Information Services (IIS) and a database tier that runs Microsoft SQL Server 2016. The web tier and the database tier are deployed to virtual machines that run on Hyper-V.
- The IT department currently uses a separate Hyper-V environment to test updates to WebApp1.

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

Problem 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.

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.

Database Requirements

Fabrikam identifies the following 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.

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 to 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 design a solution for the web tier of WebApp1 as shown in the exhibit.
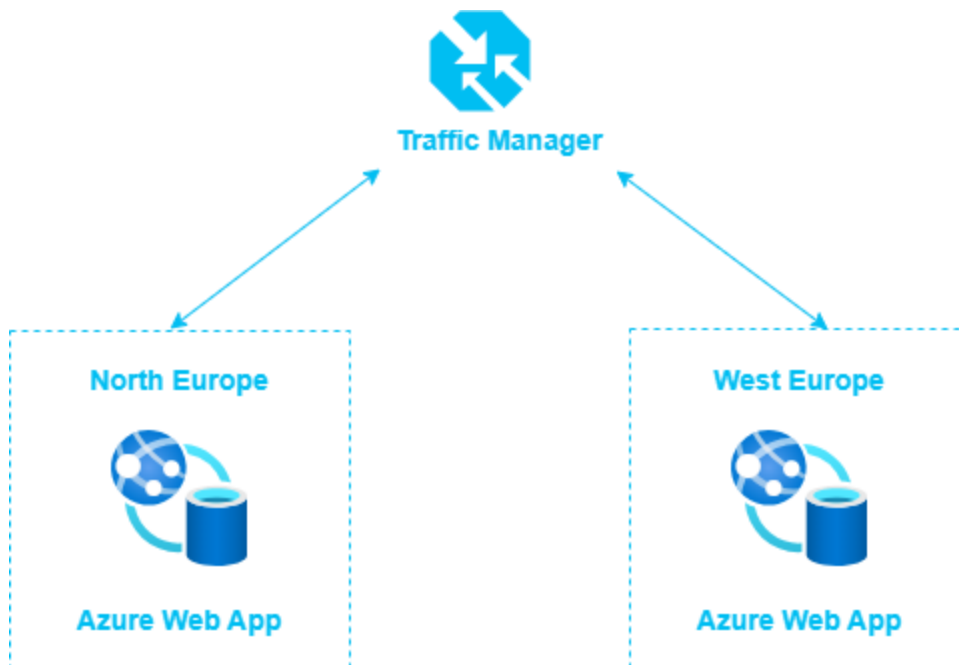
For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Statements

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

Correct selection

The design supports the technical requirements for redundancy.
Yes

The design supports the technical requirements for redundancy.
No

Correct selection

The design supports autoscaling.
Yes

The design supports autoscaling.
No

The design requires a manual configuration if an Azure region fails.
Yes

Correct selection

The design requires a manual configuration if an Azure region fails.
No

Overall explanation

Statements

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

Yes - The traffic manager distributes the load to two sites (redundancy).

Yes - The graphic clearly shows an "Azure Web App", which is production. By default, production web apps support auto-scale.

No - Azure Traffic Manager does automatic failover, so no manual configuration is necessary.