Microsoft Azure Architect Design (beta)

Microsoft AZ-304

Total Questions: 196

https://dumpsarena.com

sales@dumpsarena.com

dumpsarena.com

Topic Break Down

Topic	No. of Questions
Topic 1, Case Study 1	2
Topic 2, Case Study 2	2
Topic 3, Case Study 3	4
Topic 4, Case Study 4	2
Topic 5, Mixed Questions	186
Total	196

Topic 1, Case Study 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

Fabrikam, Inc. is an engineering company that has offices throughout Europe. The company has a main office in London and three branch offices in Amsterdam, Berlin, and Rome.

Existing Environment. Active Directory Environment

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

Corp.fabrikam.com is a production forest that contains identities used for internal user and computer authentication.

Rd.fabrikam.com is used by the research and development (R&D) department only. 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 365 deployment.

All R&D operations will remain on-premises.

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

Requirements. Technical Requirements

Fabrikam identifies the following technical requirements:

- 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 NO: 1 - (Topic 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.

ANSWER: C

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 NO: 2 - (HOTSPOT) - (Topic 1)

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:

Answer Area

Minimum number of Azure AD tenants:

0
1
2
3
4

Minimum number of custom domains to add:

0
1
2
3
4

Minimum number of conditional access policies to create:

0
1
2
3
4

ANSWER:

Answer Area

Minimum number of Azure AD tenants:

0
1
2
3
4

Minimum number of custom domains to add:

0
1
2
3
4

Minimum number of conditional access policies to create:

0
1
2
3
4

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

Topic 2, Case Study 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 NO: 3 - (Topic 2)

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

ANSWER: A

QUESTION NO: 4 - (HOTSPOT) - (Topic 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

Sizing requirements:

- A table that has unlimited capacity
- A table that has a fixed capacity
- Multiple tables that have unlimited capacity
- Multiple tables that have fixed capacity

Resiliency:

- An additional read region
- An availability set
- An availability zone

ANSWER:

Answer Area

Sizing requirements:

- A table that has unlimited capacity
- A table that has a fixed capacity
- Multiple tables that have unlimited capacity
- Multiple tables that have fixed capacity

Resiliency:

- An additional read region
- An availability set
- An availability zone

Explanation:

Design Business Continuity

Topic 3, Case Study 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

Fabrikam, Inc. is an engineering company that has offices throughout Europe. The company has a main office in London and three branch offices in Amsterdam, Berlin, and Rome.

Existing Environment. Active Directory Environment

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

Corp.fabrikam.com is a production forest that contains identities used for internal user and computer authentication.

Rd.fabrikam.com is used by the research and development (R&D) department only. 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 365 deployment.

All R&D operations will remain on-premises.

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

Requirements. Technical Requirements

Fabrikam identifies the following technical requirements:

- 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 NO: 5 - (Topic 3)

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.

