AZ-304.prepaway.premium.exam.102q

Number: AZ-304
Passing Score: 800
Time Limit: 120 min
File Version: 2.0

AZ-304

Microsoft Azure Architect Design

Version 2.0

Design Monitoring

Question Set 1

QUESTION 1
You need to recommend a solution to generate a monthly report of all the new Azure Resource Manager resource deployments in your subscription.

What should you include in the recommendation?

A. the Change Tracking management solution
B. Application Insights
C. Azure Monitor action groups
D. Azure Activity Log

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Activity logs are kept for 90 days. You can query for any range of dates, as long as the starting date isn't more than 90 days in the past.

Through activity logs, you can determine:

- what operations were taken on the resources in your subscription
- who started the operation
- when the operation occurred
- the status of the operation
- the values of other properties that might help you research the operation

Reference:
https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/view-activity-logs

QUESTION 2
You have an Azure subscription that contains an Azure SQL database named DB1.

Several queries that query the data in DB1 take a long time to execute.

You need to recommend a solution to identify the queries that take the longest to execute.

What should you include in the recommendation?

A. SQL Database Advisor
B. Azure Monitor
C. Performance Recommendations
D. Query Performance Insight

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Query Performance Insight provides intelligent query analysis for single and pooled databases. It helps identify the top resource consuming and long-running queries in your workload. This helps you find the queries to

optimize to improve overall workload performance and efficiently use the resource that you are paying for.

Reference:
https://docs.microsoft.com/en-us/azure/azure-sql/database/query-performance-insight-use

QUESTION 3
HOTSPOT

You have an Azure App Service Web App that includes Azure Blob storage and an Azure SQL Database instance. The application is instrumented by using the Application Insights SDK.

You need to design a monitoring solution for the web app.

Which Azure monitoring services should you use? To answer, select the appropriate Azure monitoring services in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Scenario	Azure monitoring service
Correlate Azure resource usage and performance data with application configuration and performance data.	Azure Application Insights / Azure Service Map / Azure Monitor Logs / Azure Activity Log
Visualize the relationships between application components.	Azure Application Insights / Azure Service Map / Azure Monitor Logs / Azure Activity Log
Track requests and exceptions to a specific line of code within the application.	Azure Application Insights / Azure Service Map / Azure Monitor Logs / Azure Activity Log
Analyze how many users return to the application and how often they select a particular dropdown value.	Azure Application Insights / Azure Service Map / Azure Monitor Logs / Azure Activity Log

Correct Answer:

Answer Area

Scenario	Azure monitoring service
Correlate Azure resource usage and performance data with application configuration and performance data.	Azure Application Insights Azure Service Map **Azure Monitor Logs** Azure Activity Log
Visualize the relationships between application components.	Azure Application Insights **Azure Service Map** Azure Monitor Logs Azure Activity Log
Track requests and exceptions to a specific line of code within the application.	**Azure Application Insights** Azure Service Map Azure Monitor Logs Azure Activity Log
Analyze how many users return to the application and how often they select a particular dropdown value.	Azure Application Insights Azure Service Map Azure Monitor Logs **Azure Activity Log**

Section: (none)
Explanation

Explanation/Reference:
Explanation:

Note: You can select Logs from either the Azure Monitor menu or the Log Analytics workspaces menu.

Reference:
https://docs.microsoft.com/en-us/azure/azure-monitor/log-query/log-query-overview

QUESTION 4
You have an on-premises Hyper-V cluster. The cluster contains Hyper-V hosts that run Windows Server 2016 Datacenter. The hosts are licensed under a Microsoft Enterprise Agreement that has Software Assurance.

The Hyper-V cluster contains 30 virtual machines that run Windows Server 2012 R2. Each virtual machine

runs a different workload. The workloads have predictable consumption patterns.

You plan to replace the virtual machines with Azure virtual machines that run Windows Server 2016. The virtual machines will be sized according to the consumption pattern of each workload.

You need to recommend a solution to minimize the compute costs of the Azure virtual machines.

Which two recommendations should you include in the solution? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Configure a spending limit in the Azure account center.
B. Create a virtual machine scale set that uses autoscaling.
C. Activate Azure Hybrid Benefit for the Azure virtual machines.
D. Purchase Azure Reserved Virtual Machine Instances for the Azure virtual machines.
E. Create a lab in Azure DevTest Labs and place the Azure virtual machines in the lab.

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
C: For customers with Software Assurance, Azure Hybrid Benefit for Windows Server allows you to use your on-premises Windows Server licenses and run Windows virtual machines on Azure at a reduced cost. You can use Azure Hybrid Benefit for Windows Server to deploy new virtual machines with Windows OS.

D: With Azure Reserved VM Instances (RIs) you reserve virtual machines in advance and save up to 80 percent.

Reference:
https://azure.microsoft.com/en-us/pricing/reserved-vm-instances/

https://docs.microsoft.com/en-us/azure/virtual-machines/windows/hybrid-use-benefit-licensing

QUESTION 5
HOTSPOT

You have an Azure subscription that contains the SQL servers on Azure shown in the following table.

Name	Resource group	Location
SQLsvr1	RG1	East US
SQLsvr2	RG2	West US

The subscription contains the storage accounts shown in the following table.

Name	Resource group	Location	Account kind
storage1	RG1	East US	StorageV2 (general purpose v2)
storage2	RG2	West US	BlobStorage

You create the Azure SQL databases shown in the following table.

Name	Resource group	Server	Pricing tier
SQLdb1	RG1	SQLsvr1	Standard
SQLdb2	RG1	SQLsvr1	Standard
SQLdb3	RG2	SQLsvr2	Premium

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
When you enable auditing for SQLdb1, you can store the audit information to storage1.	○	○
When you enable auditing for SQLdb2, you can store the audit information to storage2.	○	○
When you enable auditing for SQLdb3, you can store the audit information to storage2.	○	○

Correct Answer:

Answer Area

Statements	Yes	No
When you enable auditing for SQLdb1, you can store the audit information to storage1.	○	○
When you enable auditing for SQLdb2, you can store the audit information to storage2.	○	○
When you enable auditing for SQLdb3, you can store the audit information to storage2.	○	○

Section: (none)
Explanation

Explanation/Reference:
Explanation:

Box 1: Yes
Be sure that the destination is in the same region as your database and server.

Box 2: No

Box 3: No

Reference:
https://docs.microsoft.com/en-us/azure/sql-database/sql-database-auditing

QUESTION 6
A company has a hybrid ASP.NET Web API application that is based on a software as a service (SaaS) offering.

Users report general issues with the data. You advise the company to implement live monitoring and use ad hoc queries on stored JSON data. You also advise the company to set up smart alerting to detect anomalies in the data.

You need to recommend a solution to set up smart alerting.

What should you recommend?

A. Azure Site Recovery and Azure Monitor Logs
B. Azure Data Lake Analytics and Azure Monitor Logs
C. Azure Application Insights and Azure Monitor Logs
D. Azure Security Center and Azure Data Lake Store

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Application Insights, a feature of Azure Monitor, is an extensible Application Performance Management (APM) service for developers and DevOps professionals. Use it to monitor your live applications. It will automatically detect performance anomalies, and includes powerful analytics tools to help you diagnose issues and to understand what users actually do with your app.

Reference:
https://docs.microsoft.com/en-us/azure/azure-monitor/app/app-insights-overview

QUESTION 7
You have an Azure subscription that is linked to an Azure Active Directory (Azure AD) tenant. The subscription contains 10 resource groups, one for each department at your company.

Each department has a specific spending limit for its Azure resources.

You need to ensure that when a department reaches its spending limit, the compute resources of the department shut down automatically.

Which two features should you include in the solution? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Azure Logic Apps
B. Azure Monitor alerts
C. the spending limit of an Azure account
D. Cost Management budgets
E. Azure Log Analytics alerts

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
C: The spending limit in Azure prevents spending over your credit amount. All new customers who sign up for an Azure free account or subscription types that include credits over multiple months have the spending limit turned on by default. The spending limit is equal to the amount of credit and it can't be changed.

D: Turn on the spending limit after removing
This feature is available only when the spending limit has been removed indefinitely for subscription types that include credits over multiple months. You can use this feature to turn on your spending limit automatically at the start of the next billing period.

1. Sign in to the Azure portal as the Account Administrator.
2. Search for Cost Management + Billing.
3. Etc.

Reference:
https://docs.microsoft.com/en-us/azure/cost-management-billing/manage/spending-limit

QUESTION 8
HOTSPOT

You have an Azure subscription that contains the resources shown in the following table.

Name	Type	Kind	Location
storage1	Azure Storage account	Storage	East US
storage2	Azure Storage account	StorageV2	East US
Workspace1	Azure Log Analytics workspace	*Not applicable*	East US
Workspace2	Azure Log Analytics workspace	*Not applicable*	East US
Hub1	Azure event hub	*Not applicable*	East US

You create an Azure SQL database named DB1 that is hosted in the East US region.

To DB1, you add a diagnostic setting named Settings1. Settings1 archives SQLInsights to storage1 and sends SQLInsights to Workspace1.

For each of the following statements, select Yes if the statement is true, Otherwise, select No.

Hot Area:

Answer Area

Statements	Yes	No
You can add a new diagnostic setting that archives SQLInsights logs to storage2.	○	○
You can add a new diagnostic setting that sends SQLInsights logs to Workspace2.	○	○
You can add a new diagnostic setting that sends SQLInsights logs to Hub1.	○	○

Correct Answer:

Answer Area

Statements	Yes	No
You can add a new diagnostic setting that archives SQLInsights logs to storage2.	○	○
You can add a new diagnostic setting that sends SQLInsights logs to Workspace2.	○	○
You can add a new diagnostic setting that sends SQLInsights logs to Hub1.	○	○

Section: (none)
Explanation

Explanation/Reference:
Explanation:

Box 1: No
You archive logs only to Azure Storage accounts.

Box 2: Yes

Box 3: Yes
Sending logs to Event Hubs allows you to stream data to external systems such as third-party SIEMs and other log analytics solutions.

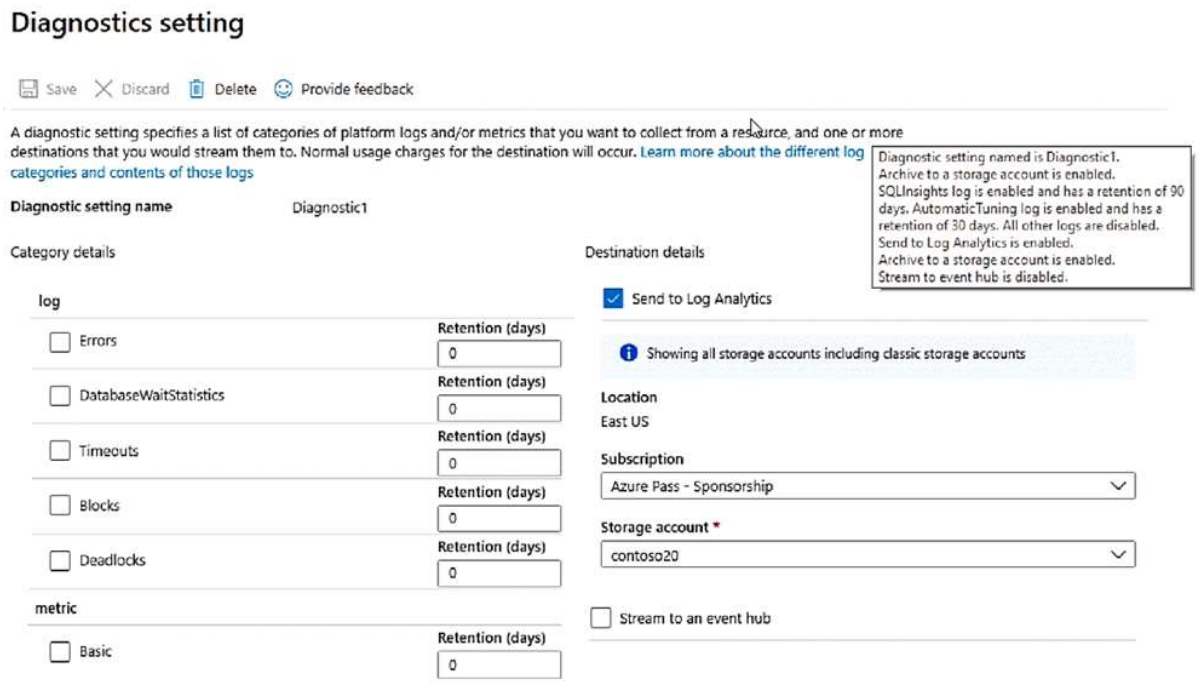
Note: A single diagnostic setting can define no more than one of each of the destinations. If you want to send data to more than one of a particular destination type (for example, two different Log Analytics workspaces), then create multiple settings. Each resource can have up to 5 diagnostic settings.

Reference:
https://docs.microsoft.com/en-us/azure/azure-monitor/platform/diagnostic-settings

QUESTION 9
HOTSPOT

You deploy several Azure SQL Database instances.

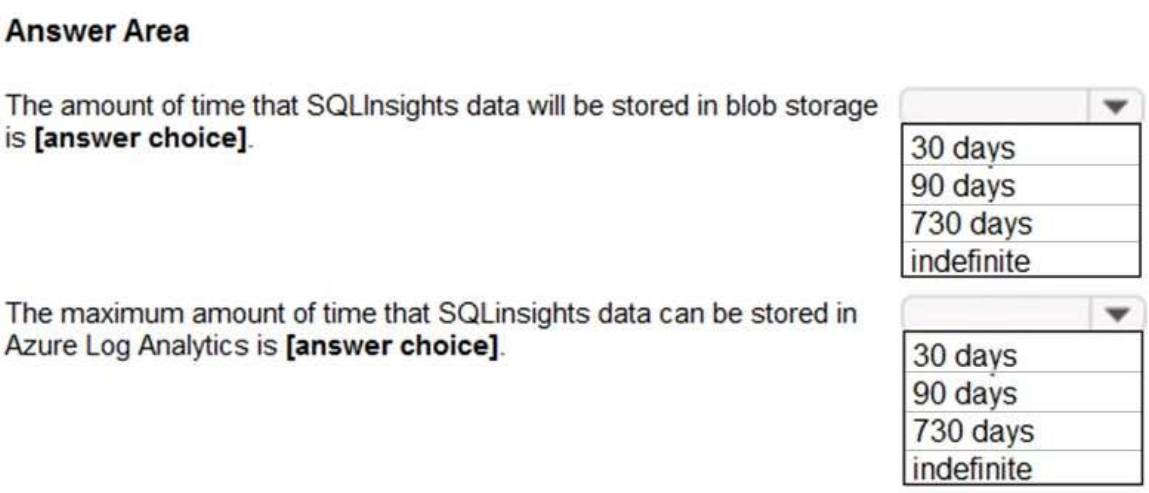
You plan to configure the Diagnostics settings on the databases as shown in the following exhibit.



Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:

Answer Area

The amount of time that SQLInsights data will be stored in blob storage is **[answer choice]**.

- 30 days
- 90 days
- 730 days
- indefinite

The maximum amount of time that SQLinsights data can be stored in Azure Log Analytics is **[answer choice]**.

- 30 days
- 90 days
- 730 days
- indefinite

Section: (none)
Explanation

Explanation/Reference:
Explanation:

In the exhibit, the SQLInsights data is configured to be stored in Azure Log Analytics for 90 days. However, the question is asking for the “maximum” amount of time that the data can be stored which is 730 days.

Design Identity and Security

Testlet 1

Case Study

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

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

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

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

Overview

Fabricam, 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.

Existing Environment. Network Infrastructure

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

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

An existing application named WebApp1 is hosted in the data center of the London office. WebApp1 is used by customers to place and track orders. WebApp1 has a web tier that uses Microsoft Internet Information Services (IIS) and a database tier that runs Microsoft SQL Server 2016. The web tier and the database tier are deployed to virtual machines that run on Hyper-V.

The IT department currently uses a separate Hyper-V environment to test updates to WebApp1.

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

Existing Environment. Problem Statements

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

Requirements. Planned Changes

Fabrikam plans to move most of its production workloads to Azure during the next few years.

As one of its first projects, the company plans to establish a hybrid identity model, facilitating an upcoming Microsoft Office 365 deployment.

All R&D operations will remain on-premises.

Fabrikam plans to migrate the production and test instances of WebApp1 to Azure and to use the S1 plan.

Requirements. Technical Requirements

Fabrikam identifies the following technical requirements:

- Web site content must be easily updated from a single point.
- User input must be minimized when provisioning new 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.
- Directory synchronization between Azure Active Directory (Azure AD) and corp.fabrikam.com must not be affected by a link failure between Azure and the on-premises network.

Requirements. Database Requirements

Fabrikam identifies the following database requirements:

- Database metrics for the production instance of WebApp1 must be available for analysis so that database administrators can optimize the performance settings.
- To avoid disrupting customer access, database downtime must be minimized when databases are migrated.
- Database backups must be retained for a minimum of seven years to meet compliance requirements.

Requirements. Security Requirements

Fabrikam identifies the following security requirements:

- Company information including policies, templates, and data must be inaccessible to anyone outside the company.
- Users on the on-premises network must be able to authenticate to corp.fabrikam.com if an Internet link fails.
- Administrators must be able authenticate to the Azure portal by using their corp.fabrikam.com credentials.
- All administrative access to the Azure portal must be secured by using multi-factor authentication.
- The testing of WebApp1 updates must not be visible to anyone outside the company.

QUESTION 1
What should you include in the identity management strategy to support the planned changes?

A. Move all the domain controllers from corp.fabrikam.com to virtual networks in Azure.
B. Deploy domain controllers for the rd.fabrikam.com forest to virtual networks in Azure.

C. Deploy domain controllers for corp.fabrikam.com to virtual networks in Azure.
D. Deploy a new Azure AD tenant for the authentication of new R&D projects.

Correct Answer: C
Section: (none)
Explanation

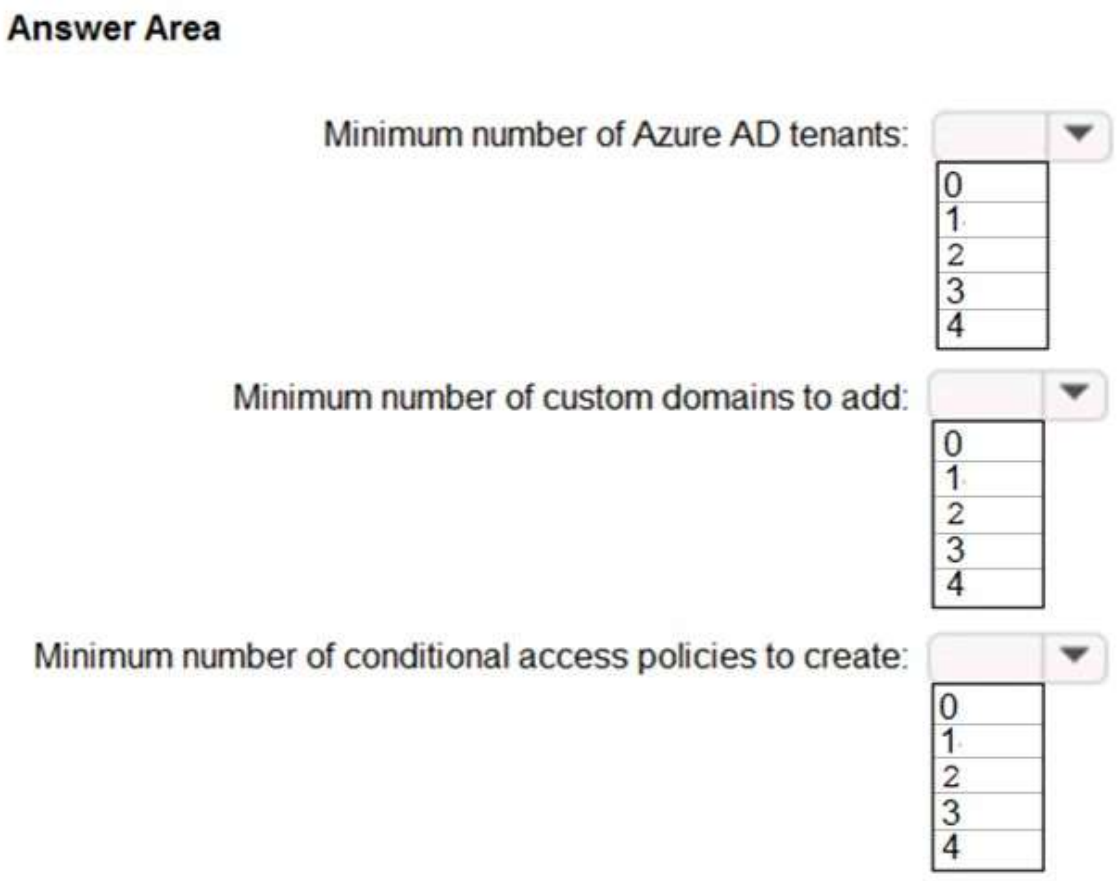
Explanation/Reference:
Explanation:
Directory synchronization between Azure Active Directory (Azure AD) and corp.fabrikam.com must not be affected by a link failure between Azure and the on-premises network. (This requires domain controllers in Azure)
Users on the on-premises network must be able to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

QUESTION 2
HOTSPOT

To meet the authentication requirements of Fabrikam, what should you include in the solution? To answer, select the appropriate options in the answer area.