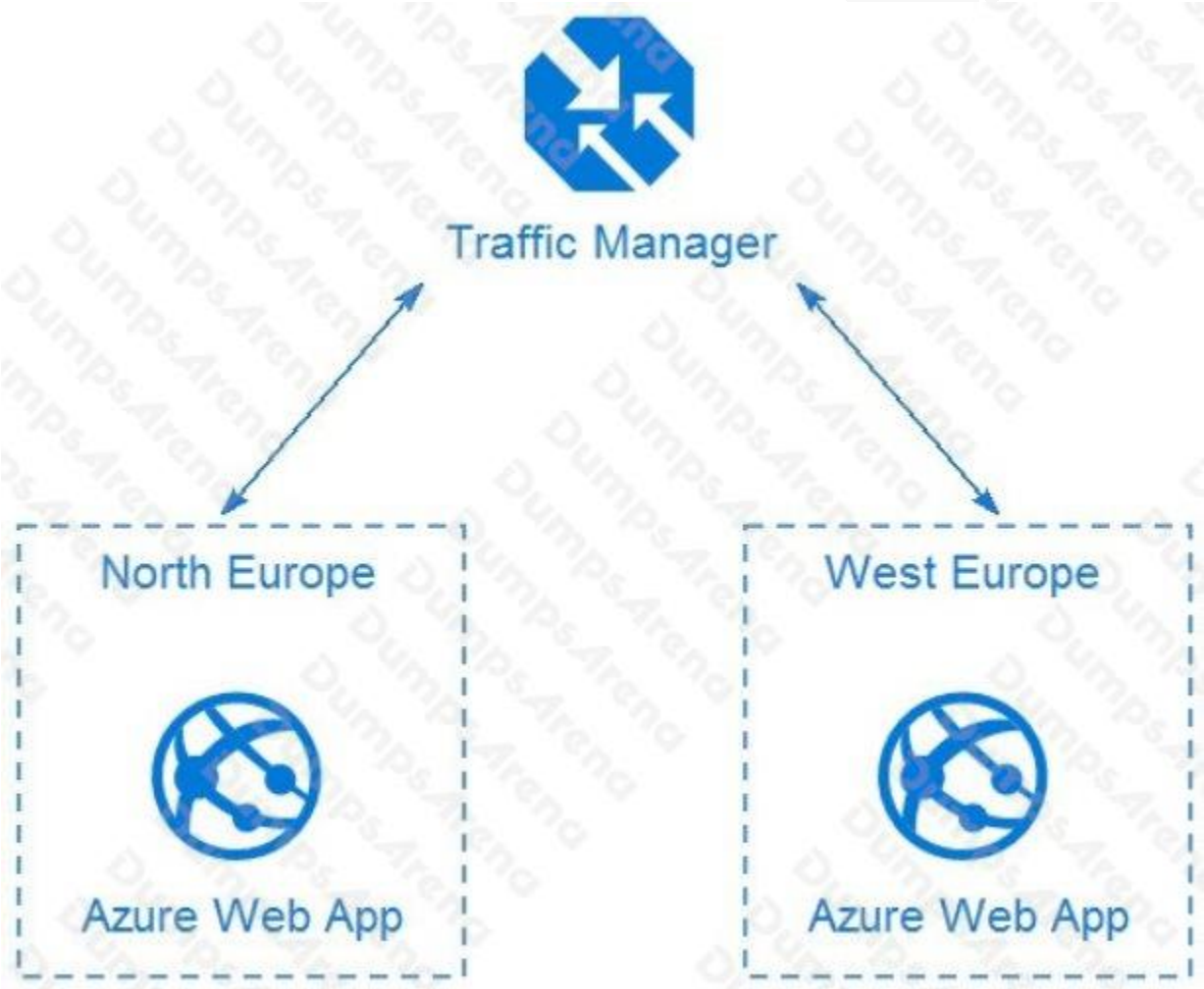
D. Use automatic Azure SQL Database backups.

ANSWER: B

QUESTION NO: 6 - (HOTSPOT) - (Topic 3)

HOTSPOT

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



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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

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

ANSWER:

Answer Area

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

Explanation:

Box 1: Yes

Any new deployments to Azure must be redundant in case an Azure region fails.

Traffic Manager uses DNS to direct client requests to the most appropriate service endpoint based on a traffic-routing method and the health of the endpoints. An endpoint is any Internet-facing service hosted inside or outside of Azure. Traffic Manager provides a range of traffic-routing methods and endpoint monitoring options to suit different application needs and automatic failover models. Traffic Manager is resilient to failure, including the failure of an entire Azure region.

Box 2: Yes

Recent changes in Azure brought some significant changes in autoscaling options for Azure Web Apps (i.e. Azure App Service to be precise as scaling happens on App Service plan level and has effect on all Web Apps running in that App Service plan).

Box 3: No

Traffic Manager provides a range of traffic-routing methods and endpoint monitoring options to suit different application needs and automatic failover models. Traffic Manager is resilient to failure, including the failure of an entire Azure region.

Reference:

https://docs.microsoft.com/en-us/azure/traffic-manager/traffic-manager-overview
https://blogs.msdn.microsoft.com/hsirtl/2017/07/03/autoscaling-azure-web-apps/

Design Infrastructure

QUESTION NO: 7 - (Topic 3)

You need to recommend a strategy for the web tier of WebApp1. The solution must minimize costs.