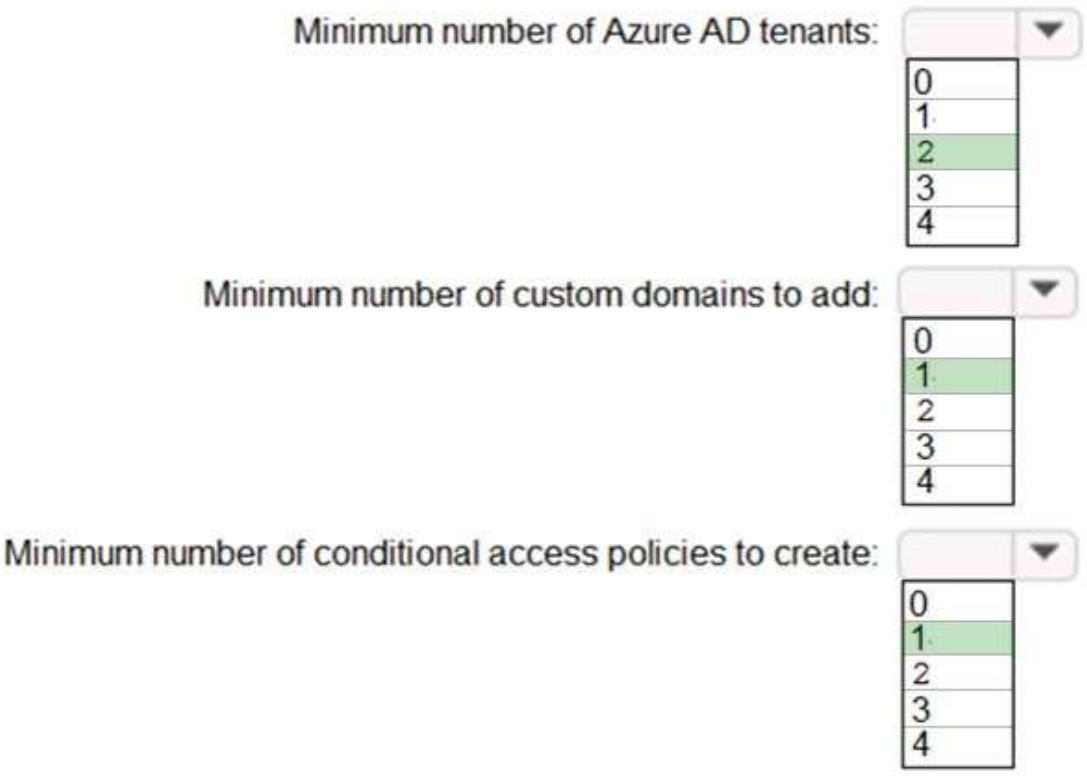
NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:

Answer Area



Section: (none)
Explanation

Explanation/Reference:
Explanation:

Box 1: 2
The network contains two Active Directory forests named corp.fabrikam.com and rd.fabrikam.com. There are no trust relationships between the forests.

Box 2: 1

Box 3: 1

Scenario:
- Users on the on-premises network must be able to authenticate to corp.fabrikam.com if an Internet link fails.
- Administrators must be able authenticate to the Azure portal by using their corp.fabrikam.com credentials.
- All administrative access to the Azure portal must be secured by using multi-factor authentication.

Note:
Users must always authenticate by using their corp.fabrikam.com UPN identity.
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.

Design Identity and Security

Question Set 2

QUESTION 1
HOTSPOT

Your company has the divisions shown in the following table.

Division	Azure subscription	Azure Active Directory (Azure AD) tenant
East	Sub1, Sub2	East.contoso.com
West	Sub3, Sub4	West.contoso.com

You plan to deploy a custom application to each subscription. The application will contain the following:

- A resource group
- An Azure web app
- Custom role assignments
- An Azure Cosmos DB account

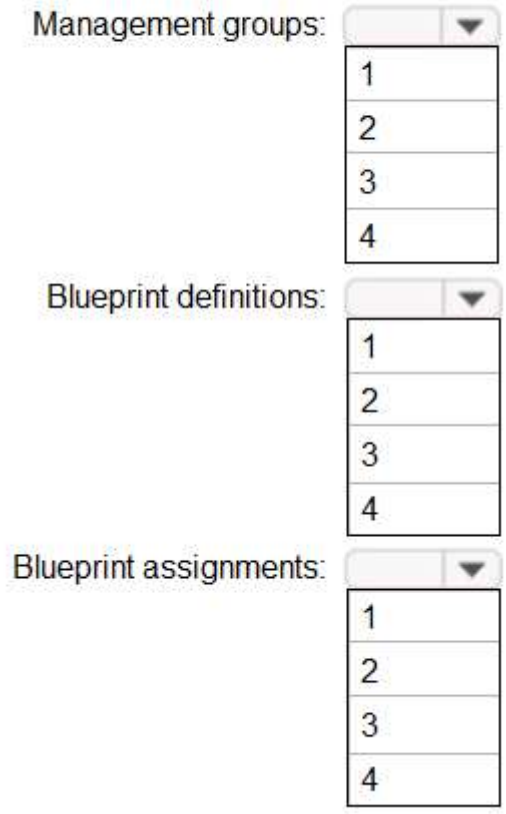
You need to use Azure Blueprints to deploy the application to each subscription.

What is the minimum number of objects required to deploy the application? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

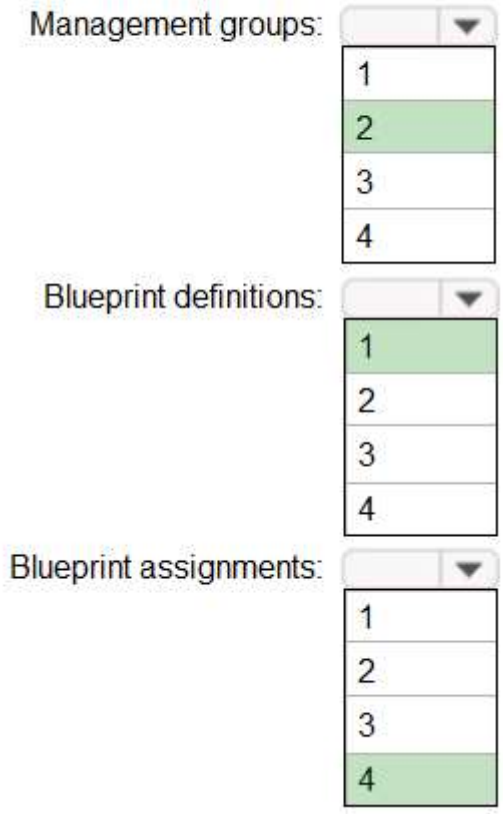
Hot Area:

Answer Area



Correct Answer:

Answer Area



Section: (none)
Explanation

Explanation/Reference:
Explanation:

Box 1: 2
One management group for East, and one for West.

When creating a blueprint definition, you'll define where the blueprint is saved. Blueprints can be saved to a management group or subscription that you have Contributor access to. If the location is a management group, the blueprint is available to assign to any child subscription of that management group.

Box 2: 1
One definition as the you plan to deploy a custom application to each subscription.

With Azure Blueprints, the relationship between the blueprint definition (what should be deployed) and the blueprint assignment (what was deployed) is preserved.

Box 3: 4
One assignment for each subscription.

Reference:
https://docs.microsoft.com/en-us/azure/governance/blueprints/overview

QUESTION 2

You have an Azure Active Directory (Azure AD) tenant.

You plan to deploy Azure Cosmos DB databases that will use the SQL API.

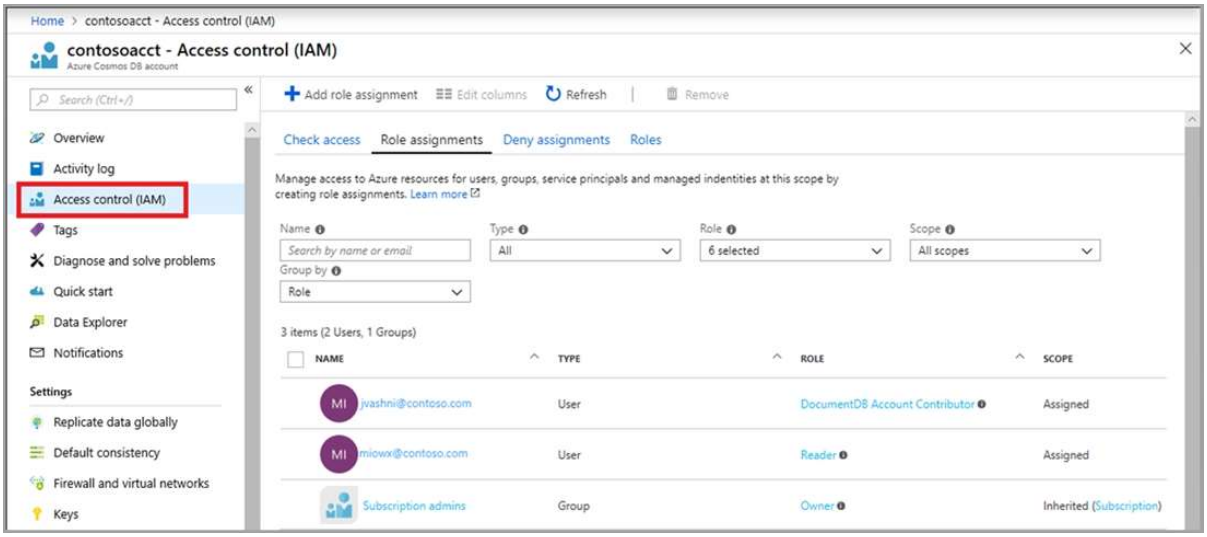
You need to recommend a solution to provide specific Azure AD user accounts with read access to the Cosmos DB databases.

What should you include in the recommendation?

A. shared access signatures (SAS) and conditional access policies
B. certificates and Azure Key Vault
C. a resource token and an Access control (IAM) role assignment
D. master keys and Azure Information Protection policies

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The Access control (IAM) pane in the Azure portal is used to configure role-based access control on Azure Cosmos resources. The roles are applied to users, groups, service principals, and managed identities in Active Directory. You can use built-in roles or custom roles for individuals and groups. The following screenshot shows Active Directory integration (RBAC) using access control (IAM) in the Azure portal:



Reference:
https://docs.microsoft.com/en-us/azure/cosmos-db/role-based-access-control

QUESTION 3
HOTSPOT

You need to design a resource governance solution for an Azure subscription. The solution must meet the following requirements:

- Ensure that all ExpressRoute resources are created in a resource group named RG1.
- Delegate the creation of the ExpressRoute resources to an Azure Active Directory (Azure AD) group named Networking.
- Use the principle of least privilege.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Ensure that all ExpressRoute resources are created in RG1:

- A custom RBAC role assignment at the level of RG1
- A custom RBAC role assignment at the subscription level
- An Azure Blueprints assignment that sets locking mode for the level of RG1
- An Azure Policy assignment at the subscription level that has an exclusion
- Multiple Azure Policy assignments at the resource group level except for RG1

Delegate the creation of the ExpressRoute resources to Networking:

- A custom RBAC role assignment at the level of RG1
- A custom RBAC role assignment at the subscription level
- An Azure Blueprints assignment that sets locking mode for the level of RG1
- An Azure Policy assignment at the subscription level that has an exclusion
- Multiple Azure Policy assignments at the resource group level except for RG1

Correct Answer:

Answer Area

Ensure that all ExpressRoute resources are created in RG1:

- A custom RBAC role assignment at the level of RG1
- A custom RBAC role assignment at the subscription level
- An Azure Blueprints assignment that sets locking mode for the level of RG1
- **An Azure Policy assignment at the subscription level that has an exclusion**
- Multiple Azure Policy assignments at the resource group level except for RG1

Delegate the creation of the ExpressRoute resources to Networking:

- **A custom RBAC role assignment at the level of RG1**
- A custom RBAC role assignment at the subscription level
- An Azure Blueprints assignment that sets locking mode for the level of RG1
- An Azure Policy assignment at the subscription level that has an exclusion
- Multiple Azure Policy assignments at the resource group level except for RG1

Section: (none)
Explanation

Explanation/Reference:
Explanation:

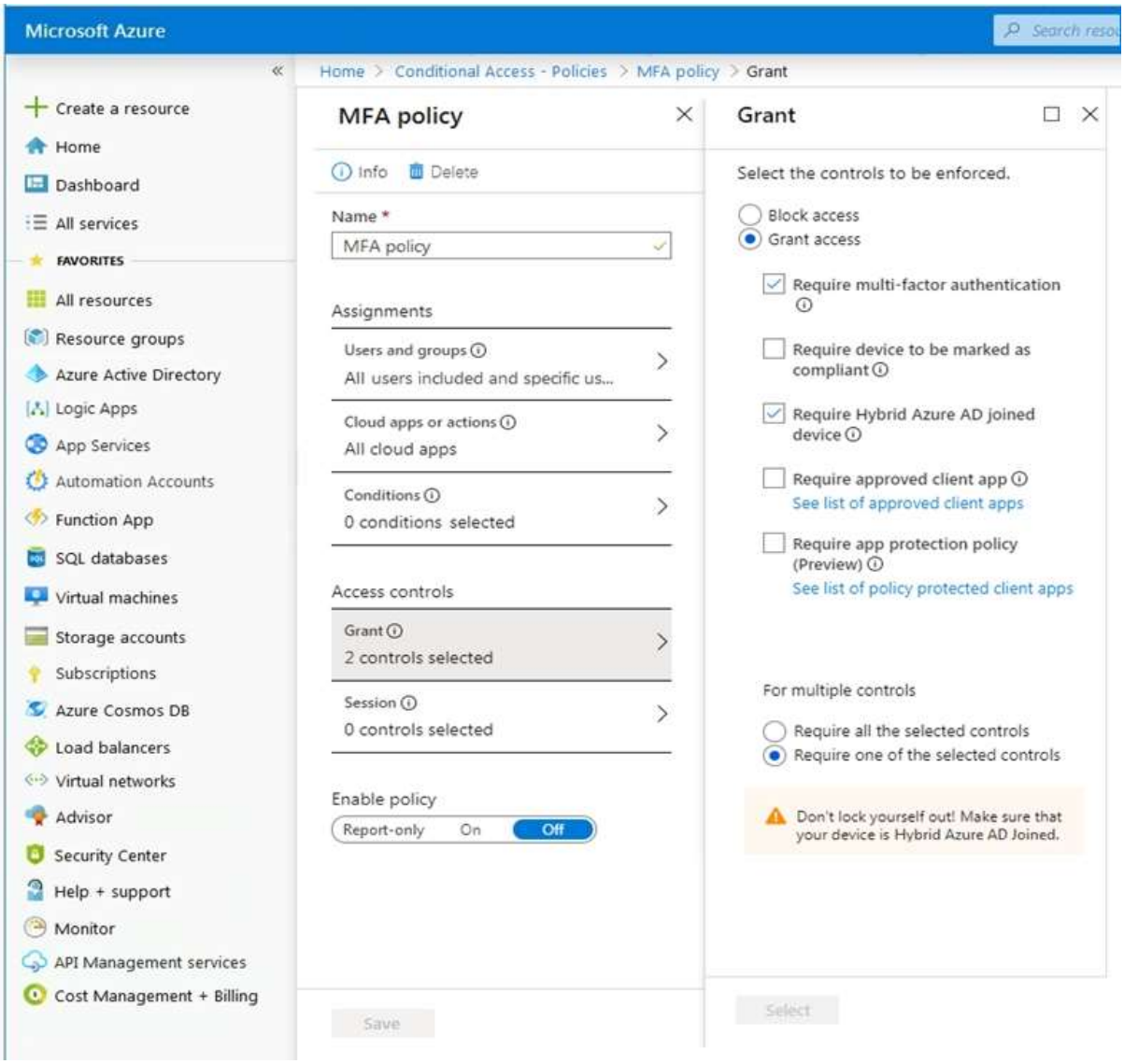
Box 1: An Azure policy assignment at the subscription level that has an exclusion

Box 2: A custom RBAC role assignment at the level of RG1
Azure role-based access control (Azure RBAC) is the authorization system you use to manage access to Azure resources. To grant access, you assign roles to users, groups, service principals, or managed identities at a particular scope.

Reference:
https://docs.microsoft.com/en-us/azure/governance/policy/tutorials/create-and-manage

QUESTION 4
You have an Azure Active Directory (Azure AD) tenant and Windows 10 devices.

You configure a conditional access policy as shown in the exhibit. (Click the **Exhibit** tab.)



What is the result of the policy?

A. All users will always be prompted for multi-factor authentication (MFA).
B. Users will be prompted for multi-factor authentication (MFA) only when they sign in from devices that are **NOT** joined to Azure AD.
C. All users will be able to sign in without using multi-factor authentication (MFA).
D. Users will be prompted for multi-factor authentication (MFA) only when they sign in from devices that are joined to Azure AD.

Correct Answer: B
Section: (none)

Explanation

Explanation/Reference:
Explanation:
Either the device should be joined to Azure AD or MFA must be used.

QUESTION 5
You are designing an Azure resource deployment that will use Azure Resource Manager templates. The deployment will use Azure Key Vault to store secrets.

You need to recommend a solution to meet the following requirements:

- Prevent the IT staff that will perform the deployment from retrieving the secrets directly from Key Vault.
- Use the principle of least privilege.

Which two actions should you recommend? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Create a Key Vault access policy that allows all get key permissions, get secret permissions, and get certificate permissions.
B. From Access policies in Key Vault, enable access to the Azure Resource Manager for template deployment.
C. Create a Key Vault access policy that allows all list key permissions, list secret permissions, and list certificate permissions.
D. Assign the IT staff a custom role that includes the Microsoft.KeyVault/Vaults/Deploy/Action permission.
E. Assign the Key Vault Contributor role to the IT staff.

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
B: To access a key vault during template deployment, set enabledForTemplateDeployment on the key vault to true.

D: The user who deploys the template must have the Microsoft.KeyVault/vaults/deploy/action permission for the scope of the resource group and key vault.

Incorrect Answers:
E: To grant access to a user to manage key vaults, you assign a predefined key vault Contributor role to the user at a specific scope.
If a user has Contributor permissions to a key vault management plane, the user can grant themselves access to the data plane by setting a Key Vault access policy. You should tightly control who has Contributor role access to your key vaults. Ensure that only authorized persons can access and manage your key vaults, keys, secrets, and certificates.

Reference:
https://docs.microsoft.com/en-us/azure/azure-resource-manager/templates/key-vault-parameter

https://docs.microsoft.com/en-us/azure/key-vault/general/overview-security

QUESTION 6
You have an Azure subscription that contains resources in three Azure regions.

You need to implement Azure Key Vault to meet the following requirements:

- In the event of a regional outage, all keys must be readable.
- All the resources in the subscription must be able to access Key Vault.
- The number of Key Vault resources to be deployed and managed must be minimized.

How many instances of Key Vault should you implement?

A. 1
B. 2
C. 3
D. 6

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The contents of your key vault are replicated within the region and to a secondary region at least 150 miles away but within the same geography. This maintains high durability of your keys and secrets. See the Azure paired regions document for details on specific region pairs.

Example: Secrets that must be shared by your application in both Europe West and Europe North. Minimize these as much as you can. Put these in a key vault in either of the two regions. Use the same URI from both regions. Microsoft will fail over the Key Vault service internally.

Reference:
https://docs.microsoft.com/en-us/azure/key-vault/general/disaster-recovery-guidance

QUESTION 7
You have an Azure Active Directory (Azure AD) tenant.

You plan to provide users with access to shared files by using Azure Storage. The users will be provided with different levels of access to various Azure file shares based on their user account or their group membership.

You need to recommend which additional Azure services must be used to support the planned deployment.

What should you include in the recommendation?

A. an Azure AD enterprise application
B. Azure Information Protection
C. an Azure AD Domain Services (Azure AD DS) instance
D. an Azure Front Door instance

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Azure Files supports identity-based authentication over Server Message Block (SMB) through two types of Domain Services: on-premises Active Directory Domain Services (AD DS) and Azure Active Directory Domain Services (Azure AD DS).

Reference:
https://docs.microsoft.com/en-us/azure/storage/files/storage-files-identity-auth-active-directory-domain-service-enable

QUESTION 8

DRAG DROP

Your company has users who work remotely from laptops.

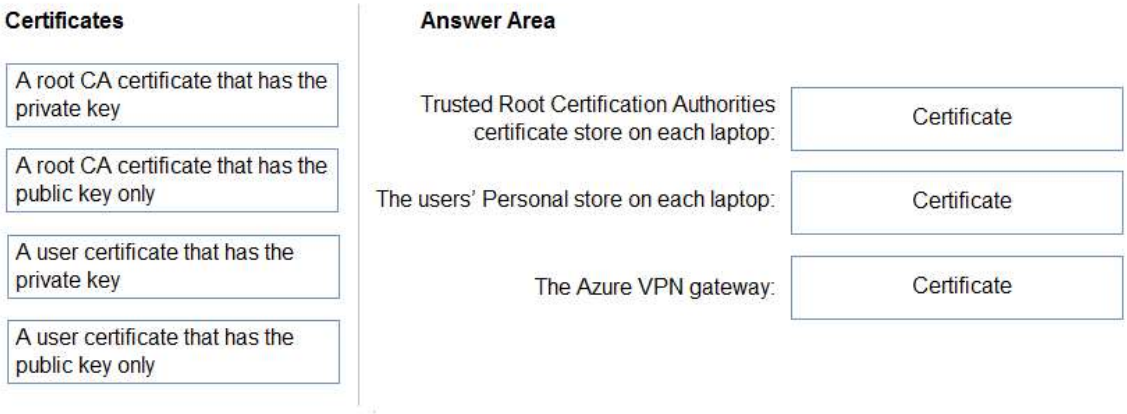
You plan to move some of the applications accessed by the remote users to Azure virtual machines. The users will access the applications in Azure by using a point-to-site VPN connection. You will use certificates generated from an on-premises-based Certification authority (CA).

You need to recommend which certificates are required for the deployment.

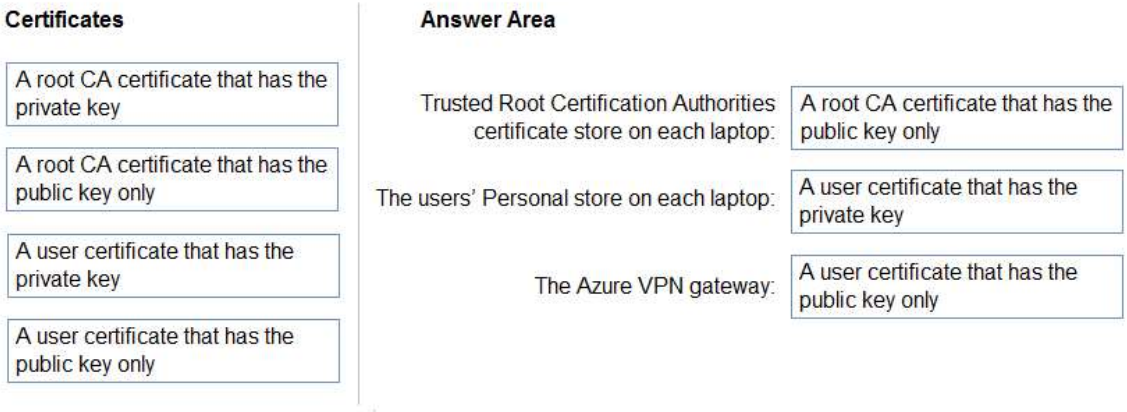
What should you include in the recommendation? To answer, drag the appropriate certificates to the correct targets. Each certificate may be used once, more than once, of not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:



Correct Answer:



Section: (none)
Explanation

Explanation/Reference:

QUESTION 9
HOTSPOT

You are building an application that will run in a virtual machine (VM). The application will use Azure Managed Identity.

The application uses Azure Key Vault, Azure SQL Database, and Azure Cosmos DB.

You need to ensure the application can use secure credentials to access these services.

Which authentication method should you recommend? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Functionality	Authorization method
Azure Key Vault	Hash-based message authentication code (HMAC) Azure Managed Identity Role-Based Access Controls (RBAC) HTTPS encryption
Azure SQL	Hash-based message authentication code (HMAC) Azure Managed Identity Role-Based Access Controls (RBAC) HTTPS encryption
Cosmos DB	Hash-based message authentication code (HMAC) Azure Managed Identity Role-Based Access Controls (RBAC) HTTPS encryption

Correct Answer:

Answer Area

Functionality	Authorization method
Azure Key Vault	Hash-based message authentication code (HMAC) **Azure Managed Identity** Role-Based Access Controls (RBAC) HTTPS encryption
Azure SQL	Hash-based message authentication code (HMAC) **Azure Managed Identity** Role-Based Access Controls (RBAC) HTTPS encryption
Cosmos DB	Hash-based message authentication code (HMAC) **Azure Managed Identity** Role-Based Access Controls (RBAC) HTTPS encryption

Section: (none)
Explanation

Explanation/Reference:
Explanation:

Note: Managed identities for Azure resources is the new name for the service formerly known as Managed Service Identity (MSI).

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/overview

QUESTION 10
You have an Azure subscription that contains a custom application named Application1. Application1 was developed by an external company named Fabrikam, Ltd. Developers at Fabrikam were assigned role-based access control (RBAC) permissions to the Application1 components. All users are licensed for the Microsoft 365 E5 plan.

You need to recommend a solution to verify whether the Fabrikam developers still require permissions to Application1. The solution must meet the following requirements:

- To the manager of the developers, send a monthly email message that lists the access permissions to Application1.
- If the manager does not verify an access permission, automatically revoke that permission.
- Minimize development effort.

What should you recommend?

A. Create an Azure Automation runbook that runs the `Get-AzureADUserAppRoleAssignment` cmdlet.

B. Create an Azure Automation runbook that runs the `Get-AzureRoleAssignment` cmdlet.
C. In Azure Active Directory (Azure AD), create an access review of Application1.
D. In Azure Active Directory (AD) Privileged Identity Management, create a custom role assignment for the Application1 resources.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11
DRAG DROP

A company named Contoso, Ltd. has an Azure Active Directory (Azure AD) tenant that uses the Basic license.

You plan to deploy two applications to Azure. The applications have the requirements shown in the following table.

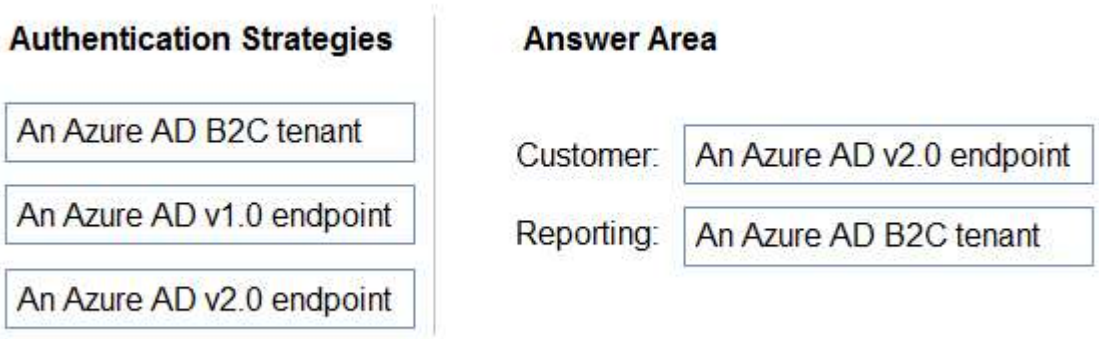
Application name	Requirement
Customer	Users must authenticate by using a personal Microsoft account and multi-factor authenication
Reporting	Users must authenticate by using either Contoso credentials or a personal Microsoft account. You must be able to manage the accounts from Azure AD.

Which authentication strategy should you recommend for each application? To answer, drag the appropriate authentication strategies to the correct applications. Each authentication strategy 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.

Select and Place:

Correct Answer:



Section: (none)
Explanation

Explanation/Reference:
Explanation:

Box 1: Azure AD V2.0 endpoint
Microsoft identity platform is an evolution of the Azure Active Directory (Azure AD) developer platform. It allows developers to build applications that sign in all Microsoft identities and get tokens to call Microsoft APIs, such as Microsoft Graph, or APIs that developers have built. The Microsoft identity platform consists of:

OAuth 2.0 and OpenID Connect standard-compliant authentication service that enables developers to authenticate any Microsoft identity, including:
Work or school accounts (provisioned through Azure AD)
Personal Microsoft accounts (such as Skype, Xbox, and Outlook.com)
Social or local accounts (via Azure AD B2C)

Box 2: Azure AD B2C tenant
Azure Active Directory B2C provides business-to-customer identity as a service. Your customers use their preferred social, enterprise, or local account identities to get single sign-on access to your applications and APIs.
Azure Active Directory B2C (Azure AD B2C) integrates directly with Azure Multi-Factor Authentication so that you can add a second layer of security to sign-up and sign-in experiences in your applications.

Reference:
https://docs.microsoft.com/en-us/azure/active-directory-b2c/active-directory-b2c-reference-mfa

https://docs.microsoft.com/en-us/azure/active-directory/develop/v2-overview

QUESTION 12
HOTSPOT

You manage a network that includes an on-premises Active Directory domain and an Azure Active Directory (Azure AD).

Employees are required to use different accounts when using on-premises or cloud resources. You must recommend a solution that lets employees sign in to all company resources by using a single account. The solution must implement an identity provider.

You need to provide guidance on the different identity providers.

How should you describe each identity provider? To answer, select the appropriate description from each list in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Identity Provider	Description
synchronized identity	User management occurs on-premises. Azure AD authenticates employees by using on-premises passwords. User management occurs on-premises. The on-premises domain controller authenticates employee credentials. Both user management and authentication occur in Azure AD.
federated identity	User management occurs on-premises. Azure AD authenticates employees by using on-premises passwords. User management occurs on-premises. The on-premises domain controller authenticates employee credentials. Both user management and authentication occur in Azure AD.

Correct Answer:

Answer Area

Identity Provider	Description
synchronized identity	User management occurs on-premises. Azure AD authenticates employees by using on-premises passwords. User management occurs on-premises. The on-premises domain controller authenticates employee credentials. Both user management and authentication occur in Azure AD.
federated identity	User management occurs on-premises. Azure AD authenticates employees by using on-premises passwords. User management occurs on-premises. The on-premises domain controller authenticates employee credentials. Both user management and authentication occur in Azure AD.

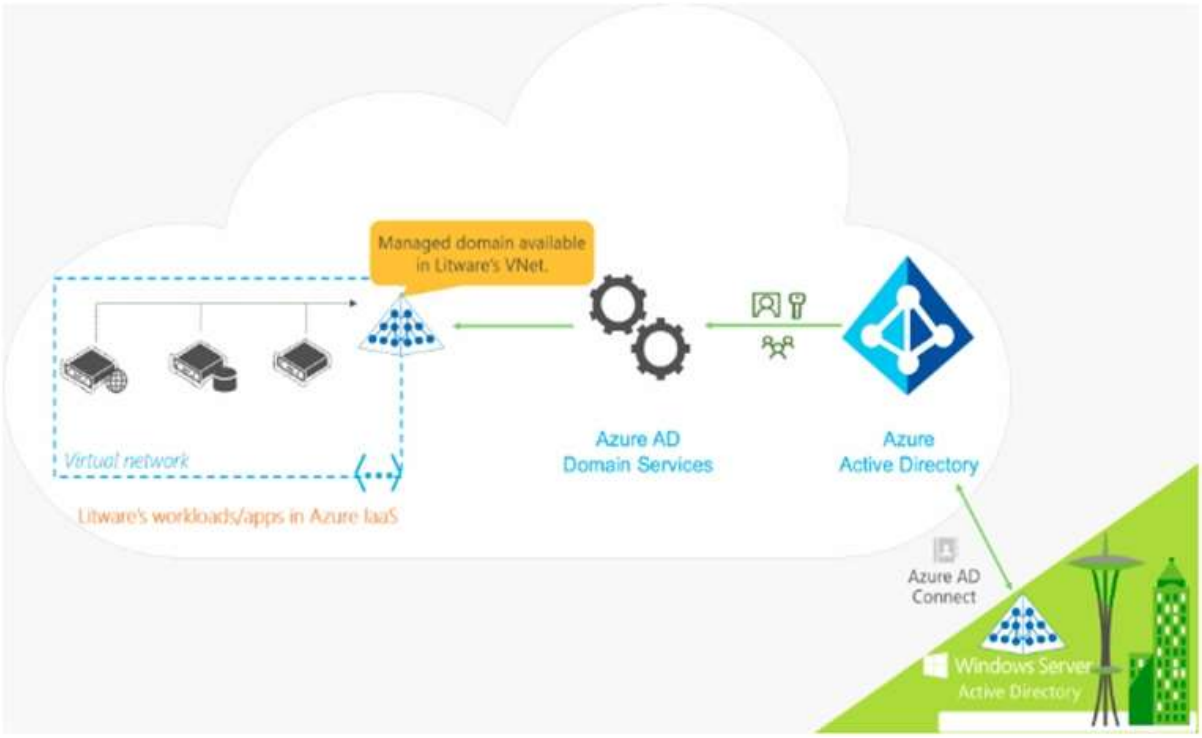
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Box1: User management occurs on-premises. Azure AD authenticates employees by using on-premises passwords.

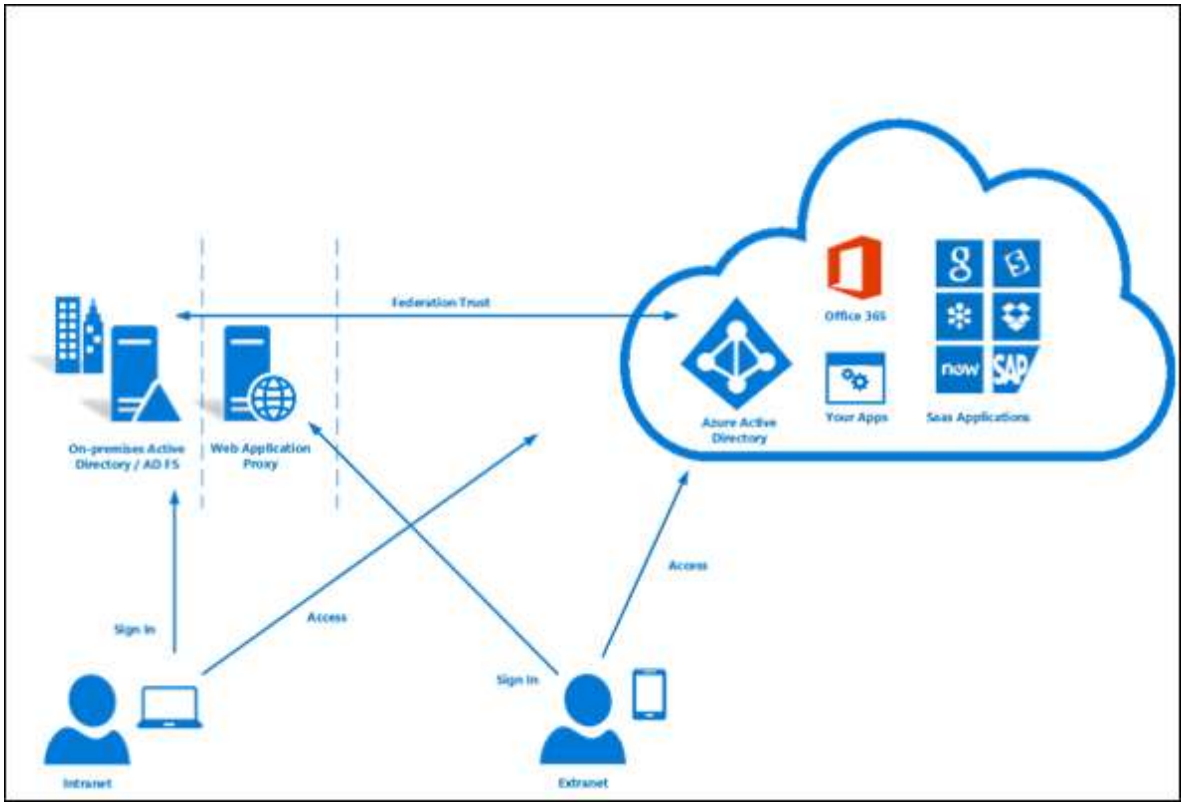
Azure AD Domain Services for hybrid organizations
Organizations with a hybrid IT infrastructure consume a mix of cloud resources and on-premises resources. Such organizations synchronize identity information from their on-premises directory to their Azure AD tenant. As hybrid organizations look to migrate more of their on-premises applications to the cloud, especially legacy directory-aware applications, Azure AD Domain Services can be useful to them.

Example: Litware Corporation has deployed Azure AD Connect, to synchronize identity information from their on-premises directory to their Azure AD tenant. The identity information that is synchronized includes user accounts, their credential hashes for authentication (password hash sync) and group memberships.



User accounts, group memberships, and credentials from Litware's on-premises directory are synchronized to Azure AD via Azure AD Connect. These user accounts, group memberships, and credentials are automatically available within the managed domain.

Box 2: User management occurs on-premises. The on-promises domain controller authenticates employee credentials.
You can federate your on-premises environment with Azure AD and use this federation for authentication and authorization. This sign-in method ensures that all user authentication occurs on-premises.

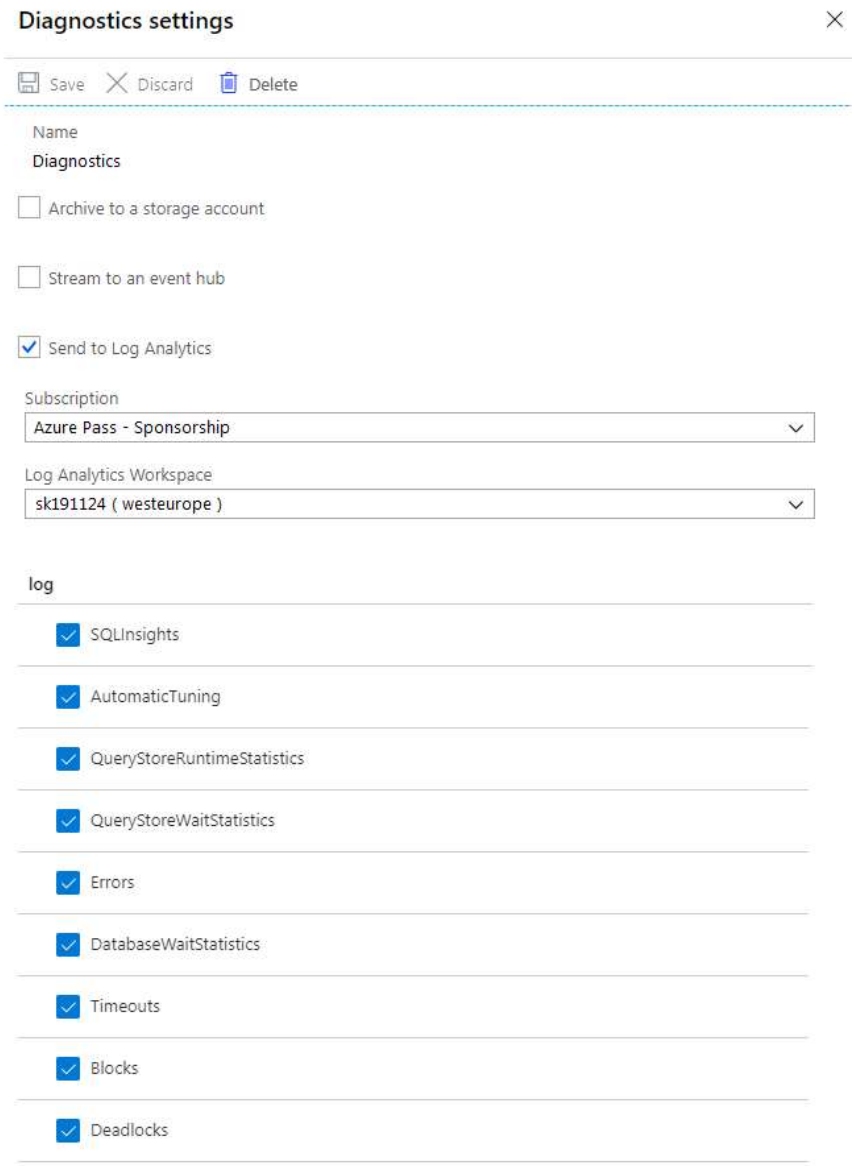


Reference:
https://docs.microsoft.com/en-us/azure/active-directory-domain-services/active-directory-ds-overview

https://docs.microsoft.com/en-us/azure/active-directory/hybrid/whatis-fed

QUESTION 13
HOTSPOT

You configure the Diagnostics settings for an Azure SQL database as shown in the following exhibit.



Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

To perform real-time reporting by using Microsoft Power BI, you must first **[answer choice]**.

- clear Send to Log Analytics
- clear SQLInsights
- select Archive to a storage account
- select Stream to an event hub

Diagnostics data can be reviewed in **[answer choice]**.

- Azure Analysis Services
- Azure Application Insights
- Azure SQL Analytics
- Microsoft SQL Server Analysis Services (SSAS)
- SQL Health Check

Correct Answer:

Answer Area

To perform real-time reporting by using Microsoft Power BI, you must first **[answer choice]**.

- clear Send to Log Analytics
- clear SQLInsights
- select Archive to a storage account
- **select Stream to an event hub**

Diagnostics data can be reviewed in **[answer choice]**.

- Azure Analysis Services
- Azure Application Insights
- **Azure SQL Analytics**
- Microsoft SQL Server Analysis Services (SSAS)
- SQL Health Check

Section: (none)
Explanation

Explanation/Reference:

QUESTION 14
You plan to deploy an application named App1 that will run on five Azure virtual machines. Additional virtual machines will be deployed later to run App1.

You need to recommend a solution to meet the following requirements for the virtual machines that will run App1:

- Ensure that the virtual machines can authenticate to Azure Active Directory (Azure AD) to gain access to an Azure key vault, Azure Logic Apps instances, and an Azure SQL database.
- Avoid assigning new roles and permissions for Azure services when you deploy additional virtual machines.
- Avoid storing secrets and certificates on the virtual machines.

- Minimize administrative effort for managing identities.

Which type of identity should you include in the recommendation?

A. a service principal that is configured to use a certificate
B. a system-assigned managed identity
C. a service principal that is configured to use a client secret
D. a user-assigned managed identity

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Managed identities for Azure resources is a feature of Azure Active Directory.
User-assigned managed identity can be shared. The same user-assigned managed identity can be associated with more than one Azure resource.

Incorrect Answers:
B: System-assigned managed identity cannot be shared. It can only be associated with a single Azure resource.

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/overview

QUESTION 15
You are designing a large Azure environment that will contain many subscriptions.

You plan to use Azure Policy as part of a governance solution.

To which three scopes can you assign Azure Policy definitions? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. management groups
B. subscriptions
C. Azure Active Directory (Azure AD) tenants
D. resource groups
E. Azure Active Directory (Azure AD) administrative units
F. compute resources

Correct Answer: ABD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Azure Policy evaluates resources in Azure by comparing the properties of those resources to business rules. Once your business rules have been formed, the policy definition or initiative is assigned to any scope of resources that Azure supports, such as management groups, subscriptions, resource groups, or individual resources.

Reference:
https://docs.microsoft.com/en-us/azure/governance/policy/overview

QUESTION 16
You are designing a microservices architecture that will be hosted in an Azure Kubernetes Service (AKS) cluster. Apps that will consume the microservices will be hosted on Azure virtual machines. The virtual machines and the AKS cluster will reside on the same virtual network.

You need to design a solution to expose the microservices to the consumer apps. The solution must meet the following requirements:

- Ingress access to the microservices must be restricted to a single private IP address and protected by using mutual TLS authentication.
- The number of incoming microservice calls must be rate-limited.
- Costs must be minimized.

What should you include in the solution?

A. Azure App Gateway with Azure Web Application Firewall (WAF)
B. Azure API Management Premium tier with virtual network connection
C. Azure API Management Standard tier with a service endpoint
D. Azure Front Door with Azure Web Application Firewall (WAF)

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
One option is to deploy APIM (API Management) inside the cluster VNet.
The AKS cluster and the applications that consume the microservices might reside within the same VNet, hence there is no reason to expose the cluster publicly as all API traffic will remain within the VNet. For these scenarios, you can deploy API Management into the cluster VNet. API Management Premium tier supports VNet deployment.

Reference:
https://docs.microsoft.com/en-us/azure/api-management/api-management-kubernetes

QUESTION 17
HOTSPOT

A company plans to implement an HTTP-based API to support a web app. The web app allows customers to check the status of their orders.

The API must meet the following requirements:

- Implement Azure Functions.
- Provide public read-only operations.
- Do not allow write operations.

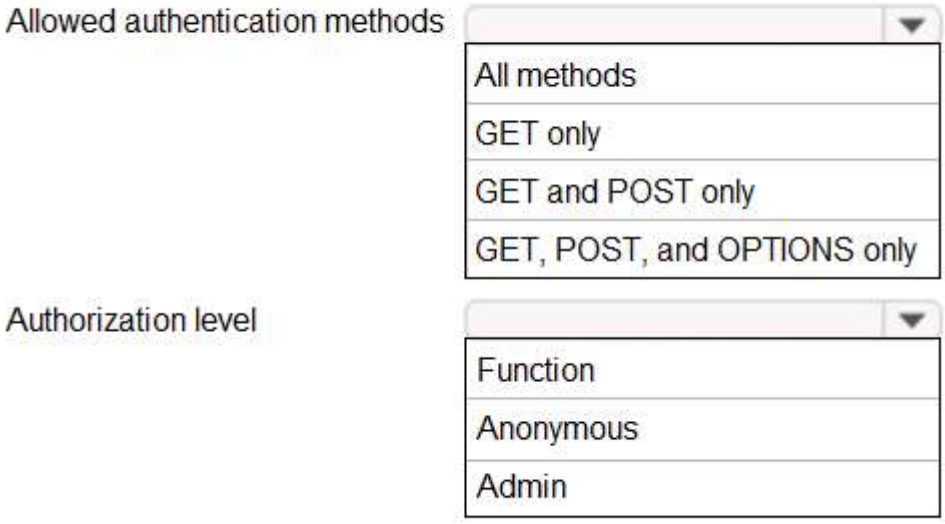
You need to recommend configuration options.

What should you recommend? To answer, configure the appropriate options in the dialog box in the answer area.

NOTE: Each correct selection is worth one point.