What should you recommend?

A. Configure the Scale Up settings for a web app.

B. Deploy a virtual machine scale set that scales out on a 75 percent CPU threshold.

C. Create a runbook that resizes virtual machines automatically to a smaller size outside of business hours.

D. Configure the Scale Out settings for a web app.

ANSWER: C

QUESTION NO: 8 - (HOTSPOT) - (Topic 3)

HOTSPOT

You are evaluating the components of the migration to Azure that require you to provision an Azure Storage account.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
You must provision an Azure Storage account for the SQL Server database migration.	○	○
You must provision an Azure Storage account for the Web site content storage.	○	○
You must provision an Azure Storage account for the Database metric monitoring.	○	○

ANSWER:

Answer Area

Statements	Yes	No
You must provision an Azure Storage account for the SQL Server database migration.	○	○
You must provision an Azure Storage account for the Web site content storage.	○	○
You must provision an Azure Storage account for the Database metric monitoring.	○	○

Explanation:

Topic 4, Case Study 4

Case Study

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

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

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

To start the case study

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

Overview

Fabrikam, Inc. is an engineering company that has offices throughout Europe. The company has a main office in London and three branch offices in Amsterdam, Berlin, and Rome.

Existing Environment. Active Directory Environment

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

Corp.fabrikam.com is a production forest that contains identities used for internal user and computer authentication.

Rd.fabrikam.com is used by the research and development (R&D) department only. 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 365 deployment.

All R&D operations will remain on-premises.

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

Requirements. Technical Requirements

Fabrikam identifies the following technical requirements:

- 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 NO: 9 - (Topic 4)

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.

ANSWER: D

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 NO: 10 - (Topic 4)

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

ANSWER: B

Explanation:

Reference:

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

Topic 5, Mixed Questions

QUESTION NO: 11 - (Topic 5)

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

ANSWER: D

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 NO: 12 - (Topic 5)

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

ANSWER: D

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 NO: 13 - (HOTSPOT) - (Topic 5)

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

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**

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 NO: 14 - (Topic 5)

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.

ANSWER: C D

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 NO: 15 - (HOTSPOT) - (Topic 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.	○	○

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.	○	○

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 NO: 16 - (Topic 5)

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

ANSWER: B

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 NO: 17 - (Topic 5)

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

ANSWER: C D

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 NO: 18 - (HOTSPOT) - (Topic 5)

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.	○	○

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.	○	○

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.