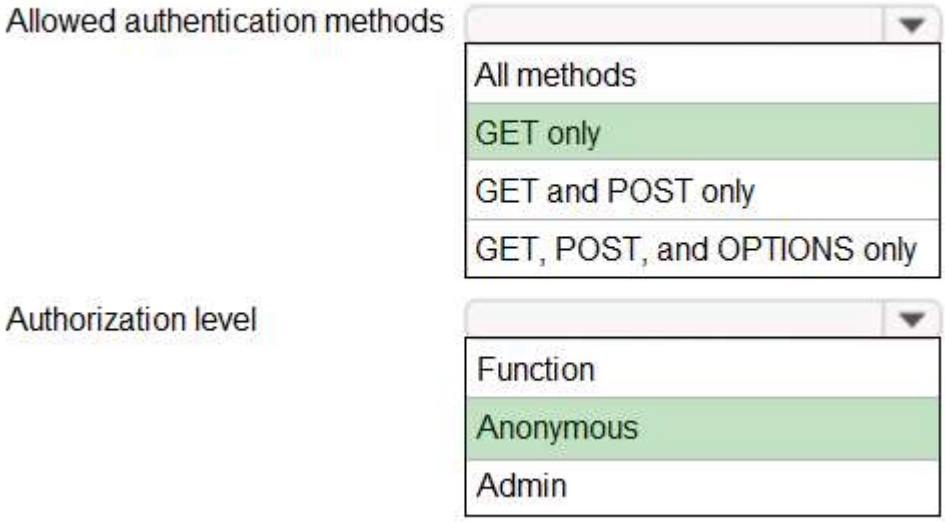
Hot Area:

Answer Area



Correct Answer:

Answer Area



Section: (none)
Explanation

Explanation/Reference:
Explanation:

Allowed authentication methods: GET only

Authorization level: Anonymous
The option is Allow Anonymous requests. This option turns on authentication and authorization in App Service,

but defers authorization decisions to your application code. For authenticated requests, App Service also passes along authentication information in the HTTP headers.

This option provides more flexibility in handling anonymous requests.

Reference:
https://docs.microsoft.com/en-us/azure/app-service/overview-authentication-authorization

QUESTION 18
A company named Contoso Ltd., has a single-domain Active Directory forest named contoso.com.

Contoso is preparing to migrate all workloads to Azure. Contoso wants users to use single sign-on (SSO) when they access cloud-based services that integrate with Azure Active Directory (Azure AD).

You need to identify any objects in Active Directory that will fail to synchronize to Azure AD due to formatting issues. The solution must minimize costs.

What should you include in the solution?

A. Azure AD Connect Health
B. Microsoft Office 365 IdFix
C. Azure Advisor
D. Password Export Server version 3.1 (PES v3.1) in Active Directory Migration Tool (ADMT)

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19
DRAG DROP

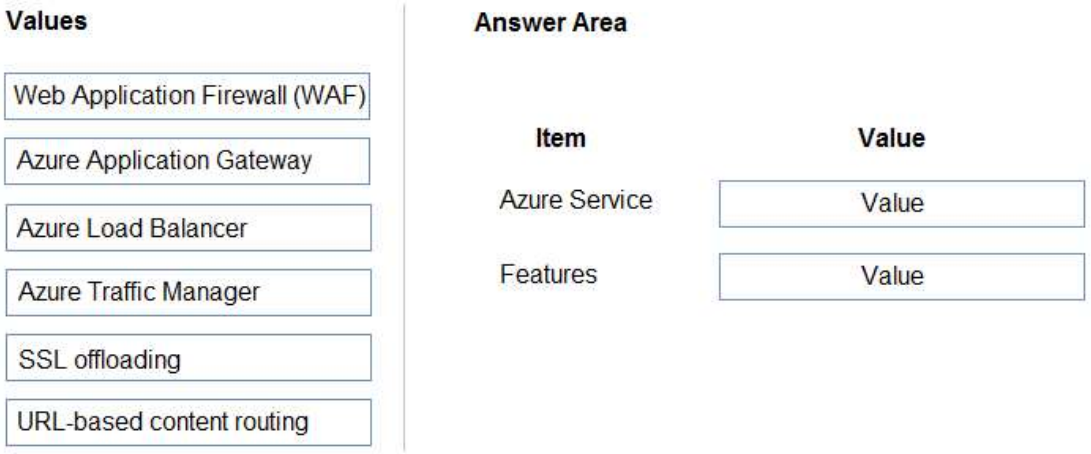
A company has an existing web application that runs on virtual machines (VMs) in Azure.

You need to ensure that the application is protected from SQL injection attempts and uses a layer-7 load balancer. The solution must minimize disruption to the code for the existing web application.

What should you recommend? To answer, drag the appropriate values to the correct items. Each value 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.

Select and Place:



Correct Answer:

Section: (none)
Explanation

Explanation/Reference:
Explanation:

Box 1: Azure Application Gateway
Azure Application Gateway provides an application delivery controller (ADC) as a service. It offers various layer 7 load-balancing capabilities for your applications.

Box 2: Web Application Firewall (WAF)
Application Gateway web application firewall (WAF) protects web applications from common vulnerabilities and exploits.
This is done through rules that are defined based on the OWASP core rule sets 3.0 or 2.2.9.
There are rules that detects SQL injection attacks.

Reference:
https://docs.microsoft.com/en-us/azure/application-gateway/application-gateway-faq

https://docs.microsoft.com/en-us/azure/application-gateway/waf-overview

QUESTION 20
You have an Azure subscription. The subscription has a blob container that contains multiple blobs.

Ten users in the finance department of your company plan to access the blobs during the month of April.

You need to recommend a solution to enable access to the blobs during the month of April only.

Which security solution should you include in the recommendation?

A. access keys
B. conditional access policies
C. certificates
D. shared access signatures (SAS)

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference:
https://docs.microsoft.com/en-us/azure/storage/common/storage-sas-overview

QUESTION 21
HOTSPOT

You plan to deploy an Azure web app named App1 that will use Azure Active Directory (Azure AD) authentication.

App1 will be accessed from the internet by the users at your company. All the users have computers that run Windows 10 and are joined to Azure AD.

You need to recommend a solution to ensure that the users can connect to App1 without being prompted for authentication and can access App1 only from company-owned computers.

What should you recommend for each requirement? To answer, select the appropriate options in the answer area.

Hot Area:

Answer Area

The users can connect to App1 without being prompted for authentication:

- An Azure AD app registration
- An Azure AD managed identity
- Azure AD Application Proxy

The users can access App1 only from company-owned computers:

- A conditional access policy
- An Azure AD administrative unit
- Azure Application Gateway
- Azure Blueprints
- Azure Policy

Correct Answer:

Answer Area

The users can connect to App1 without being prompted for authentication:

- An Azure AD app registration
- An Azure AD managed identity
- Azure AD Application Proxy

The users can access App1 only from company-owned computers:

- A conditional access policy
- An Azure AD administrative unit
- Azure Application Gateway
- Azure Blueprints
- Azure Policy

Section: (none)
Explanation

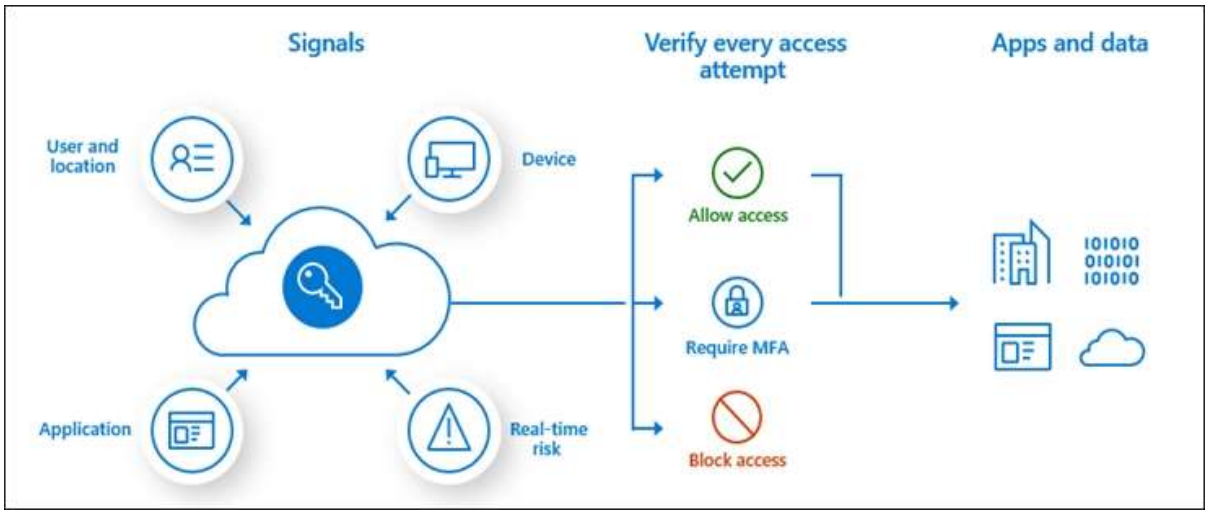
Explanation/Reference:
Explanation:

Box 1: An Azure AD app registration
Azure active directory (AD) provides cloud based directory and identity management services.You can use

azure AD to manage users of your application and authenticate access to your applications using azure active directory.
You register your application with Azure active directory tenant.

Box 2: A conditional access policy
Conditional Access policies at their simplest are if-then statements, if a user wants to access a resource, then they must complete an action.

By using Conditional Access policies, you can apply the right access controls when needed to keep your organization secure and stay out of your user's way when not needed.



Reference:
https://codingcanvas.com/using-azure-active-directory-authentication-in-your-web-application/

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

QUESTION 22
HOTSPOT

You plan to create an Azure environment that will contain a root management group and 10 child management groups. Each child management group will contain five Azure subscriptions. You plan to have between 10 and 30 resource groups in each subscription.

You need to design an Azure governance solution. The solution must meet the following requirements:

- Use Azure Blueprints to control governance across all the subscriptions and resource groups.
- Ensure that Blueprints-based configurations are consistent across all the subscriptions and resource groups.
- Minimize the number of blueprint definitions and assignments.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Level at which to define the blueprints:

- The child management groups
- The root management group
- The subscriptions

Level at which to create the blueprint assignments:

- The child management groups
- The root management group
- The subscriptions

Correct Answer:

Answer Area

Level at which to define the blueprints:

- The child management groups
- **The root management group**
- The subscriptions

Level at which to create the blueprint assignments:

- The child management groups
- **The root management group**
- The subscriptions

Section: (none)
Explanation

Explanation/Reference:
Explanation:

Box 1: The root management group
When creating a blueprint definition, you'll define where the blueprint is saved. Blueprints can be saved to a management group or subscription that you have Contributor access to. If the location is a management group, the blueprint is available to assign to any child subscription of that management group.

Box 2: The root management group
Each directory is given a single top-level management group called the "Root" management group. This root management group is built into the hierarchy to have all management groups and subscriptions fold up to it. This root management group allows for global policies and Azure role assignments to be applied at the directory level.

Each Published Version of a blueprint can be assigned to an existing management group or subscription.

Reference:
https://docs.microsoft.com/en-us/azure/governance/blueprints/overview

https://docs.microsoft.com/en-us/azure/governance/management-groups/overview

QUESTION 23
You have an Azure subscription.

You need to recommend a solution to provide developers with the ability to provision Azure virtual machines. The solution must meet the following requirements:

- Only allow the creation of the virtual machines in specific regions.
- Only allow the creation of specific sizes of virtual machines.

What should you include in the recommendation?

A. Azure Resource Manager templates
B. Azure Policy
C. conditional access policies
D. role-based access control (RBAC)

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24
Your company has the offices shown in the following table.

Location	IP address space	Public NAT segment
Montreal	10.10.0.0/16	190.15.1.0/24
Seattle	172.16.0.0/16	194.25.2.0/24

The network contains an Active Directory domain named contoso.com that is synced to Azure Active Directory (Azure AD).

All users connect to an Exchange Online.

You need to recommend a solution to ensure that all the users use Azure Multi-Factor Authentication (MFA) to connect to Exchange Online from one of the offices.

What should you include in the recommendation?

A. a virtual network and two Microsoft Cloud App Security policies
B. a named location and two Microsoft Cloud App Security policies
C. a conditional access policy and two virtual networks
D. a conditional access policy and two named locations

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

Explanation:
Conditional Access policies are at their most basic an if-then statement combining signals, to make decisions, and enforce organization policies. One of those signals that can be incorporated into the decision-making process is network location.

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition#named-locations

QUESTION 25
HOTSPOT

Your organization has developed and deployed several Azure App Service Web and API applications. The applications use Azure Key Vault to store several authentication, storage account, and data encryption keys. Several departments have the following requests to support the applications:

Department	Request
Security	• Review membership of administrative roles and require users to provide a justification for continued membership. • Get alerts about changes in administrator assignments. • See a history of administrator activation, including which changes administrators made to Azure resources.
Development	• Enable the applications to access Azure Key Vault and retrieve keys for use in code.
Quality Assurance	• Receive temporary administrator access to create and configure additional Web and API applications in the test environment.

You need to recommend the appropriate Azure service for each department request.

What should you recommend? To answer, configure the appropriate options in the dialog box in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Department	Azure Service
Security	Azure AD Privileged Identity Management Azure Managed Identity Azure AD Connect Azure AD Identity Protection
Development	Azure AD Privileged Identity Management Azure Managed Identity Azure AD Connect Azure AD Identity Protection
Quality Assurance	Azure AD Privileged Identity Management Azure Managed Identity Azure AD Connect Azure AD Identity Protection

Correct Answer:

Answer Area

Department	Azure Service
Security	Azure AD Privileged Identity Management
Development	Azure Managed Identity
Quality Assurance	Azure AD Privileged Identity Management

Azure AD Privileged Identity Management
Azure Managed Identity
Azure AD Connect
Azure AD Identity Protection

Section: (none)
Explanation

Explanation/Reference:

QUESTION 26
Your network contains an on-premises Active Directory forest.

You discover that when users change jobs within your company, the membership of the user groups are not being updated. As a result, the users can access resources that are no longer relevant to their job.

You plan to integrate Active Directory and Azure Active Directory (Azure AD) by using Azure AD Connect.

You need to recommend a solution to ensure that group owners are emailed monthly about the group memberships they manage.

What should you include in the recommendation?

A. Azure AD Identity Protection
B. Azure AD access reviews
C. Tenant Restrictions
D. conditional access policies

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 27
HOTSPOT

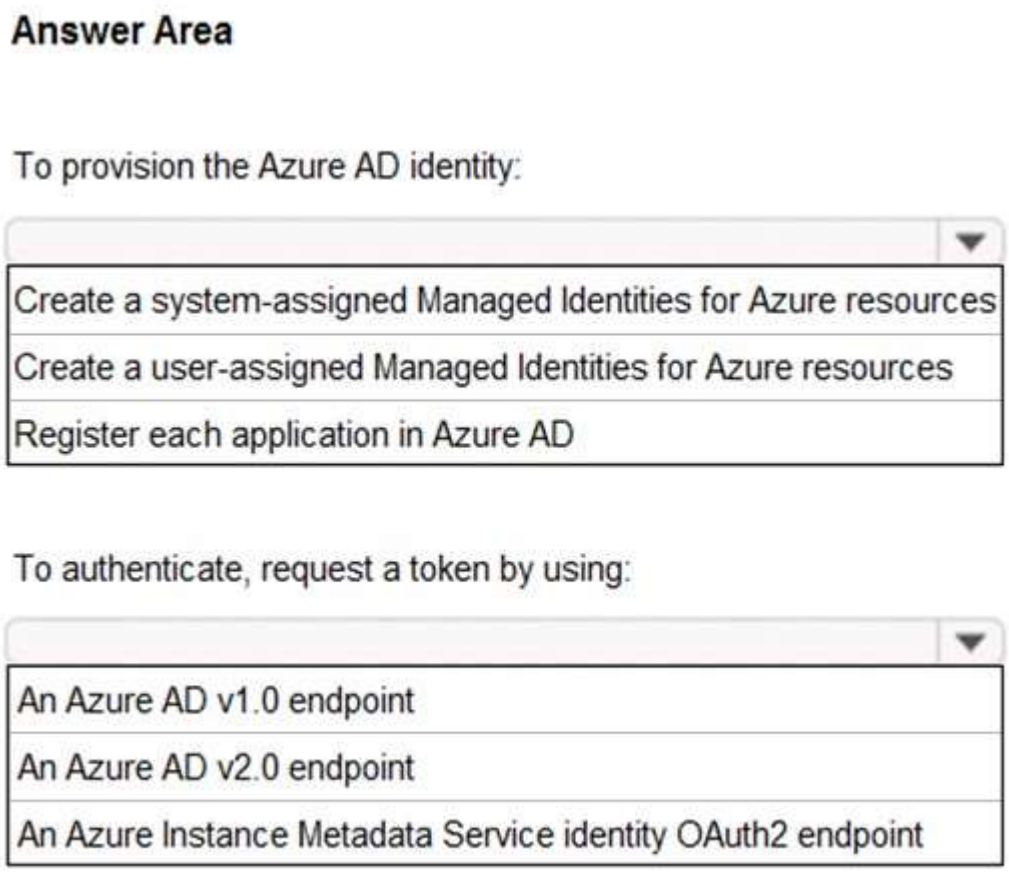
You have five .NET Core applications that run on 10 Azure virtual machines in the same subscription.

You need to recommend a solution to ensure that the applications can authenticate by using the same Azure Active Directory (Azure AD) identity. The solution must meet the following requirements:

- Ensure that the applications can authenticate only when running on the 10 virtual machines.
- Minimize administrative effort.

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

Hot Area:



Correct Answer:

Answer Area

To provision the Azure AD identity:

Create a system-assigned Managed Identities for Azure resources
Create a user-assigned Managed Identities for Azure resources
Register each application in Azure AD

To authenticate, request a token by using:

An Azure AD v1.0 endpoint
An Azure AD v2.0 endpoint
An Azure Instance Metadata Service identity OAuth2 endpoint

Section: (none)
Explanation

Explanation/Reference:
Explanation:

Box 1: Create a system-assigned Managed Identities for Azure resource
The managed identities for Azure resources feature in Azure Active Directory (Azure AD) feature provides Azure services with an automatically managed identity in Azure AD. You can use the identity to authenticate to any service that supports Azure AD authentication, including Key Vault, without any credentials in your code.

A system-assigned managed identity is enabled directly on an Azure service instance. When the identity is enabled, Azure creates an identity for the instance in the Azure AD tenant that's trusted by the subscription of the instance. After the identity is created, the credentials are provisioned onto the instance.

Box 2: An Azure Instance Metadata Service Identity
See step 3 and 5 below.

How a system-assigned managed identity works with an Azure VM
1. Azure Resource Manager receives a request to enable the system-assigned managed identity on a VM.
2. Azure Resource Manager creates a service principal in Azure AD for the identity of the VM. The service principal is created in the Azure AD tenant that's trusted by the subscription.
3. Azure Resource Manager configures the identity on the VM by updating the Azure Instance Metadata Service identity endpoint with the service principal client ID and certificate.
4. After the VM has an identity, use the service principal information to grant the VM access to Azure resources. To call Azure Resource Manager, use role-based access control (RBAC) in Azure AD to assign

the appropriate role to the VM service principal. To call Key Vault, grant your code access to the specific secret or key in Key Vault.
5. Your code that's running on the VM can request a token from the Azure Instance Metadata service endpoint, accessible only from within the VM

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/overview

QUESTION 28
You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains two administrative user accounts named Admin1 and Admin2.

You create two Azure virtual machines named VM1 and VM2.

You need to ensure that Admin1 and Admin2 are notified when more than five events are added to the security log of VM1 or VM2 during a period of 120 seconds. The solution must minimize administrative tasks.

What should you create?

A. two action groups and two alert rules
B. one action group and one alert rule
C. five action groups and one alert rule
D. two action groups and one alert rule

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have an Azure Active Directory (Azure AD) tenant named contoso.com. The tenant contains a group named Group1. Group1 contains all the administrative user accounts.

You discover several login attempts to the Azure portal from countries where administrative users do **NOT** work.

You need to ensure that all login attempts to the Azure portal from those countries require Azure Multi-Factor Authentication (MFA).

Solution: Create an Access Review for Group1.

Does this solution meet the goal?

A. Yes
B. No

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Instead implement Azure AD Privileged Identity Management.

Note: Azure Active Directory (Azure AD) Privileged Identity Management (PIM) is a service that enables you to manage, control, and monitor access to important resources in your organization.

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure

QUESTION 30
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have an Azure Active Directory (Azure AD) tenant named contoso.com. The tenant contains a group named Group1. Group1 contains all the administrative user accounts.

You discover several login attempts to the Azure portal from countries where administrative users do **NOT** work.

You need to ensure that all login attempts to the Azure portal from those countries require Azure Multi-Factor Authentication (MFA).

Solution: Implement Azure AD Identity Protection for Group1.

Does this solution meet the goal?

A. Yes
B. No

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Implement Azure AD Privileged Identity Management for everyone.

Note: Azure Active Directory (Azure AD) Privileged Identity Management (PIM) is a service that enables you to manage, control, and monitor access to important resources in your organization.

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure

QUESTION 31
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have an Azure Active Directory (Azure AD) tenant named contoso.com. The tenant contains a group named Group1. Group1 contains all the administrative user accounts.

You discover several login attempts to the Azure portal from countries where administrative users do **NOT** work.

You need to ensure that all login attempts to the Azure portal from those countries require Azure Multi-Factor Authentication (MFA).

Solution: You implement an access package.

Does this meet the goal?

A. Yes
B. No

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Instead implement Azure AD Privileged Identity Management.

Note: Azure Active Directory (Azure AD) Privileged Identity Management (PIM) is a service that enables you to manage, control, and monitor access to important resources in your organization.

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure

Design Data Storage

Question Set 1

QUESTION 1
You have 100 servers that run Windows Server 2012 R2 and host Microsoft SQL Server 2014 instances. The instances host databases that have the following characteristics:

- The largest database is currently 3 TB. None of the databases will ever exceed 4 TB.
- Stored procedures are implemented by using CLR.

You plan to move all the data from SQL Server to Azure.

You need to recommend an Azure service to host the databases. The solution must meet the following requirements:

- Whenever possible, minimize management overhead for the migrated databases.
- Minimize the number of database changes required to facilitate the migration.
- Ensure that users can authenticate by using their Active Directory credentials.

What should you include in the recommendation?

A. Azure SQL Database elastic pools
B. Azure SQL Database Managed Instance
C. Azure SQL Database single databases
D. SQL Server 2016 on Azure virtual machines

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference:
https://docs.microsoft.com/en-us/azure/sql-database/sql-database-managed-instance

QUESTION 2
You are designing an order processing system in Azure that will contain the Azure resources shown in the following table.

Name	Type	Purpose
App1	Web app	Processes customer orders
Function1	Function	Check product availability at vendor 1
Function2	Function	Check product availability at vendor 2
storage1	Storage account	Stores order processing logs

The order processing system will have the following transaction flow:

- A customer will place an order by using App1.
- When the order is received, App1 will generate a message to check for product availability at vendor 1 and vendor 2.
- An integration component will process the message, and then trigger either Function1 or Function2 depending on the type of order.
- Once a vendor confirms the product availability, a status message for App1 will be generated by Function1 or Function2.
- All the steps of the transaction will be logged to storage1.

Which type of resource should you recommend for the integration component?

A. an Azure Data Factory pipeline
B. an Azure Service Bus queue
C. an Azure Event Grid domain
D. an Azure Event Hubs capture

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A data factory can have one or more pipelines. A pipeline is a logical grouping of activities that together perform a task.

The activities in a pipeline define actions to perform on your data.

Data Factory has three groupings of activities: data movement activities, data transformation activities, and control activities.

Azure Functions is now integrated with Azure Data Factory, allowing you to run an Azure function as a step in your data factory pipelines.

Reference:
https://docs.microsoft.com/en-us/azure/data-factory/concepts-pipelines-activities

QUESTION 3
HOTSPOT

You have an existing implementation of Microsoft SQL Server Integration Services (SSIS) packages stored in an SSISDB catalog on your on-premises network. The on-premises network does not have hybrid connectivity to Azure by using Site-to-Site VPN or ExpressRoute.

You want to migrate the packages to Azure Data Factory.

You need to recommend a solution that facilitates the migration while minimizing changes to the existing packages. The solution must minimize costs.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Store the SSISDB catalog by using:

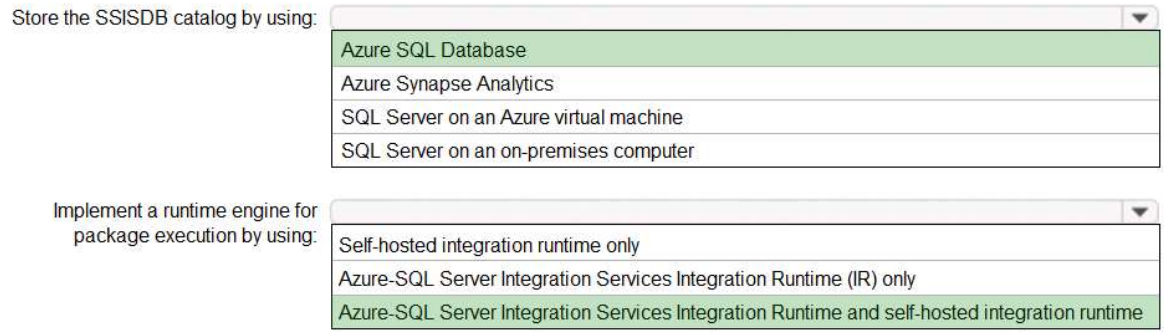
- Azure SQL Database
- Azure Synapse Analytics
- SQL Server on an Azure virtual machine
- SQL Server on an on-premises computer

Implement a runtime engine for package execution by using:

- Self-hosted integration runtime only
- Azure-SQL Server Integration Services Integration Runtime (IR) only
- Azure-SQL Server Integration Services Integration Runtime and self-hosted integration runtime

Correct Answer:

Answer Area



Section: (none)
Explanation

Explanation/Reference:
Explanation:

Box 1: Azure SQL database
You can't create the SSISDB Catalog database on Azure SQL Database at this time independently of creating the Azure-SSIS Integration Runtime in Azure Data Factory. The Azure-SSIS IR is the runtime environment that runs SSIS packages on Azure.

Box 2: Azure-SQL Server Integration Service Integration Runtime and self-hosted integration runtime

The Integration Runtime (IR) is the compute infrastructure used by Azure Data Factory to provide data integration capabilities across different network environments. Azure-SSIS Integration Runtime (IR) in Azure Data Factory (ADF) supports running SSIS packages.

Self-hosted integration runtime can be used for data movement in this scenario.

Reference:
https://docs.microsoft.com/en-us/azure/data-factory/create-azure-integration-runtime

https://docs.microsoft.com/en-us/sql/integration-services/lift-shift/ssis-azure-connect-to-catalog-database

QUESTION 4
You have 70 TB of files on your on-premises file server.

You need to recommend solution for importing data to Azure. The solution must minimize cost.

What Azure service should you recommend?

A. Azure StorSimple
B. Azure Batch
C. Azure Data Box
D. Azure Stack

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

Explanation:
Microsoft has engineered an extremely powerful solution that helps customers get their data to the Azure public cloud in a cost-effective, secure, and efficient manner with powerful Azure and machine learning at play. The solution is called Data Box.
Data Box and is in general availability status. It is a rugged device that allows organizations to have 100 TB of capacity on which to copy their data and then send it to be transferred to Azure.

Incorrect Answers:
A: StoreSimple would not be able to handle 70 TB of data.

Reference:
https://www.vembu.com/blog/what-is-microsoft-azure-data-box-disk-edge-heavy-gateway-overview/

QUESTION 5
You have an Azure subscription that contains 100 virtual machines.

You plan to design a data protection strategy to encrypt the virtual disks.

You need to recommend a solution to encrypt the disks by using Azure Disk Encryption. The solution must provide the ability to encrypt operating system disks and data disks.

What should you include in the recommendation?

A. a certificate
B. a key
C. a passphrase
D. a secret

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
For enhanced virtual machine (VM) security and compliance, virtual disks in Azure can be encrypted. Disks are encrypted by using cryptographic keys that are secured in an Azure Key Vault. You control these cryptographic keys and can audit their use.

Reference:
https://docs.microsoft.com/en-us/azure/virtual-machines/windows/encrypt-disks

QUESTION 6
You have data files in Azure Blob storage.

You plan to transform the files and move them to Azure Data Lake Storage.

You need to transform the data by using mapping data flow.

Which Azure service should you use?

A. Azure Data Box Gateway
B. Azure Storage Sync
C. Azure Data Factory
D. Azure Databricks

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
You can use Copy Activity in Azure Data Factory to copy data from and to Azure Data Lake Storage Gen2, and use Data Flow to transform data in Azure Data Lake Storage Gen2.

Reference:
https://docs.microsoft.com/en-us/azure/data-factory/connector-azure-data-lake-storage

QUESTION 7
You have an Azure virtual machine named VM1 that runs Windows Server 2019 and contains 500 GB of data files.

You are designing a solution that will use Azure Data Factory to transform the data files, and then load the files to Azure Data Lake Storage.

What should you deploy on VM1 to support the design?

A. the Azure Pipelines agent
B. the Azure File Sync agent
C. the On-premises data gateway
D. the self-hosted integration runtime in Azure

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The integration runtime (IR) is the compute infrastructure that Azure Data Factory uses to provide data-integration capabilities across different network environments. For details about IR, see Integration runtime overview.

A self-hosted integration runtime can run copy activities between a cloud data store and a data store in a private network. It also can dispatch transform activities against compute resources in an on-premises network or an Azure virtual network. The installation of a self-hosted integration runtime needs an on-premises machine or a virtual machine inside a private network.

Reference:
https://docs.microsoft.com/en-us/azure/data-factory/create-self-hosted-integration-runtime

QUESTION 8
HOTSPOT

Your company is designing a multi-tenant application that will use elastic pools and Azure SQL databases. The application will be used by 30 customers.

You need to design a storage solution for the application. The solution must meet the following requirements:

- Operational costs must be minimized.
- All customers must have their own database.
- The customer databases will be in one of the following three Azure regions: East US, North Europe, or South Africa North.

What is the minimum number of elastic pools and Azure SQL Database servers required? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Elastic pools:
- 1
- 3
- 6
- 10
- 30

Azure SQL Database servers:
- 1
- 3
- 6
- 10
- 30

Correct Answer:

Answer Area

Elastic pools:
- 1
- 3 ✓
- 6
- 10
- 30

Azure SQL Database servers:
- 1
- 3 ✓
- 6
- 10
- 30

Section: (none)
Explanation

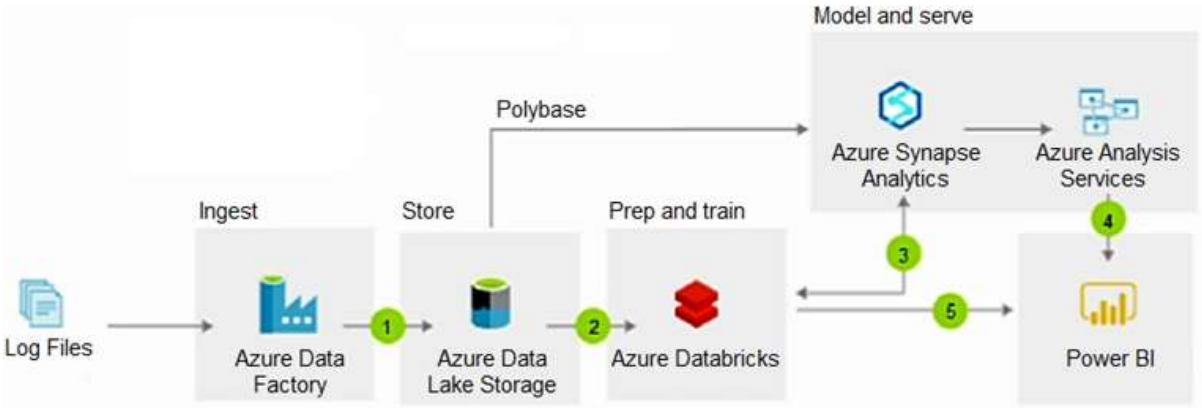
Explanation/Reference:
Explanation:

Box 1: 3
The server, its pools & databases must be in the same Azure region under the same subscription.

Box 2: 3
A server can have up to 5000 databases associated to it.

Reference:
https://vincentlauzon.com/2016/12/18/azure-sql-elastic-pool-overview/

QUESTION 9
You are reviewing an Azure architecture as shown in the Architecture exhibit. (Click the **Architecture** tab.)



The estimated monthly costs for the architecture are shown in the Costs exhibit. (Click the **Costs** tab.)

Estimate total: US$7,739.99

Azure Synapse Analytics	Tier: Compute-optimised Gen2, Compute: DWU 100 x 1 ...	US$998.88
Data Factory	Azure Data Factory V2 Type, Data Pipeline Service type, ...	US$4,993.14
Azure Analysis Services	Developer (hours), 5 Instance(s), 720 Hours	US$475.20
Power BI Embedded	1 node(s) x 1 Months, Node type: A1, 1 Virtual Core(s), 3...	US$735.91
Storage Accounts	Block Blob Storage, General Purpose V2, LRS Redundan...	US$21.84
Azure Databricks	Data Analytics Workload, Premium Tier, 1 D3V2 (4 vCPU...	US$515.02

The log files are generated by user activity to Apache web servers. The log files are in a consistent format. Approximately 1 GB of logs are generated per day. Microsoft Power BI is used to display weekly reports of the user activity.

You need to recommend a solution to minimize costs while maintaining the functionality of the architecture.

What should you recommend?

A. Replace Azure Synapse Analytics and Azure Analysis Services with SQL Server on an Azure virtual machine.
B. Replace Azure Synapse Analytics with Azure SQL Database Hyperscale.

C. Replace Azure Data Factory with CRON jobs that use AzCopy.
D. Replace Azure Databricks with Azure Machine Learning.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
AzCopy is a command-line utility that you can use to copy blobs or files to or from a storage account.

Cron is one of the most useful utility that you can find in any Unix-like operating system. It is used to schedule commands at a specific time. These scheduled commands or tasks are known as "Cron Jobs".

Reference:
https://docs.microsoft.com/en-us/azure/storage/common/storage-use-azcopy-configure

QUESTION 10
You deploy Azure App Service Web Apps that connect to on-premises Microsoft SQL Server instances by using Azure ExpressRoute. You plan to migrate the SQL Server instances to Azure.

Migration of the SQL Server instances to Azure must:

- Support automatic patching and version updates to SQL Server.
- Provide automatic backup services.
- Allow for high-availability of the instances.
- Provide a native VNET with private IP addressing.
- Encrypt all data in transit.
- Be in a single-tenant environment with dedicated underlying infrastructure (compute, storage).

You need to migrate the SQL Server instances to Azure.

Which Azure service should you use?

A. SQL Server in a Docker container running on Azure Container Instances (ACI)
B. SQL Server in Docker containers running on Azure Kubernetes Service (AKS)
C. SQL Server Infrastructure-as-a-Service (IaaS) virtual machine (VM)
D. Azure SQL Database Managed Instance
E. Azure SQL Database with elastic pools

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Azure SQL Database Managed Instance configured for Hybrid workloads. Use this topology if your Azure SQL Database Managed Instance is connected to your on-premises network. This approach provides the most simplified network routing and yields maximum data throughput during the migration.

Reference:
https://docs.microsoft.com/en-us/azure/dms/resource-network-topologies

QUESTION 11
You plan to store data in Azure Blob storage for many years. The stored data will be accessed rarely.

You need to ensure that the data in Blob storage is always available for immediate access. The solution must minimize storage costs.

Which storage tier should you use?

A. Cool
B. Archive
C. Hot

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Data in the cool access tier can tolerate slightly lower availability, but still requires high durability, retrieval latency, and throughput characteristics similar to hot data. For cool data, a slightly lower availability service-level agreement (SLA) and higher access costs compared to hot data are acceptable trade-offs for lower storage costs.

Incorrect Answers:
B: Archive storage stores data offline and offers the lowest storage costs but also the highest data rehydrate and access costs.
Archive - Optimized for storing data that is rarely accessed and stored for at least 180 days with flexible latency requirements (on the order of hours).

Reference:
https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blob-storage-tiers

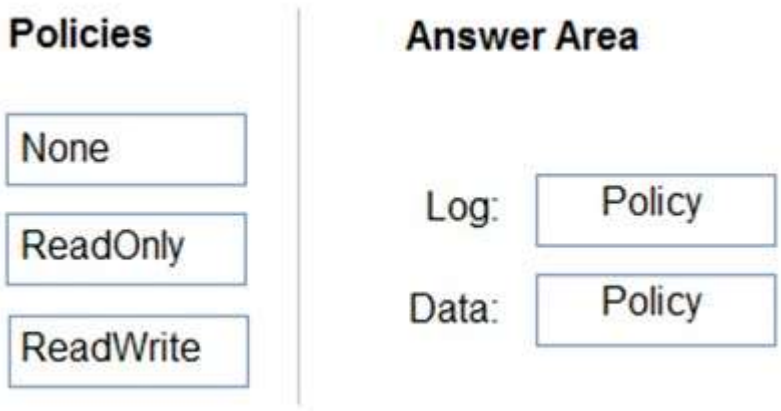
QUESTION 12
DRAG DROP

You are designing a virtual machine that will run Microsoft SQL Server and will contain two data disks. The first data disk will store log files, and the second data disk will store data. Both disks are P40 managed disks.

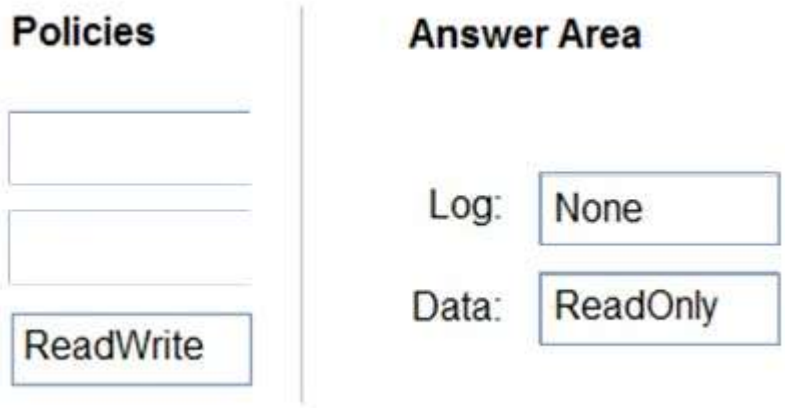
You need to recommend a caching policy for each disk. The policy must provide the best overall performance for the virtual machine while preserving integrity of the SQL data and logs.

Which caching policy should you recommend for each disk? To answer, drag the appropriate policies to the correct disks. Each policy 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.

Select and Place:



Correct Answer:



Section: (none)
Explanation

Explanation/Reference:
Reference:
https://docs.microsoft.com/en-us/azure/virtual-machines/windows/sql/virtual-machines-windows-sql-performance

QUESTION 13
You are designing a SQL database solution. The solution will include 20 databases that will be 20 GB each and have varying usage patterns.

You need to recommend a database platform to host the databases. The solution must meet the following requirements:

- The compute resources allocated to the databases must scale dynamically.
- The solution must meet an SLA of 99.99% uptime.
- The solution must have reserved capacity.
- Compute charges must be minimized.

What should you include in the recommendation?

A. 20 databases on a Microsoft SQL server that runs on an Azure virtual machine in an availability set
B. 20 instances of Azure SQL Database serverless
C. 20 databases on a Microsoft SQL server that runs on an Azure virtual machine
D. an elastic pool that contains 20 Azure SQL databases

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Azure SQL Database elastic pools are a simple, cost-effective solution for managing and scaling multiple databases that have varying and unpredictable usage demands. The databases in an elastic pool are on a single server and share a set number of resources at a set price. Elastic pools in Azure SQL Database enable SaaS developers to optimize the price performance for a group of databases within a prescribed budget while delivering performance elasticity for each database.

Guaranteed 99.995 percent uptime for SQL Database

Reference:
https://docs.microsoft.com/en-us/azure/azure-sql/database/elastic-pool-overview

https://azure.microsoft.com/en-us/pricing/details/sql-database/elastic/

QUESTION 14
You have an app named App1 that uses two on-premises Microsoft SQL Server databases named DB1 and DB2.

You plan to migrate DB1 and DB2 to Azure.

You need to recommend an Azure solution to host DB1 and DB2. The solution must meet the following requirements:

- Support server-side transactions across DB1 and DB2.
- Minimize administrative effort to update the solution.

What should you recommend?

A. two Azure SQL databases in an elastic pool
B. two Azure SQL databases on different Azure SQL Database servers
C. two Azure SQL databases on the same Azure SQL Database managed instance
D. two SQL Server databases on an Azure virtual machine

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
SQL Managed Instance enables system administrators to spend less time on administrative tasks because the service either performs them for you or greatly simplifies those tasks.

Note: Azure SQL Managed Instance is designed for customers looking to migrate a large number of apps from an on-premises or IaaS, self-built, or ISV provided environment to a fully managed PaaS cloud environment, with as low a migration effort as possible. Using the fully automated Azure Data Migration Service, customers can lift and shift their existing SQL Server instance to SQL Managed Instance, which offers compatibility with SQL Server and complete isolation of customer instances with native VNet support. With Software Assurance, you can exchange your existing licenses for discounted rates on SQL Managed Instance using the Azure Hybrid Benefit for SQL Server. SQL Managed Instance is the best migration destination in the cloud for SQL Server instances that require high security and a rich programmability surface.

Reference:
https://docs.microsoft.com/en-us/azure/azure-sql/managed-instance/sql-managed-instance-paas-overview

Design Data Storage

Testlet 2

Case Study

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

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

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

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

Overview

Contoso, Ltd, is a US-based financial services company that has a main office in New York and a branch office in San Francisco.

Existing Environment. Payment Processing System

Contoso hosts a business-critical payment processing system in its New York data center. The system has three tiers: a front-end web app, a middle-tier web API, and a back-end data store implemented as a Microsoft SQL Server 2014 database. All servers run Windows Server 2012 R2.

The front-end and middle-tier components are hosted by using Microsoft Internet Information Services (IIS). The application code is written in C# and ASP.NET. The middle-tier API uses the Entity Framework to communicate to the SQL Server database. Maintenance of the database is performed by using SQL Server Agent jobs.

The database is currently 2 TB and is not expected to grow beyond 3 TB.

The payment processing system has the following compliance-related requirements:

- Encrypt data in transit and at rest. Only the front-end and middle-tier components must be able to access the encryption keys that protect the data store.
- Keep backups of the data in two separate physical locations that are at least 200 miles apart and can be restored for up to seven years.
- Support blocking inbound and outbound traffic based on the source IP address, the destination IP address, and the port number.
- Collect Windows security logs from all the middle-tier servers and retain the logs for a period of seven years.
- Inspect inbound and outbound traffic from the front-end tier by using highly available network appliances.
- Only allow all access to all the tiers from the internal network of Contoso.

Tape backups are configured by using an on-premises deployment of Microsoft System Center Data Protection Manager (DPM), and then shipped offsite for long term storage.

Existing Environment. Historical Transaction Query System

Contoso recently migrated a business-critical workload to Azure. The workload contains a .NET web service for querying the historical transaction data residing in Azure Table Storage. The .NET web service is accessible from a client app that was developed in-house and runs on the client computers in the New York office. The data in the table storage is 50 GB and is not expected to increase.

Existing Environment. Current Issues

The Contoso IT team discovers poor performance of the historical transaction query system, as the queries frequently cause table scans.

Requirements. Planned Changes

Contoso plans to implement the following changes:

- Migrate the payment processing system to Azure.
- Migrate the historical transaction data to Azure Cosmos DB to address the performance issues.

Requirements. Migration Requirements

Contoso identifies the following general migration requirements:

- Infrastructure services must remain available if a region or a data center fails. Failover must occur without any administrative intervention.
- Whenever possible, Azure managed services must be used to minimize management overhead.
- Whenever possible, costs must be minimized.

Contoso identifies the following requirements for the payment processing system:

- If a data center fails, ensure that the payment processing system remains available without any administrative intervention. The middle-tier and the web front end must continue to operate without any additional configurations.
- Ensure that the number of compute nodes of the front-end and the middle tiers of the payment processing system can increase or decrease automatically based on CPU utilization.
- Ensure that each tier of the payment processing system is subject to a Service Level Agreement (SLA) of 99.99 percent availability.
- Minimize the effort required to modify the middle-tier API and the back-end tier of the payment processing system.
- Payment processing system must be able to use grouping and joining tables on encrypted columns.
- Generate alerts when unauthorized login attempts occur on the middle-tier virtual machines.
- Ensure that the payment processing system preserves its current compliance status.
- Host the middle tier of the payment processing system on a virtual machine

Contoso identifies the following requirements for the historical transaction query system:

- Minimize the use of on-premises infrastructure services.
- Minimize the effort required to modify the .NET web service querying Azure Cosmos DB.
- Minimize the frequency of table scans.
- If a region fails, ensure that the historical transaction query system remains available without any administrative intervention.

Requirements. Information Security Requirements

The IT security team wants to ensure that identity management is performed by using Active Directory. Password hashes must be stored on-premises only.

Access to all business-critical systems must rely on Active Directory credentials. Any suspicious authentication attempts must trigger a multi-factor authentication prompt automatically.

QUESTION 1
You need to recommend a solution for protecting the content of the payment processing system.