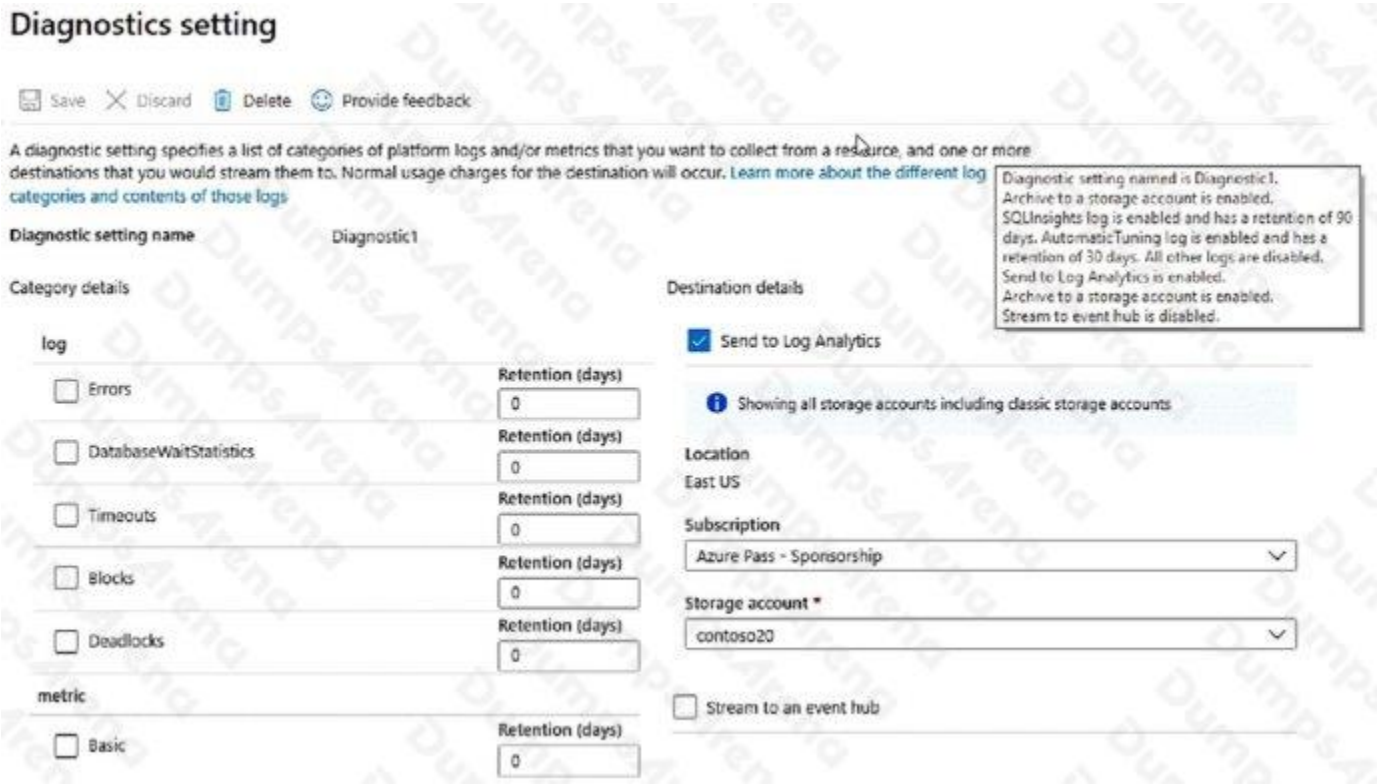
Reference: https://docs.microsoft.com/en-us/azure/azure-monitor/platform/diagnostic-settings

QUESTION NO: 19 - (HOTSPOT) - (Topic 5)

HOTSPOT

You deploy several Azure SQL Database instances.

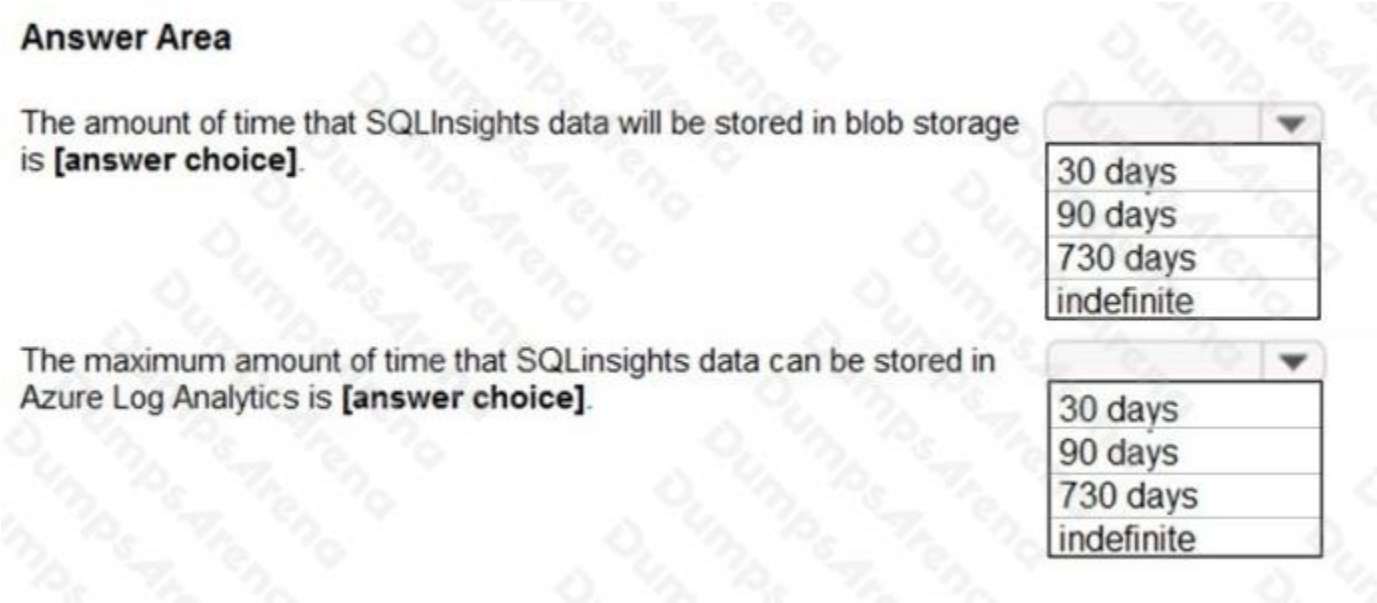
You plan to configure the Diagnostics settings on the databases as shown in the following exhibit.



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:



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

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

QUESTION NO: 20 - (Topic 5)

Your company uses Microsoft System Center Service Manager on its on-premises network.

You plan to deploy several services to Azure.

You need to recommend a solution to push Azure service health alerts to Service Manager.

What should you include in the recommendation?

A. IT Service Management Connector (ITSM)

B. Azure Event Hubs

C. Azure Notification Hubs

D. Application Insights Connector

ANSWER: A

Explanation:

Reference: https://docs.microsoft.com/en-us/azure/azure-monitor/platform/itsmc-overview

QUESTION NO: 21 - (HOTSPOT) - (Topic 5)

HOTSPOT

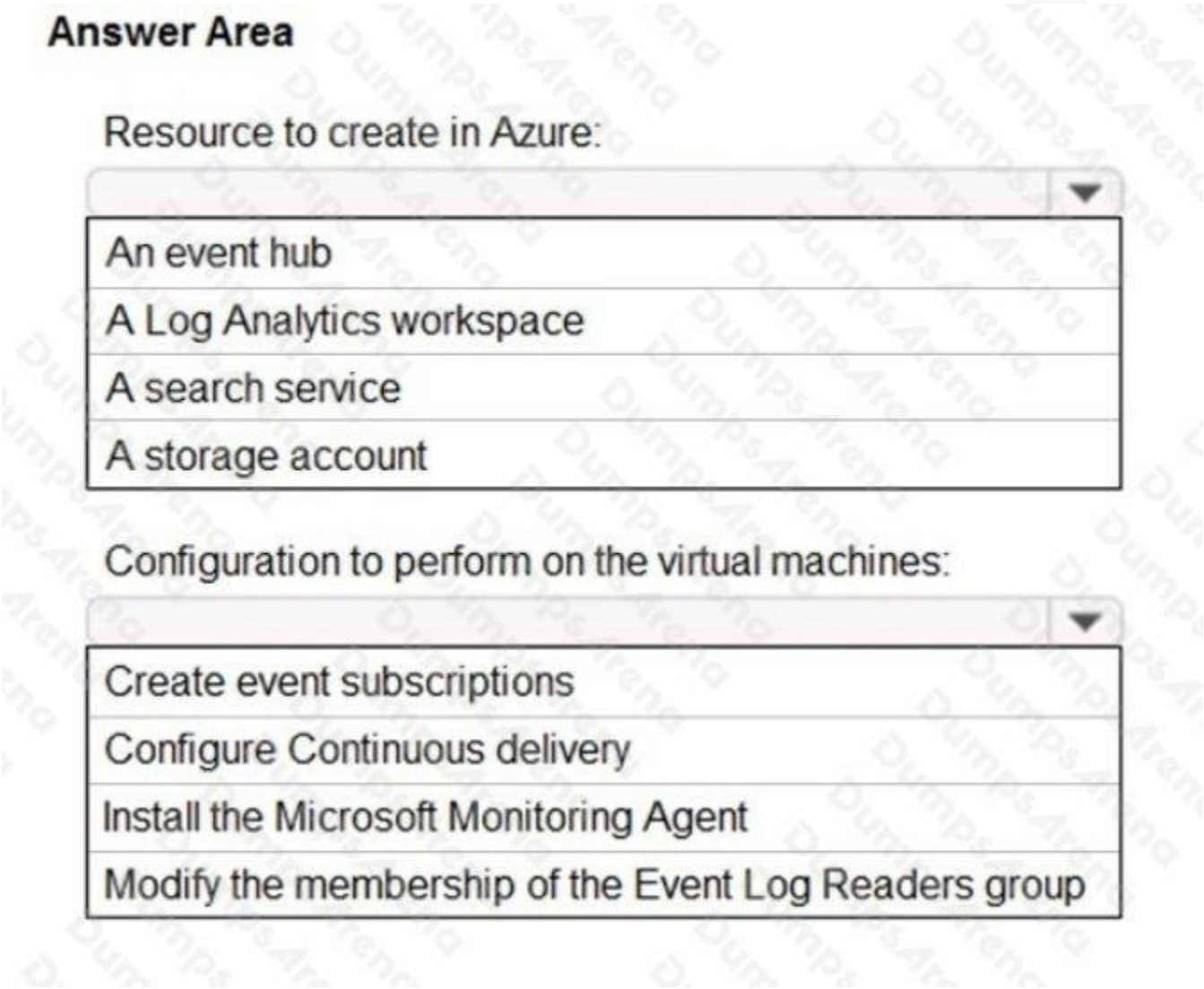
You have an Azure subscription that contains 300 Azure virtual machines that run Windows Server 2016.