What should you include in the recommendation?

A. Always Encrypted with deterministic encryption
B. Always Encrypted with randomized encryption
C. Transparent Data Encryption (TDE)
D. Azure Storage Service Encryption

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
HOTSPOT

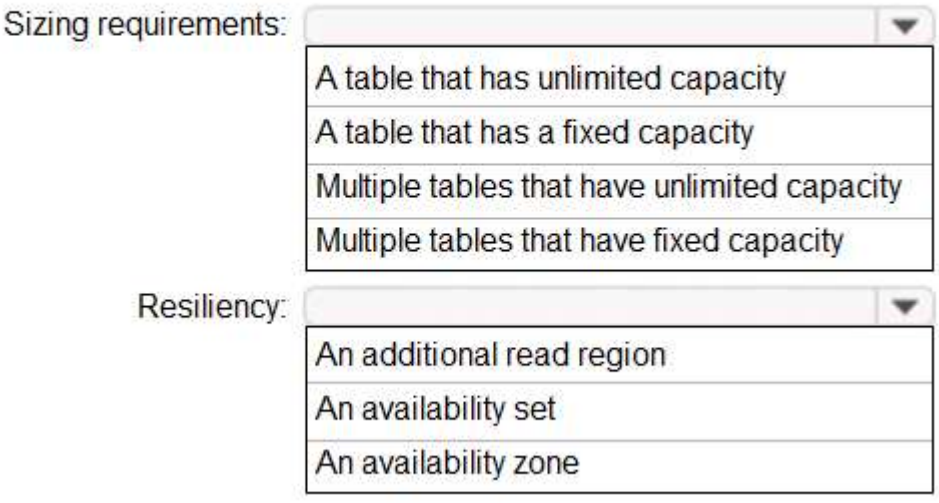
You need to recommend a solution for the data store of the historical transaction query system.

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

NOTE: Each correct selection is worth one point.

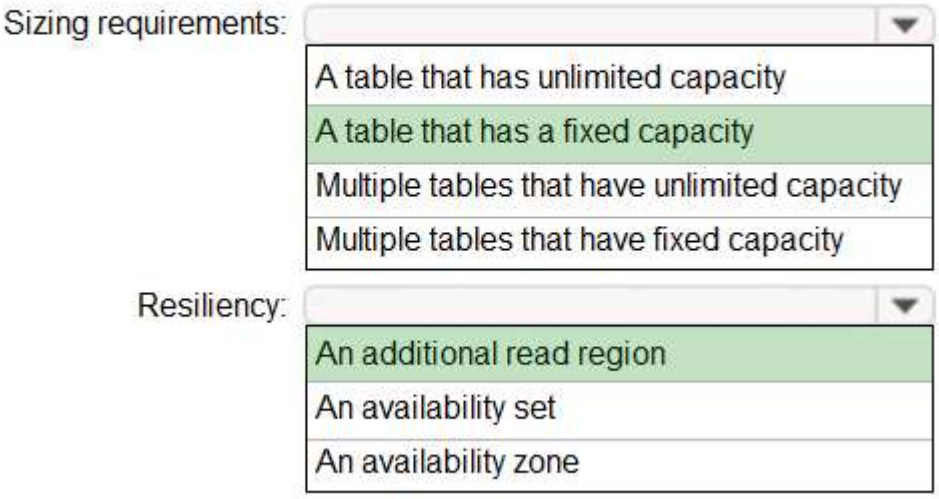
Hot Area:

Answer Area



Correct Answer:

Answer Area



Section: (none)
Explanation

Explanation/Reference:

Design Business Continuity

Question Set 1

QUESTION 1
Your company purchases an app named App1.

You plan to run App1 on seven Azure virtual machines in an Availability Set. The number of fault domains is set to 3. The number of update domains is set to 20.

You need to identify how many App1 instances will remain available during a period of planned maintenance.

How many App1 instances should you identify?

A. 1
B. 2
C. 6
D. 7

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Only one update domain is rebooted at a time. Here there are 7 update domain with one VM each (and 13 update domain with no VM).

Reference:
https://docs.microsoft.com/en-us/azure/virtual-machines/windows/manage-availability

QUESTION 2
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have an Azure Storage v2 account named storage1.

You plan to archive data to storage1.

You need to ensure that the archived data cannot be deleted for five years. The solution must prevent administrators from deleting the data.

Solution: You create an Azure Blob storage container, and you configure a legal hold access policy.

Does this meet the goal?

A. Yes
B. No

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

Explanation:
Use an Azure Blob storage container, but use a time-based retention policy instead of a legal hold.

Note:
Immutable storage for Azure Blob storage enables users to store business-critical data objects in a WORM (Write Once, Read Many) state. This state makes the data non-erasable and non-modifiable for a user-specified interval. For the duration of the retention interval, blobs can be created and read, but cannot be modified or deleted. Immutable storage is available for general-purpose v2 and Blob storage accounts in all Azure regions.

Note: Set retention policies and legal holds

1. Create a new container or select an existing container to store the blobs that need to be kept in the immutable state. The container must be in a general-purpose v2 or Blob storage account.

2. Select Access policy in the container settings. Then select Add policy under Immutable blob storage.

Either

3a. To enable legal holds, select Add Policy. Select Legal hold from the drop-down menu.

Or
3b. To enable time-based retention, select Time-based retention from the drop-down menu.

4. Enter the retention interval in days (acceptable values are 1 to 146000 days).

Reference:
https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blob-immutable-storage

https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blob-immutability-policies-manage

QUESTION 3
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have an Azure Storage v2 account named storage1.

You plan to archive data to storage1.

You need to ensure that the archived data cannot be deleted for five years. The solution must prevent administrators from deleting the data.

Solution: You create a file share and snapshots.

Does this meet the goal?

A. Yes
B. No

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Instead you could create an Azure Blob storage container, and you configure a legal hold access policy.

Reference:
https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blob-immutable-storage

QUESTION 4
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have an Azure Storage v2 account named storage1.

You plan to archive data to storage1.

You need to ensure that the archived data cannot be deleted for five years. The solution must prevent administrators from deleting the data.

Solution: You create a file share, and you configure an access policy.

Does this meet the goal?

A. Yes
B. No

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Instead of a file share, an immutable Blob storage is required.

Time-based retention policy support: Users can set policies to store data for a specified interval. When a time-based retention policy is set, blobs can be created and read, but not modified or deleted. After the retention period has expired, blobs can be deleted but not overwritten.

Note: Set retention policies and legal holds

1. Create a new container or select an existing container to store the blobs that need to be kept in the immutable state. The container must be in a general-purpose v2 or Blob storage account.

2. Select Access policy in the container settings. Then select Add policy under Immutable blob storage.

3. To enable time-based retention, select Time-based retention from the drop-down menu.

4. Enter the retention interval in days (acceptable values are 1 to 146000 days).

Reference:
https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blob-immutable-storage

https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blob-immutability-policies-manage

QUESTION 5
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have an on-premises Hyper-V cluster that hosts 20 virtual machines. Some virtual machines run Windows Server 2016 and some run Linux.

You plan to migrate the virtual machines to an Azure subscription.

You need to recommend a solution to replicate the disks of the virtual machines to Azure. The solution must ensure that the virtual machines remain available during the migration of the disks.

Solution: You recommend implementing an Azure Storage account, and then running `AzCopy`.

Does this meet the goal?

A. Yes
B. No

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
AzCopy only copy files, not the disks.
Instead use Azure Site Recovery.

Reference:
https://docs.microsoft.com/en-us/azure/site-recovery/site-recovery-overview

QUESTION 6
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have an on-premises Hyper-V cluster that hosts 20 virtual machines. Some virtual machines run Windows Server 2016 and some run Linux.

You plan to migrate the virtual machines to an Azure subscription.

You need to recommend a solution to replicate the disks of the virtual machines to Azure. The solution must ensure that the virtual machines remain available during the migration of the disks.

Solution: You recommend implementing an Azure Storage account that has a file service and a blob service, and then using the Data Migration Assistant.

Does this meet the goal?

A. Yes
B. No

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Data Migration Assistant is used to migrate SQL databases.
Instead use Azure Site Recovery.

Reference:
https://docs.microsoft.com/en-us/azure/site-recovery/site-recovery-overview

QUESTION 7
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have an on-premises Hyper-V cluster that hosts 20 virtual machines. Some virtual machines run Windows Server 2016 and some run Linux.

You plan to migrate the virtual machines to an Azure subscription.

You need to recommend a solution to replicate the disks of the virtual machines to Azure. The solution must ensure that the virtual machines remain available during the migration of the disks.

Solution: You recommend implementing a Recovery Services vault, and then using Azure Site Recovery.

Does this meet the goal?

A. Yes
B. No

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Site Recovery can replicate on-premises VMware VMs, Hyper-V VMs, physical servers (Windows and Linux), Azure Stack VMs to Azure.

Note: Site Recovery helps ensure business continuity by keeping business apps and workloads running during outages. Site Recovery replicates workloads running on physical and virtual machines (VMs) from a primary site to a secondary location. When an outage occurs at your primary site, you fail over to secondary location, and access apps from there. After the primary location is running again, you can fail back to it.

Reference:
https://docs.microsoft.com/en-us/azure/site-recovery/site-recovery-overview

QUESTION 8
You are designing a storage solution that will use Azure Blob storage. The data will be stored in a cool access tier or an archive access tier based on the access patterns of the data.

You identify the following types of infrequently accessed data:

- Telemetry data: Deleted after two years
- Promotional material: Deleted after 14 days
- Virtual machine audit data: Deleted after 200 days

A colleague recommends using the archive access tier to store the data.

Which statement accurately describes the recommendation?

A. Storage costs will be based on a minimum of 30 days.
B. Access to the data is guaranteed within five minutes.
C. Access to the data is guaranteed within 30 minutes.
D. Storage costs will be based on a minimum of 180 days.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The following table shows a comparison of premium performance block blob storage, and the hot, cool, and archive access tiers.

	Premium performance	Hot tier	Cool tier	Archive tier
Availability	99.9%	99.9%	99%	Offline
Availability (RA-GRS reads)	N/A	99.99%	99.9%	Offline
Usage charges	Higher storage costs, lower access, and transaction cost	Higher storage costs, lower access, and transaction costs	Lower storage costs, higher access, and transaction costs	Lowest storage costs, highest access, and transaction costs
Minimum object size	N/A	N/A	N/A	N/A
Minimum storage duration	N/A	N/A	30 days[1]	180 days
Latency (Time to first byte)	Single-digit milliseconds	milliseconds	milliseconds	hours[2]

Reference:
https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blob-storage-tiers

QUESTION 9

You are planning to deploy an application named App1 that will run in containers on Azure Kubernetes Service (AKS) clusters. The AKS clusters will be distributed across four Azure regions.

You need to recommend a storage solution for App1. Updated container images must be replicated automatically to all the AKS clusters.

Which storage solution should you recommend?

A. Azure Cache for Redis
B. Azure Content Delivery Network (CDN)
C. Premium SKU Azure Container Registry
D. geo-redundant storage (GRS) accounts

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Enable geo-replication for container images.
Best practice: Store your container images in Azure Container Registry and geo-replicate the registry to each AKS region.

To deploy and run your applications in AKS, you need a way to store and pull the container images. Container Registry integrates with AKS, so it can securely store your container images or Helm charts. Container Registry supports multimaster geo-replication to automatically replicate your images to Azure regions around the world.

Geo-replication is a feature of Premium SKU container registries.

Note:
When you use Container Registry geo-replication to pull images from the same region, the results are:

Faster: You pull images from high-speed, low-latency network connections within the same Azure region.
More reliable: If a region is unavailable, your AKS cluster pulls the images from an available container registry.
Cheaper: There's no network egress charge between datacenters.

Reference:
https://docs.microsoft.com/en-us/azure/aks/operator-best-practices-multi-region

QUESTION 10
You have an on-premises network and an Azure subscription. The on-premises network has several branch offices.

A branch office in Toronto contains a virtual machine named VM1 that is configured as a file server. Users access the shared files on VM1 from all the offices.

You need to recommend a solution to ensure that the users can access the shared files as quickly as possible if the Toronto branch office is inaccessible.

What should you include in the recommendation?

A. an Azure file share and Azure File Sync
B. a Recovery Services vault and Windows Server Backup
C. a Recovery Services vault and Azure Backup
D. Azure blob containers and Azure File Sync

Correct Answer: A
Section: (none)

Explanation

Explanation/Reference:
Explanation:
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 need an Azure file share in the same region that you want to deploy Azure File Sync.

Incorrect Answer:
C: Backups would be a slower solution.

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

QUESTION 11
DRAG DROP

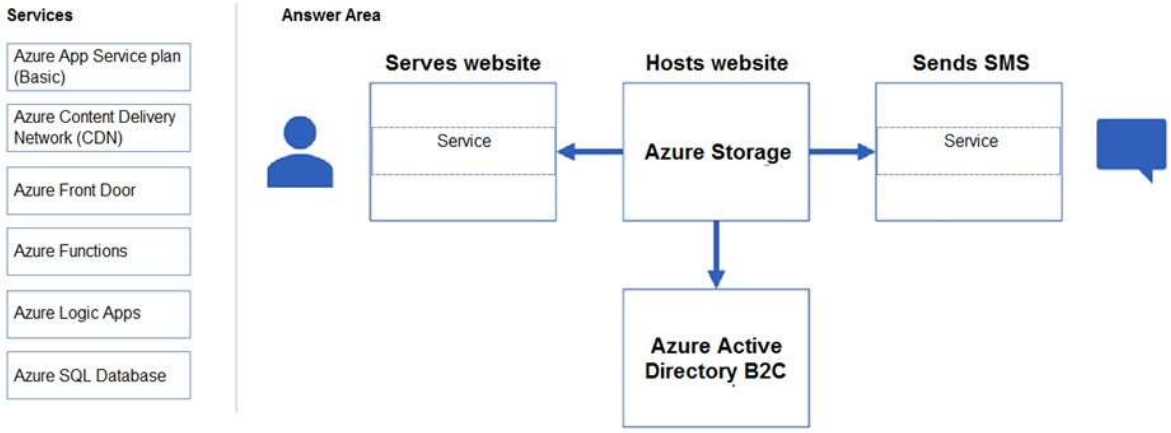
The developers at your company are building a static web app to support users sending text messages. The app must meet the following requirements:

- Website latency must be consistent for users in different geographical regions.
- Users must be able to authenticate by using Twitter and Facebook.
- Code must include only HTML, native JavaScript, and jQuery.
- Costs must be minimized.

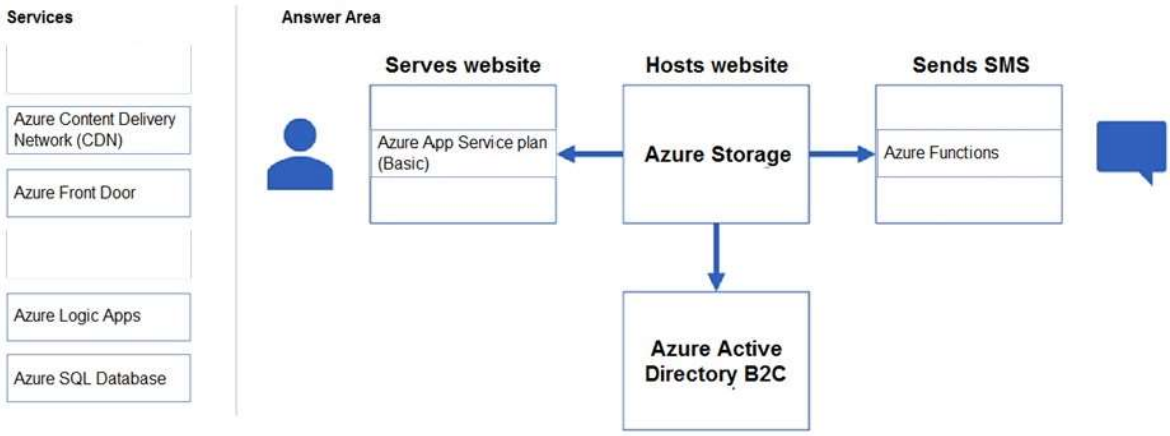
Which Azure service should you use to complete the architecture? To answer, drag the appropriate services to the correct locations. Each service may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:



Correct Answer:



Section: (none)
Explanation

Explanation/Reference:
Explanation:

Box 1: Azure App Service plan (Basic)
With App Service you can authenticate your customers with Azure Active Directory, and integrate with Facebook, Twitter, Google.

Box 2: Azure Functions
You can send SMS messages with Azure Functions with Javascript.

Reference:
https://docs.microsoft.com/en-us/azure/active-directory-b2c/partner-whoiam

https://www.codeproject.com/Articles/1368337/Implementing-SMS-API-using-Azure-Serverless-Functi

QUESTION 12
You need to design a highly available Azure SQL database that meets the following requirements:

- Failover between replicas of the database must occur without any data loss.
- The database must remain available in the event of a zone outage.
- Costs must be minimized.

Which deployment option should you use?

A. Azure SQL Database Standard
B. Azure SQL Database Business Critical
C. Azure SQL Database Managed Instance Business Critical
D. Azure SQL Database Basic

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Standard geo-replication is available with Standard and Premium databases in the current Azure Management Portal and standard APIs.

Incorrect:
Not B: Business Critical service tier is designed for applications that require low-latency responses from the

underlying SSD storage (1-2 ms in average), fast recovery if the underlying infrastructure fails, or need to off-load reports, analytics, and read-only queries to the free of charge readable secondary replica of the primary database.

Note: Azure SQL Database and Azure SQL Managed Instance are both based on SQL Server database engine architecture that is adjusted for the cloud environment in order to ensure 99.99% availability even in the cases of infrastructure failures. There are three architectural models that are used:

- General Purpose/Standard
- Business Critical/Premium
- Hyperscale

Reference:
https://docs.microsoft.com/en-us/azure/azure-sql/database/service-tier-business-critical

QUESTION 13
DRAG DROP

Your company identifies the following business continuity and disaster recovery objectives for virtual machines that host sales, finance, and reporting applications in the company's on-premises data center:

- The sales application must be able to fail over to a second on-premises data center.
- The finance application requires that data be retained for seven years. In the event of a disaster, the application must be able to run from Azure. The recovery time objective (RTO) is 10 minutes.
- The reporting application must be able to recover point-in-time data at a daily granularity. The RTO is eight hours.

You need to recommend which Azure services meet the business continuity and disaster recovery objectives. The solution must minimize costs.

What should you recommend for each application? To answer, drag the appropriate services to the correct applications. 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.

Select and Place:

Correct Answer:

Section: (none)
Explanation

Explanation/Reference:

QUESTION 14
You have an Azure Storage v2 account named storage1.

You plan to archive data to storage1.

You need to ensure that the archived data cannot be deleted for five years. The solution must prevent administrators from deleting the data.

What should you do?

A. You create an Azure Blob storage container, and you configure a legal hold access policy.
B. You create a file share and snapshots.
C. You create a file share, and you configure an access policy.
D. You create an Azure Blob storage container, and you configure a time-based retention policy and lock the policy.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Time-based retention policy support: Users can set policies to store data for a specified interval. When a time-based retention policy is set, blobs can be created and read, but not modified or deleted. After the retention period has expired, blobs can be deleted but not overwritten.

Note:
Immutable storage for Azure Blob storage enables users to store business-critical data objects in a WORM (Write Once, Read Many) state. This state makes the data non-erasable and non-modifiable for a user-specified interval. For the duration of the retention interval, blobs can be created and read, but cannot be modified or deleted. Immutable storage is available for general-purpose v2 and Blob storage accounts in all Azure regions.

Reference:

https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blob-immutable-storage

Design Business Continuity

Testlet 2

Case Study

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

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

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

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

Overview

Contoso, Ltd, is a US-based financial services company that has a main office in New York and a branch office in San Francisco.

Existing Environment. Payment Processing System

Contoso hosts a business-critical payment processing system in its New York data center. The system has three tiers: a front-end web app, a middle-tier web API, and a back-end data store implemented as a Microsoft SQL Server 2014 database. All servers run Windows Server 2012 R2.

The front-end and middle-tier components are hosted by using Microsoft Internet Information Services (IIS). The application code is written in C# and ASP.NET. The middle-tier API uses the Entity Framework to communicate to the SQL Server database. Maintenance of the database is performed by using SQL Server Agent jobs.

The database is currently 2 TB and is not expected to grow beyond 3 TB.

The payment processing system has the following compliance-related requirements:

- Encrypt data in transit and at rest. Only the front-end and middle-tier components must be able to access the encryption keys that protect the data store.
- Keep backups of the data in two separate physical locations that are at least 200 miles apart and can be restored for up to seven years.
- Support blocking inbound and outbound traffic based on the source IP address, the destination IP address, and the port number.
- Collect Windows security logs from all the middle-tier servers and retain the logs for a period of seven years.
- Inspect inbound and outbound traffic from the front-end tier by using highly available network appliances.
- Only allow all access to all the tiers from the internal network of Contoso.

Tape backups are configured by using an on-premises deployment of Microsoft System Center Data Protection Manager (DPM), and then shipped offsite for long term storage.

Existing Environment. Historical Transaction Query System

Contoso recently migrated a business-critical workload to Azure. The workload contains a .NET web service for querying the historical transaction data residing in Azure Table Storage. The .NET web service is accessible from a client app that was developed in-house and runs on the client computers in the New York office. The data in the table storage is 50 GB and is not expected to increase.

Existing Environment. Current Issues

The Contoso IT team discovers poor performance of the historical transaction query system, as the queries frequently cause table scans.

Requirements. Planned Changes

Contoso plans to implement the following changes:

- Migrate the payment processing system to Azure.
- Migrate the historical transaction data to Azure Cosmos DB to address the performance issues.

Requirements. Migration Requirements

Contoso identifies the following general migration requirements:

- Infrastructure services must remain available if a region or a data center fails. Failover must occur without any administrative intervention.
- Whenever possible, Azure managed services must be used to minimize management overhead.
- Whenever possible, costs must be minimized.

Contoso identifies the following requirements for the payment processing system:

- If a data center fails, ensure that the payment processing system remains available without any administrative intervention. The middle-tier and the web front end must continue to operate without any additional configurations.
- Ensure that the number of compute nodes of the front-end and the middle tiers of the payment processing system can increase or decrease automatically based on CPU utilization.
- Ensure that each tier of the payment processing system is subject to a Service Level Agreement (SLA) of 99.99 percent availability.
- Minimize the effort required to modify the middle-tier API and the back-end tier of the payment processing system.
- Payment processing system must be able to use grouping and joining tables on encrypted columns.
- Generate alerts when unauthorized login attempts occur on the middle-tier virtual machines.
- Ensure that the payment processing system preserves its current compliance status.
- Host the middle tier of the payment processing system on a virtual machine

Contoso identifies the following requirements for the historical transaction query system:

- Minimize the use of on-premises infrastructure services.
- Minimize the effort required to modify the .NET web service querying Azure Cosmos DB.
- Minimize the frequency of table scans.
- If a region fails, ensure that the historical transaction query system remains available without any administrative intervention.

Requirements. Information Security Requirements

The IT security team wants to ensure that identity management is performed by using Active Directory. Password hashes must be stored on-premises only.

Access to all business-critical systems must rely on Active Directory credentials. Any suspicious authentication attempts must trigger a multi-factor authentication prompt automatically.

QUESTION 1
You need to recommend a backup solution for the data store of the payment processing system.

What should you include in the recommendation?

A. Microsoft System Center Data Protection Manager (DPM)
B. Azure Backup Server
C. Azure SQL long-term backup retention
D. Azure Managed Disks

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference:
https://docs.microsoft.com/en-us/azure/sql-database/sql-database-long-term-backup-retention-configure

Design Business Continuity

Testlet 3

Case Study

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

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

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

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

Overview

Fabricam, 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.

Existing Environment. Network Infrastructure

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

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

An existing application named WebApp1 is hosted in the data center of the London office. WebApp1 is used by customers to place and track orders. WebApp1 has a web tier that uses Microsoft Internet Information Services (IIS) and a database tier that runs Microsoft SQL Server 2016. The web tier and the database tier are deployed to virtual machines that run on Hyper-V.

The IT department currently uses a separate Hyper-V environment to test updates to WebApp1.

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

Existing Environment. Problem Statements

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

Requirements. Planned Changes

Fabrikam plans to move most of its production workloads to Azure during the next few years.

As one of its first projects, the company plans to establish a hybrid identity model, facilitating an upcoming Microsoft Office 365 deployment.

All R&D operations will remain on-premises.

Fabrikam plans to migrate the production and test instances of WebApp1 to Azure and to use the S1 plan.

Requirements. Technical Requirements

Fabrikam identifies the following technical requirements:

- Web site content must be easily updated from a single point.
- User input must be minimized when provisioning new 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.
- Directory synchronization between Azure Active Directory (Azure AD) and corp.fabrikam.com must not be affected by a link failure between Azure and the on-premises network.

Requirements. Database Requirements

Fabrikam identifies the following database requirements:

- Database metrics for the production instance of WebApp1 must be available for analysis so that database administrators can optimize the performance settings.
- To avoid disrupting customer access, database downtime must be minimized when databases are migrated.
- Database backups must be retained for a minimum of seven years to meet compliance requirements.

Requirements. Security Requirements

Fabrikam identifies the following security requirements:

- Company information including policies, templates, and data must be inaccessible to anyone outside the company.
- Users on the on-premises network must be able to authenticate to corp.fabrikam.com if an Internet link fails.
- Administrators must be able authenticate to the Azure portal by using their corp.fabrikam.com credentials.
- All administrative access to the Azure portal must be secured by using multi-factor authentication.
- The testing of WebApp1 updates must not be visible to anyone outside the company.

QUESTION 1
You need to recommend a solution to meet the database retention requirement.

What should you recommend?

A. Configure geo-replication of the database.

B. Configure a long-term retention policy for the database.
C. Configure Azure Site Recovery.
D. Use automatic Azure SQL Database backups.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

Design Infrastructure

Question Set 1

QUESTION 1
You deploy two instances of an Azure web app. One instance is in the East US Azure region and the other instance is in the West US Azure region. The web app uses Azure Blob storage to deliver large files to end users.

You need to recommend a solution for delivering the files to the users. The solution must meet the following requirements:

- Ensure that the users receive files from the same region as the web app that they access.
- Ensure that the files only need to be uploaded once.
- Minimize costs.

What should you include in the recommendation?

A. Distributed File System (DFS)
B. read-access geo-redundant storage (RA-GRS)
C. Azure File Sync
D. geo-redundant storage (GRS)

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
You are developing a web application that provides streaming video to users. You configure the application to use continuous integration and deployment.

The app must be highly available and provide a continuous streaming experience for users.

You need to recommend a solution that allows the application to store data in a geographical location that is closest to the user.

What should you recommend?

A. Azure Content Delivery Network (CDN)
B. Azure Redis Cache
C. Azure App Service Web Apps
D. Azure App Service Isolated

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Azure Content Delivery Network (CDN) is a global CDN solution for delivering high-bandwidth content. It can be hosted in Azure or any other location. With Azure CDN, you can cache static objects loaded from Azure Blob storage, a web application, or any publicly accessible web server, by using the closest point of presence (POP) server. Azure CDN can also accelerate dynamic content, which cannot be cached, by leveraging various network and routing optimizations.

Reference:
https://docs.microsoft.com/en-in/azure/cdn/

QUESTION 3
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You need to deploy resources to host a stateless web app in an Azure subscription. The solution must meet the following requirements:

- Provide access to the full .NET framework.
- Provide redundancy if an Azure region fails.
- Grant administrators access to the operating system to install custom application dependencies.

Solution: You deploy a virtual machine scale set that uses autoscaling.

Does this meet the goal?

A. Yes
B. No

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Instead, you should deploy two Azure virtual machines to two Azure regions, and you create a Traffic Manager profile.

QUESTION 4
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You need to deploy resources to host a stateless web app in an Azure subscription. The solution must meet the following requirements:

- Provide access to the full .NET framework.
- Provide redundancy if an Azure region fails.
- Grant administrators access to the operating system to install custom application dependencies.

Solution: You deploy two Azure virtual machines to two Azure regions, and you deploy an Azure Application Gateway.

Does this meet the goal?

A. Yes
B. No

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
You need to deploy two Azure virtual machines to two Azure regions, but also create a Traffic Manager profile.

QUESTION 5
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You need to deploy resources to host a stateless web app in an Azure subscription. The solution must meet the following requirements:

- Provide access to the full .NET framework.
- Provide redundancy if an Azure region fails.
- Grant administrators access to the operating system to install custom application dependencies.

Solution: You deploy two Azure virtual machines to two Azure regions, and create a Traffic Manager profile.

Does this meet the goal?

A. Yes
B. No

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6
HOTSPOT

You plan to deploy a network-intensive application to several Azure virtual machines.

You need to recommend a solution that meets the following requirements:

- Minimizes the use of the virtual machine processors to transfer data
- Minimizes network latency

Which virtual machine size and feature should you use? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Virtual machine size:

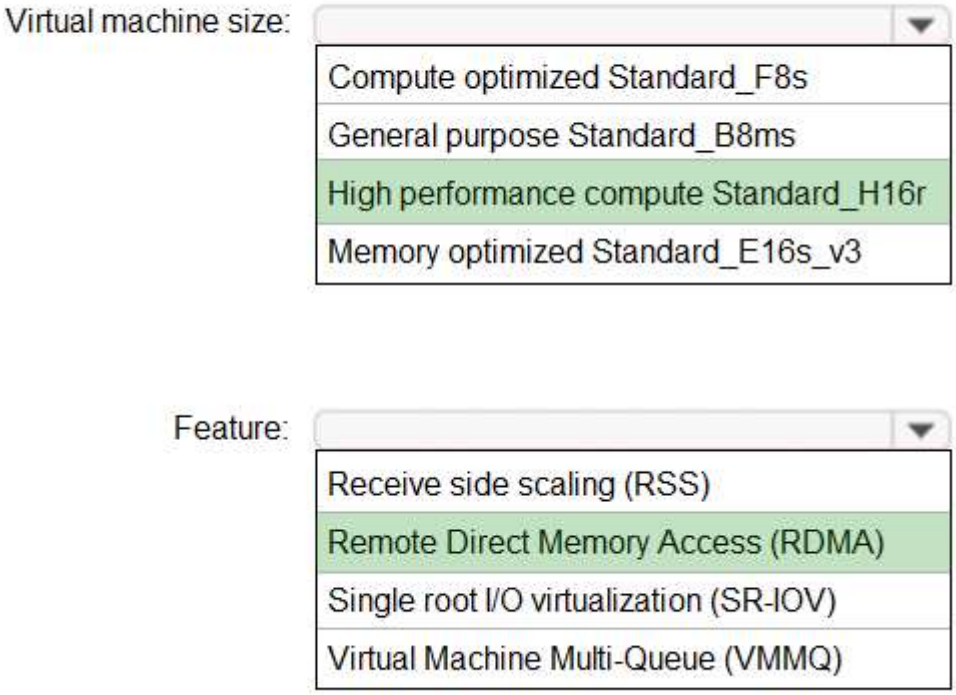
- Compute optimized Standard_F8s
- General purpose Standard_B8ms
- High performance compute Standard_H16r
- Memory optimized Standard_E16s_v3

Feature:

- Receive side scaling (RSS)
- Remote Direct Memory Access (RDMA)
- Single root I/O virtualization (SR-IOV)
- Virtual Machine Multi-Queue (VMMQ)

Correct Answer:

Answer Area



Section: (none)
Explanation

Explanation/Reference:
Reference:
https://docs.microsoft.com/en-us/azure/virtual-machines/windows/sizes-hpc#h-series

QUESTION 7
You need to recommend a solution to deploy containers that run an application. The application has two tiers. Each tier is implemented as a separate Docker Linux-based image. The solution must meet the following requirements:

- The front-end tier must be accessible by using a public IP address on port 80.
- The backend tier must be accessible by using port 8080 from the front-end tier only.
- Both containers must be able to access the same Azure file share.
- If a container fails, the application must restart automatically.
- Costs must be minimized.

What should you recommend using to host the application?

A. Azure Kubernetes Service (AKS)
B. Azure Service Fabric
C. Azure Container instances

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Azure Container Instances enables a layered approach to orchestration, providing all of the scheduling and management capabilities required to run a single container, while allowing orchestrator platforms to manage multi-container tasks on top of it.

Because the underlying infrastructure for container instances is managed by Azure, an orchestrator platform does not need to concern itself with finding an appropriate host machine on which to run a single container.

Azure Container Instances can schedule both Windows and Linux containers with the same API.

Orchestration of container instances exclusively
Because they start quickly and bill by the second, an environment based exclusively on Azure Container Instances offers the fastest way to get started and to deal with highly variable workloads.

Reference:
https://docs.microsoft.com/en-us/azure/container-instances/container-instances-overview

https://docs.microsoft.com/en-us/azure/container-instances/container-instances-orchestrator-relationship

QUESTION 8
You architect a solution that calculates 3D geometry from height-map data.

You have the following requirements:

- Perform calculations in Azure.
- Each node must communicate data to every other node.
- Maximize the number of nodes to calculate multiple scenes as fast as possible.
- Require the least amount of effort to implement.

You need to recommend a solution.

Which two actions should you recommend? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Create a render farm that uses Azure Batch.
B. Create a render farm that uses virtual machines (VMs).
C. Enable parallel task execution on compute nodes.
D. Create a render farm that uses virtual machine (VM) scale sets.
E. Enable parallel file systems on Azure.

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9
Your company plans to publish APIs for its services by using Azure API Management.

You discover that service responses include the AspNet-Version header.

You need to recommend a solution to remove AspNet-Version from the response of the published APIs.

What should you include in the recommendation?

A. a new product
B. a modification to the URL scheme
C. a new policy
D. a new revision

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Set a new transformation policy to transform an API to strip response headers.

Reference:
https://docs.microsoft.com/en-us/azure/api-management/transform-api

QUESTION 10
You have an Azure subscription that contains a storage account.

An application sometimes writes duplicate files to the storage account.

You have a PowerShell script that identifies and deletes duplicate files in the storage account. Currently, the script is run manually after approval from the operations manager.

You need to recommend a serverless solution that performs the following actions:

- Runs the script once an hour to identify whether duplicate files exist
- Sends an email notification to the operations manager requesting approval to delete the duplicate files
- Processes an email response from the operations manager specifying whether the deletion was approved
- Runs the script if the deletion was approved

What should you include in the recommendation?

A. Azure Logic Apps and Azure Functions
B. Azure Pipelines and Azure Service Fabric
C. Azure Logic Apps and Azure Event Grid
D. Azure Functions and Azure Batch

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
You can schedule a powershell script with Azure Logic Apps.

When you want to run code that performs a specific job in your logic apps, you can create your own function by using Azure Functions. This service helps you create Node.js, C#, and F# functions so you don't have to build a complete app or infrastructure to run code. You can also call logic apps from inside Azure functions. Azure Functions provides serverless computing in the cloud and is useful for performing tasks such as these examples:

Reference:
https://docs.microsoft.com/en-us/azure/logic-apps/logic-apps-azure-functions

QUESTION 11
DRAG DROP

You have an on-premises network that uses an IP address space of 172.16.0.0/16.

You plan to deploy 25 virtual machines to a new Azure subscription.

You identify the following technical requirements:

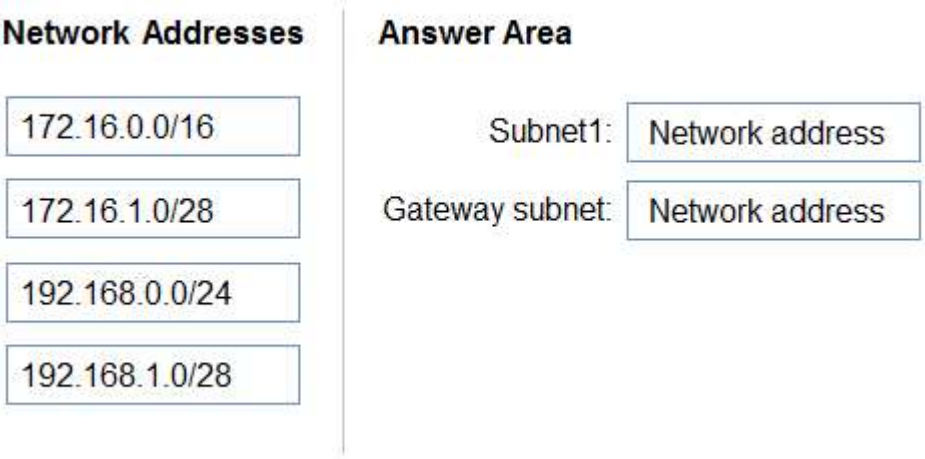
- All Azure virtual machines must be placed on the same subnet named Subnet1.
- All the Azure virtual machines must be able to communicate with all on-premises servers.
- The servers must be able to communicate between the on-premises network and Azure by using a site-to-site VPN.

You need to recommend a subnet design that meets the technical requirements.

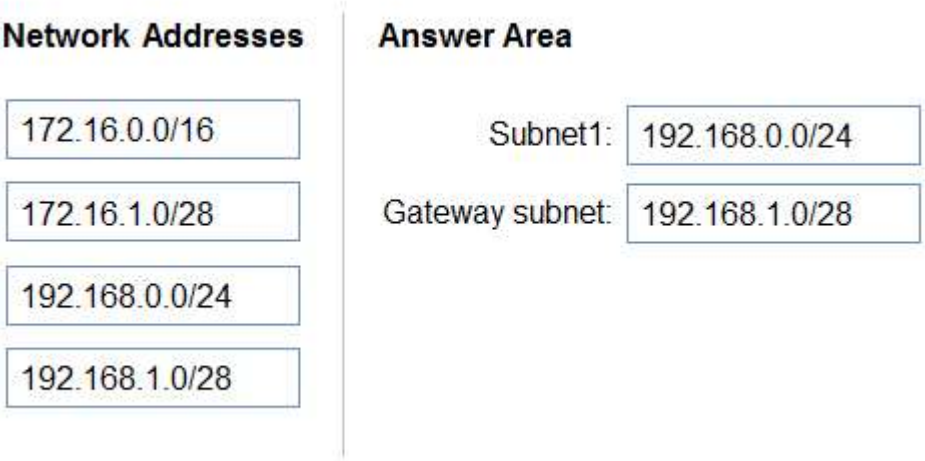
What should you include in the recommendation? To answer, drag the appropriate network addresses to the correct subnets. Each network address may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:



Correct Answer:



Section: (none)
Explanation

Explanation/Reference:

QUESTION 12
You are designing an Azure solution.

The network traffic for the solution must be securely distributed by providing the following features:

- HTTPS protocol
- Round robin routing
- SSL offloading

You need to recommend a load balancing option.

What should you recommend?

A. Azure Load Balancer
B. Azure Internal Load Balancer (ILB)
C. Azure Traffic Manager
D. Azure Application Gateway

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
If you are looking for Transport Layer Security (TLS) protocol termination ("SSL offload") or per-HTTP/HTTPS request, application-layer processing, review Application Gateway.

Application Gateway is a layer 7 load balancer, which means it works only with web traffic (HTTP, HTTPS, WebSocket, and HTTP/2). It supports capabilities such as SSL termination, cookie-based session affinity, and round robin for load-balancing traffic. Load Balancer load-balances traffic at layer 4 (TCP or UDP).

Reference:
https://docs.microsoft.com/en-us/azure/application-gateway/application-gateway-faq

QUESTION 13
Your company, named Contoso, Ltd, implements several Azure logic apps that have HTTP triggers: The logic apps provide access to an on-premises web service.

Contoso establishes a partnership with another company named Fabrikam, Inc.

Fabrikam does not have an existing Azure Active Directory (Azure AD) tenant and uses third-party OAuth 2.0 identity management to authenticate its users.

Developers at Fabrikam plan to use a subset of the logics apps to build applications that will integrate with the on-premises web service of Contoso.

You need to design a solution to provide the Fabrikam developers with access to the logic apps. The solution must meet the following requirements:

- Requests to the logic apps from the developers must be limited to lower rates than the requests from the users at Contoso.
- The developers must be able to rely on their existing OAuth 2.0 provider to gain access to the logic apps.
- The solution must **NOT** require changes to the logic apps.
- The solution must **NOT** use Azure AD guest accounts.

What should you include in the solution?

A. Azure AD business-to-business (B2B)
B. Azure Front Door
C. Azure API Management
D. Azure AD Application Proxy

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
API Management helps organizations publish APIs to external, partner, and internal developers to unlock the potential of their data and services.
You can secure API Management using the OAuth 2.0 client credentials flow.

Incorrect Answers:
A: Azure Active Directory B2B uses guest users.

B: Azure Front Door is an Application Delivery Network (ADN) as a service, offering various layer 7 load-balancing capabilities for your applications.
Azure Front Door supports HTTP, HTTPS and HTTP/2.
Applications can be authorized through OAuth 2.0.

D: Application Proxy is a feature of Azure AD that enables users to access on-premises web applications from a remote client. Application Proxy includes both the Application Proxy service which runs in the cloud, and the Application Proxy connector which runs on an on-premises server.

Application Proxy works with:
- Web applications that use Integrated Windows Authentication for authentication
- Web applications that use form-based or header-based access

Reference:
https://docs.microsoft.com/en-us/azure/api-management/api-management-key-concepts

QUESTION 14
You need to design a solution that will execute custom C# code in response to an event routed to Azure Event Grid. The solution must meet the following requirements:

- The executed code must be able to access the private IP address of a Microsoft SQL Server instance that runs on an Azure virtual machine.
- Costs must be minimized.

What should you include in the solution?

A. Azure Logic Apps in the integrated service environment
B. Azure Functions in the Dedicated plan and the Basic Azure App Service plan
C. Azure Logic Apps in the Consumption plan
D. Azure Functions in the Consumption plan

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
When you create a function app in Azure, you must choose a hosting plan for your app. There are three basic

hosting plans available for Azure Functions: Consumption plan, Premium plan, and Dedicated (App Service) plan.
For the Consumption plan, you don't have to pay for idle VMs or reserve capacity in advance.

Connect to private endpoints with Azure Functions
As enterprises continue to adopt serverless (and Platform-as-a-Service, or PaaS) solutions, they often need a way to integrate with existing resources on a virtual network. These existing resources could be databases, file storage, message queues or event streams, or REST APIs.

Reference:
https://docs.microsoft.com/en-us/azure/azure-functions/functions-scale

https://techcommunity.microsoft.com/t5/azure-functions/connect-to-private-endpoints-with-azure-functions/ba-p/1426615

QUESTION 15
The developers at your company are building a containerized Python Django app.

You need to recommend platform to host the app. The solution must meet the following requirements:

- Support autoscaling.
- Support continuous deployment from an Azure Container Registry.
- Provide built-in functionality to authenticate app users by using Azure Active Directory (Azure AD).

Which platform should you include in the recommendation?

A. Azure Container instances
B. an Azure App Service instance that uses containers
C. Azure Kubernetes Service (AKS)

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
To keep up with application demands in Azure Kubernetes Service (AKS), you may need to adjust the number of nodes that run your workloads. The cluster autoscaler component can watch for pods in your cluster that can't be scheduled because of resource constraints. When issues are detected, the number of nodes in a node pool is increased to meet the application demand.

Azure Container Registry is a private registry for hosting container images. It integrates well with orchestrators like Azure Container Service, including Docker Swarm, DC/OS, and the new Azure Kubernetes service. Moreover, ACR provides capabilities such as Azure Active Directory-based authentication, webhook support, and delete operations.

Reference:
https://docs.microsoft.com/en-us/azure/aks/cluster-autoscaler

https://medium.com/velotio-perspectives/continuous-deployment-with-azure-kubernetes-service-azure-container-registry-jenkins-ca337940151b

QUESTION 16
You have an on-premises network to which you deploy a virtual appliance.

You plan to deploy several Azure virtual machines and connect the on-premises network to Azure by using a Site-to-Site connection.

All network traffic that will be directed from the Azure virtual machines to a specific subnet must flow through

the virtual appliance.

You need to recommend solutions to manage network traffic.

Which two options should you recommend? Each correct answer presents a complete solution.

A. Configure Azure Traffic Manager.
B. Implement Azure ExpressRoute.
C. Configure a routing table.
D. Implement an Azure virtual network.

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
Explanation:
B: Forced tunneling lets you redirect or "force" all Internet-bound traffic back to your on-premises location via a Site-to-Site VPN tunnel for inspection and auditing. This is a critical security requirement for most enterprise IT policies. Without forced tunneling, Internet-bound traffic from your VMs in Azure always traverses from Azure network infrastructure directly out to the Internet, without the option to allow you to inspect or audit the traffic.

Forced tunneling in Azure is configured via virtual network user-defined routes.

C: ExpressRoute lets you extend your on-premises networks into the Microsoft cloud over a private connection facilitated by a connectivity provider. With ExpressRoute, you can establish connections to Microsoft cloud services, such as Microsoft Azure, Office 365, and Dynamics 365.

Connectivity can be from an any-to-any (IP VPN) network, a point-to-point Ethernet network, or a virtual cross-connection through a connectivity provider at a co-location facility. ExpressRoute connections do not go over the public Internet. This allows ExpressRoute connections to offer more reliability, faster speeds, lower latencies, and higher security than typical connections over the Internet.

Reference:
https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-forced-tunneling-rm

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

QUESTION 17
You are developing a sales application that will contain several Azure cloud services and will handle different components of a transaction. Different cloud services will process customer orders, billing, payment, inventory, and shipping.

You need to recommend a solution to enable the cloud services to asynchronously communicate transaction information by using REST messages.

What should you include in the recommendation?

A. Azure Service Bus
B. Azure Blob storage
C. Azure Notification Hubs
D. Azure Application Gateway

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

Explanation:
Service Bus is a transactional message broker and ensures transactional integrity for all internal operations against its message stores. All transfers of messages inside of Service Bus, such as moving messages to a dead-letter queue or automatic forwarding of messages between entities, are transactional.

Incorrect Answers:
C: Azure Notification Hubs is a massively scalable mobile push notification engine for quickly sending millions of notifications to iOS, Android, Windows, or Kindle devices.

Reference:
https://docs.microsoft.com/en-us/azure/service-bus-messaging/service-bus-transactions

QUESTION 18
You are designing a message application that will run on an on-premises Ubuntu virtual machine. The application will use Azure Storage queues.

You need to recommend a processing solution for the application to interact with the storage queues. The solution must meet the following requirements:

- Create and delete queues daily.
- Be scheduled by using a CRON job.
- Upload messages every five minutes.

What should developers use to interact with the queues?

A. Azure CLI
B. AzCopy
C. Azure Data Factory
D. .NET Core

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Incorrect Answers:
A: It is not possible to have Linux running in Windows Azure

B: AzCopy is a command-line utility that you can use to copy blobs or files to or from a storage account.

Reference:
https://docs.microsoft.com/en-us/azure/storage/queues/storage-tutorial-queues

QUESTION 19
You have a .NET web service named Service1 that has the following requirements:

- Must read and write temporary files to the local file system.
- Must write to the Application event log.

You need to recommend a solution to host Service1 in Azure. The solution must meet the following requirements:

- Minimize maintenance overhead.
- Minimize costs.

What should you include in the recommendation?

A. an App Service Environment
B. an Azure web app
C. an Azure virtual machine scale set
D. an Azure function

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 20
You are designing a microservices architecture that will support a web application.

The solution must meet the following requirements:

- Allow independent upgrades to each microservice.
- Deploy the solution on-premises and to Azure.
- Set policies for performing automatic repairs to the microservices.
- Support low-latency and hyper-scale operations.

You need to recommend a technology.

A. Azure Container Instance
B. Azure Virtual Machine Scale Set
C. Azure Service Fabric
D. Azure Logic App

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Azure Service Fabric is a distributed systems platform that makes it easy to package, deploy, and manage scalable and reliable microservices and containers.

You can use Azure Service Fabric to create Service Fabric clusters on any virtual machines or computers running Windows Server.

Reference:
https://docs.microsoft.com/en-us/azure/service-fabric/service-fabric-overview

QUESTION 21
Your company has the infrastructure shown in the following table.

Location	Resource
Azure	• Azure subscription named Subscription1 • 20 Azure web apps
On-premises datacenter	• Active Directory domain • Server running Azure AD Connect • Linux computer named Server1

The on-premises Active Directory domain syncs to Azure Active Directory (Azure AD).

Server1 runs an application named App1 that uses LDAP queries to verify user identities in the on-premises Active Directory domain.

You plan to migrate Server1 to a virtual machine in Subscription1.

A company security policy states that the virtual machines and services deployed to Subscription1 must be prevented from accessing the on-premises network.

You need to recommend a solution to ensure that App1 continues to function after the migration. The solution must meet the security policy.

What should you include in the recommendation?

A. Azure AD Application Proxy
B. an Azure VPN gateway
C. Azure AD Domain Services (Azure AD DS)
D. the Active Directory Domain Services role on a virtual machine

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
You can join a Windows Server virtual machine to an Azure Active Directory Domain Services managed domain.

Reference:
https://docs.microsoft.com/en-us/azure/active-directory-domain-services/join-windows-vm

QUESTION 22
HOTSPOT

Your company deploys an Azure App Service Web App.

During testing the application fails under load. The application cannot handle more than 100 concurrent user sessions. You enable the Always On feature. You also configure auto-scaling to increase instance counts from two to 10 based on HTTP queue length.

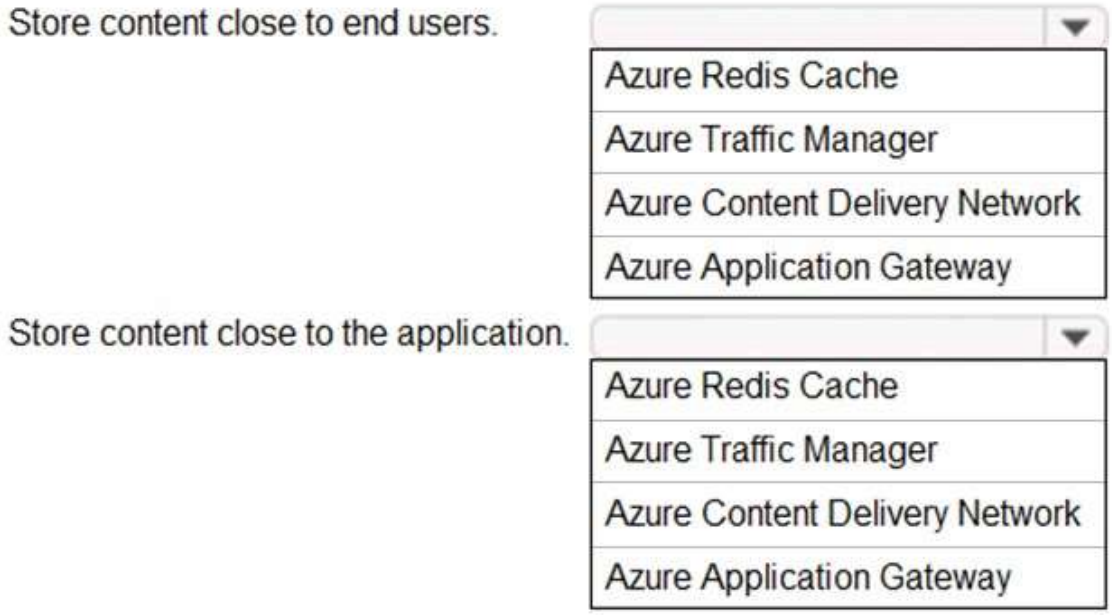
You need to improve the performance of the application.

Which solution should you use for each application scenario? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

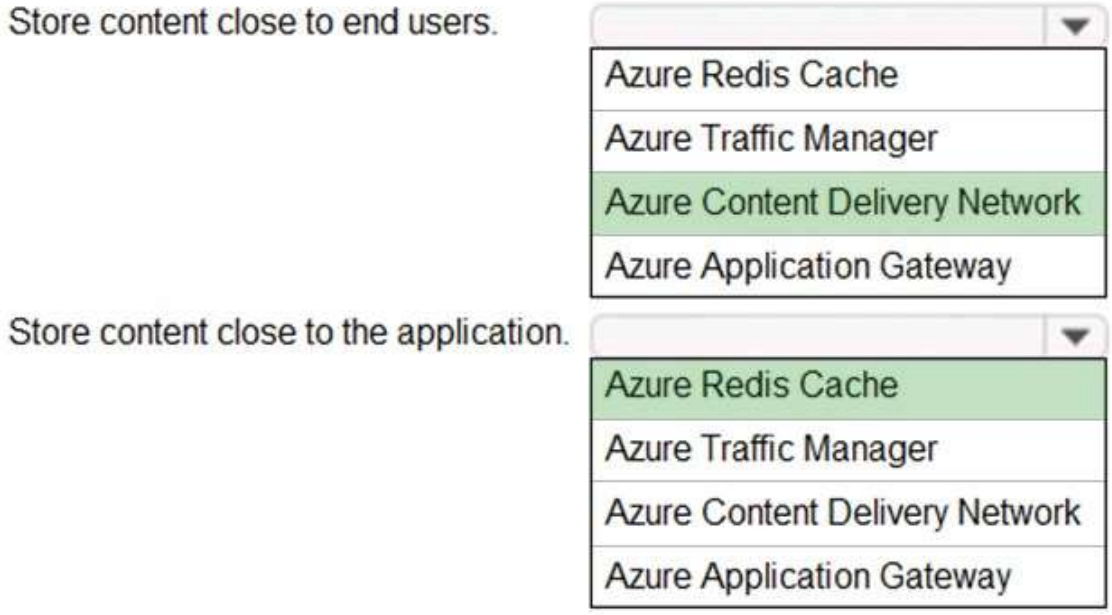
Hot Area:

Answer Area



Correct Answer:

Answer Area



Section: (none)
Explanation

Explanation/Reference:

Explanation:

Box 1: Content Delivery Network
A content delivery network (CDN) is a distributed network of servers that can efficiently deliver web content to users. CDNs store cached content on edge servers in point-of-presence (POP) locations that are close to end users, to minimize latency.

Azure Content Delivery Network (CDN) offers developers a global solution for rapidly delivering high-bandwidth content to users by caching their content at strategically placed physical nodes across the world. Azure CDN can also accelerate dynamic content, which cannot be cached, by leveraging various network optimizations using CDN POPs. For example, route optimization to bypass Border Gateway Protocol (BGP).

Box 2: Azure Redis Cache
Azure Cache for Redis is based on the popular software Redis. It is typically used as a cache to improve the performance and scalability of systems that rely heavily on backend data-stores. Performance is improved by temporarily copying frequently accessed data to fast storage located close to the application. With Azure Cache for Redis, this fast storage is located in-memory with Azure Cache for Redis instead of being loaded from disk by a database.

Reference:
https://docs.microsoft.com/en-us/azure/azure-cache-for-redis/cache-overview

QUESTION 23
You use Azure virtual machines to run a custom application that uses an Azure SQL Database instance on the back end.

The IT department at your company recently enabled forced tunneling.

Since the configuration change, developers have noticed degraded performance when they access the database from the Azure virtual machine.

You need to recommend a solution to minimize latency when accessing the database. The solution must minimize costs.

What should you include in the recommendation?

A. Virtual Network (VNET) service endpoints
B. Azure virtual machines that run Microsoft SQL Server servers
C. Azure SQL Database Managed Instance
D. Always On availability groups

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24
DRAG DROP

You are planning an Azure solution that will host production databases for a high-performance application. The solution will include the following components:

- Two virtual machines that will run Microsoft SQL Server 2016, will be deployed to different data centers in the same Azure region, and will be part of an Always On availability group
- SQL Server data that will be backed up by using the Automated Backup feature of the SQL Server IaaS Agent Extension (SQLIaaSExtension)

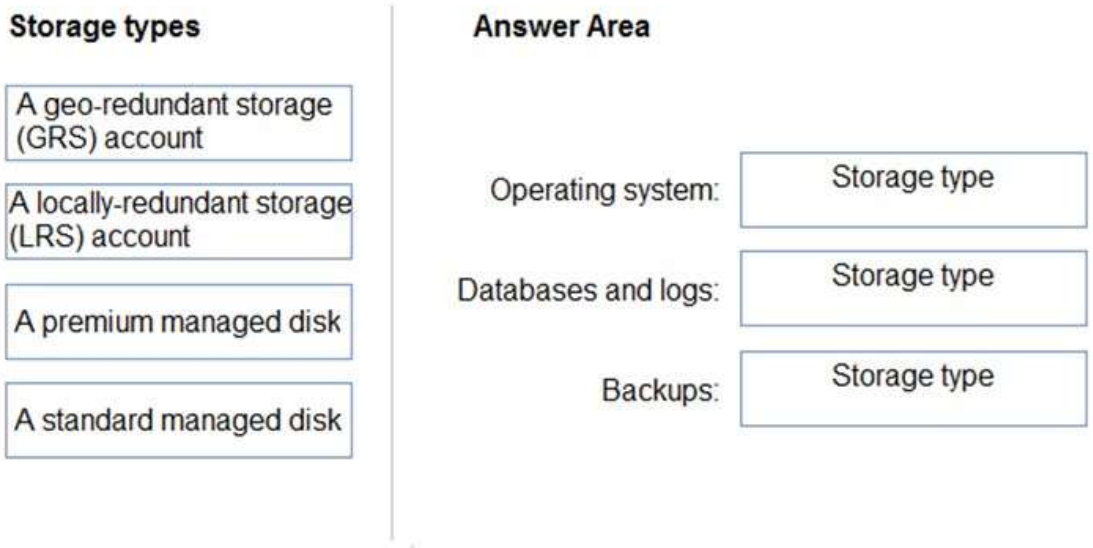
You identify the storage priorities for various data types as shown in the following table.

Data type	Storage priority
Operating system	Speed and availability
Databases and logs	Speed and availability
Backups	Lowest cost

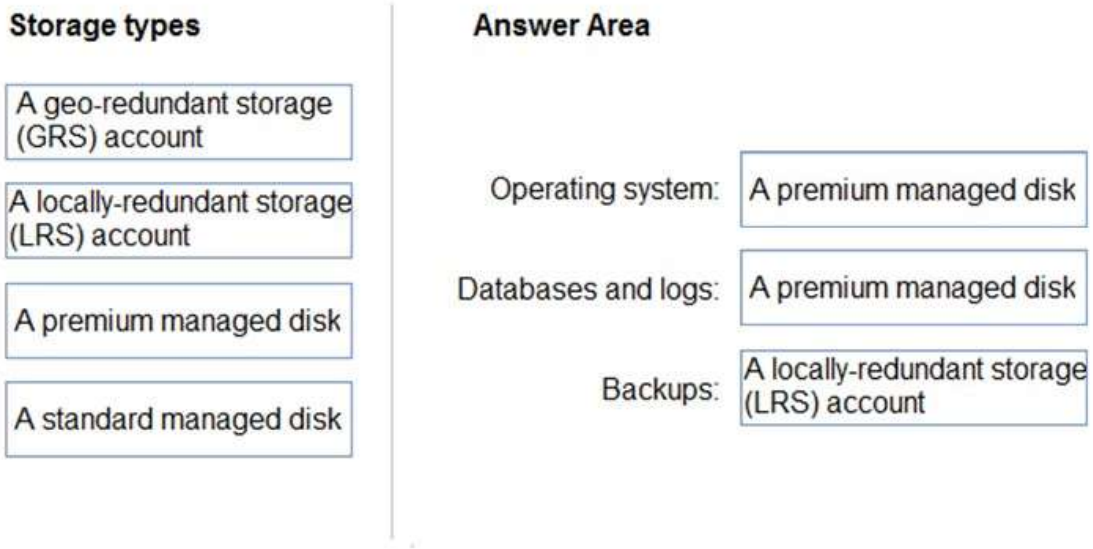
Which storage type should you recommend for each data type? To answer, drag the appropriate storage types to the correct data types. Each storage type may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:



Correct Answer:



Section: (none)

Explanation

Explanation/Reference:

QUESTION 25
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your company plans to deploy various Azure App Service instances that will use Azure SQL databases. The App Service instances will be deployed at the same time as the Azure SQL databases.

The company has a regulatory requirement to deploy the App Service instances only to specific Azure regions. The resources for the App Service instances must reside in the same region.

You need to recommend a solution to meet the regulatory requirement.

Solution: You recommend using the Regulatory compliance dashboard in Azure Security Center.

Does this meet the goal?

A. Yes
B. No

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The Regulatory compliance dashboard in Azure Security Center is not used for regional compliance.

Note: Instead Azure Resource Policy Definitions can be used which can be applied to a specific Resource Group with the App Service instances.

Note 2: In the Azure Security Center regulatory compliance blade, you can get an overview of key portions of your compliance posture with respect to a set of supported standards. Currently supported standards are Azure CIS, PCI DSS 3.2, ISO 27001, and SOC TSP.

Reference:
https://docs.microsoft.com/en-us/azure/governance/policy/overview

https://azure.microsoft.com/en-us/blog/regulatory-compliance-dashboard-in-azure-security-center-now-available/

Design Infrastructure

Testlet 2

Case Study

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

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

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

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

Overview

Contoso, Ltd, is a US-based financial services company that has a main office in New York and a branch office in San Francisco.

Existing Environment. Payment Processing System

Contoso hosts a business-critical payment processing system in its New York data center. The system has three tiers: a front-end web app, a middle-tier web API, and a back-end data store implemented as a Microsoft SQL Server 2014 database. All servers run Windows Server 2012 R2.

The front-end and middle-tier components are hosted by using Microsoft Internet Information Services (IIS). The application code is written in C# and ASP.NET. The middle-tier API uses the Entity Framework to communicate to the SQL Server database. Maintenance of the database is performed by using SQL Server Agent jobs.

The database is currently 2 TB and is not expected to grow beyond 3 TB.

The payment processing system has the following compliance-related requirements:

- Encrypt data in transit and at rest. Only the front-end and middle-tier components must be able to access the encryption keys that protect the data store.
- Keep backups of the data in two separate physical locations that are at least 200 miles apart and can be restored for up to seven years.
- Support blocking inbound and outbound traffic based on the source IP address, the destination IP address, and the port number.
- Collect Windows security logs from all the middle-tier servers and retain the logs for a period of seven years.
- Inspect inbound and outbound traffic from the front-end tier by using highly available network appliances.
- Only allow all access to all the tiers from the internal network of Contoso.

Tape backups are configured by using an on-premises deployment of Microsoft System Center Data Protection Manager (DPM), and then shipped offsite for long term storage.

Existing Environment. Historical Transaction Query System

Contoso recently migrated a business-critical workload to Azure. The workload contains a .NET web service for querying the historical transaction data residing in Azure Table Storage. The .NET web service is accessible from a client app that was developed in-house and runs on the client computers in the New York office. The data in the table storage is 50 GB and is not expected to increase.

Existing Environment. Current Issues

The Contoso IT team discovers poor performance of the historical transaction query system, as the queries frequently cause table scans.

Requirements. Planned Changes

Contoso plans to implement the following changes:

- Migrate the payment processing system to Azure.
- Migrate the historical transaction data to Azure Cosmos DB to address the performance issues.

Requirements. Migration Requirements

Contoso identifies the following general migration requirements:

- Infrastructure services must remain available if a region or a data center fails. Failover must occur without any administrative intervention.
- Whenever possible, Azure managed services must be used to minimize management overhead.
- Whenever possible, costs must be minimized.

Contoso identifies the following requirements for the payment processing system:

- If a data center fails, ensure that the payment processing system remains available without any administrative intervention. The middle-tier and the web front end must continue to operate without any additional configurations.
- Ensure that the number of compute nodes of the front-end and the middle tiers of the payment processing system can increase or decrease automatically based on CPU utilization.
- Ensure that each tier of the payment processing system is subject to a Service Level Agreement (SLA) of 99.99 percent availabilty.
- Minimize the effort required to modify the middle-tier API and the back-end tier of the payment processing system.
- Payment processing system must be able to use grouping and joining tables on encrypted columns.
- Generate alerts when unauthorized login attempts occur on the middle-tier virtual machines.
- Ensure that the payment processing system preserves its current compliance status.
- Host the middle tier of the payment processing system on a virtual machine

Contoso identifies the following requirements for the historical transaction query system:

- Minimize the use of on-premises infrastructure services.
- Minimize the effort required to modify the .NET web service querying Azure Cosmos DB.
- Minimize the frequency of table scans.
- If a region fails, ensure that the historical transaction query system remains available without any administrative intervention.

Requirements. Information Security Requirements

The IT security team wants to ensure that identity management is performed by using Active Directory. Password hashes must be stored on-premises only.

Access to all business-critical systems must rely on Active Directory credentials. Any suspicious authentication attempts must trigger a multi-factor authentication prompt automatically.

QUESTION 1
You need to recommend a compute solution for the middle tier of the payment processing system.

What should you include in the recommendation?

A. virtual machine scale sets
B. availability sets
C. Azure Kubernetes Service (AKS)
D. Function App

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

Design Infrastructure

Testlet 3

Case Study

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

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

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

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

Overview

Fabricam, 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.

Existing Environment. Network Infrastructure

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

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

An existing application named WebApp1 is hosted in the data center of the London office. WebApp1 is used by customers to place and track orders. WebApp1 has a web tier that uses Microsoft Internet Information Services (IIS) and a database tier that runs Microsoft SQL Server 2016. The web tier and the database tier are deployed to virtual machines that run on Hyper-V.

The IT department currently uses a separate Hyper-V environment to test updates to WebApp1.

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

Existing Environment. Problem Statements

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

Requirements. Planned Changes

Fabrikam plans to move most of its production workloads to Azure during the next few years.

As one of its first projects, the company plans to establish a hybrid identity model, facilitating an upcoming Microsoft Office 365 deployment.

All R&D operations will remain on-premises.

Fabrikam plans to migrate the production and test instances of WebApp1 to Azure and to use the S1 plan.

Requirements. Technical Requirements

Fabrikam identifies the following technical requirements:

- Web site content must be easily updated from a single point.
- User input must be minimized when provisioning new 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.
- Directory synchronization between Azure Active Directory (Azure AD) and corp.fabrikam.com must not be affected by a link failure between Azure and the on-premises network.

Requirements. Database Requirements

Fabrikam identifies the following database requirements:

- Database metrics for the production instance of WebApp1 must be available for analysis so that database administrators can optimize the performance settings.
- To avoid disrupting customer access, database downtime must be minimized when databases are migrated.
- Database backups must be retained for a minimum of seven years to meet compliance requirements.

Requirements. Security Requirements

Fabrikam identifies the following security requirements:

- Company information including policies, templates, and data must be inaccessible to anyone outside the company.
- Users on the on-premises network must be able to authenticate to corp.fabrikam.com if an Internet link fails.
- Administrators must be able authenticate to the Azure portal by using their corp.fabrikam.com credentials.
- All administrative access to the Azure portal must be secured by using multi-factor authentication.
- The testing of WebApp1 updates must not be visible to anyone outside the company.

QUESTION 1
You need to recommend a strategy for migrating the database content of WebApp1 to Azure.

What should you include in the recommendation?

A. Use Azure Site Recovery to replicate the SQL servers to Azure.

B. Copy the BACPAC file that contains the Azure SQL database files to Azure Blob storage.
C. Use SQL Server transactional replication.
D. Copy the VHD that contains the Azure SQL database files to Azure Blob storage.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Before you upload a Windows virtual machine (VM) from on-premises to Azure, you must prepare the virtual hard disk (VHD or VHDX).

Scenario: 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.

Reference:
https://docs.microsoft.com/en-us/azure/virtual-machines/windows/prepare-for-upload-vhd-image

QUESTION 2
You need to recommend a notification solution for the IT Support distribution group.

What should you include in the recommendation?

A. a SendGrid account with advanced reporting
B. Azure AD Connect Health
C. Azure Network Watcher
D. an action group

Correct Answer: B
Section: (none)
Explanation

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