You need to centrally monitor all warning events in the System logs of the virtual machines.

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:

Answer Area

Resource to create in Azure:

- An event hub
- A Log Analytics workspace
- A search service
- A storage account

Configuration to perform on the virtual machines:

- Create event subscriptions
- Configure Continuous delivery
- Install the Microsoft Monitoring Agent
- Modify the membership of the Event Log Readers group

Explanation:

Reference:

https://docs.microsoft.com/en-us/azure/azure-monitor/platform/data-sources-windows-events https://docs.microsoft.com/en-us/azure/azure-monitor/platform/agent-windows

QUESTION NO: 22 - (Topic 5)

You have an Azure SQL database named DB1 that contains multiple tables.

You need to improve the performance of DB1. The solution must minimize administrative effort.

What should you use?

A. automatic tuning

B. Azure Advisor

C. Azure Monitor

D. Query Performance Insight

ANSWER: A

Explanation:

Azure SQL Database and Azure SQL Managed Instance automatic tuning provides peak performance and stable workloads through continuous performance tuning based on AI and machine learning.

Automatic tuning is a fully managed intelligent performance service that uses built-in intelligence to continuously monitor queries executed on a database, and it automatically improves their performance.

Reference:

https://docs.microsoft.com/en-us/azure/azure-sql/database/automatic-tuning-overview

QUESTION NO: 23 - (Topic 5)

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. Azure Advisor

B. Azure Monitor metrics

C. Azure Monitor action groups

D. Azure Log Analytics

ANSWER: D

Explanation:

Log Analytics is a tool in the Azure portal used to edit and run log queries with data in Azure Monitor Logs. You may write a simple query that returns a set of records and then use features of Log Analytics to sort, filter, and analyze them. Or you may write a more advanced query to perform statistical analysis and visualize the results in a chart to identify a particular trend.

Reference:

https://docs.microsoft.com/en-us/azure/azure-monitor/logs/log-analytics-overview

QUESTION NO: 24 - (Topic 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.

ANSWER: B D

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 NO: 25 - (Topic 5)

You have an Azure subscription that contains web apps 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 web apps 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

ANSWER: A

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 NO: 26 - (Topic 5)

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

ANSWER: C

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 NO: 27 - (DRAG DROP) - (Topic 5)

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:

ANSWER:

Explanation:

QUESTION NO: 28 - (HOTSPOT) - (Topic 5)

HOTSPOT

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

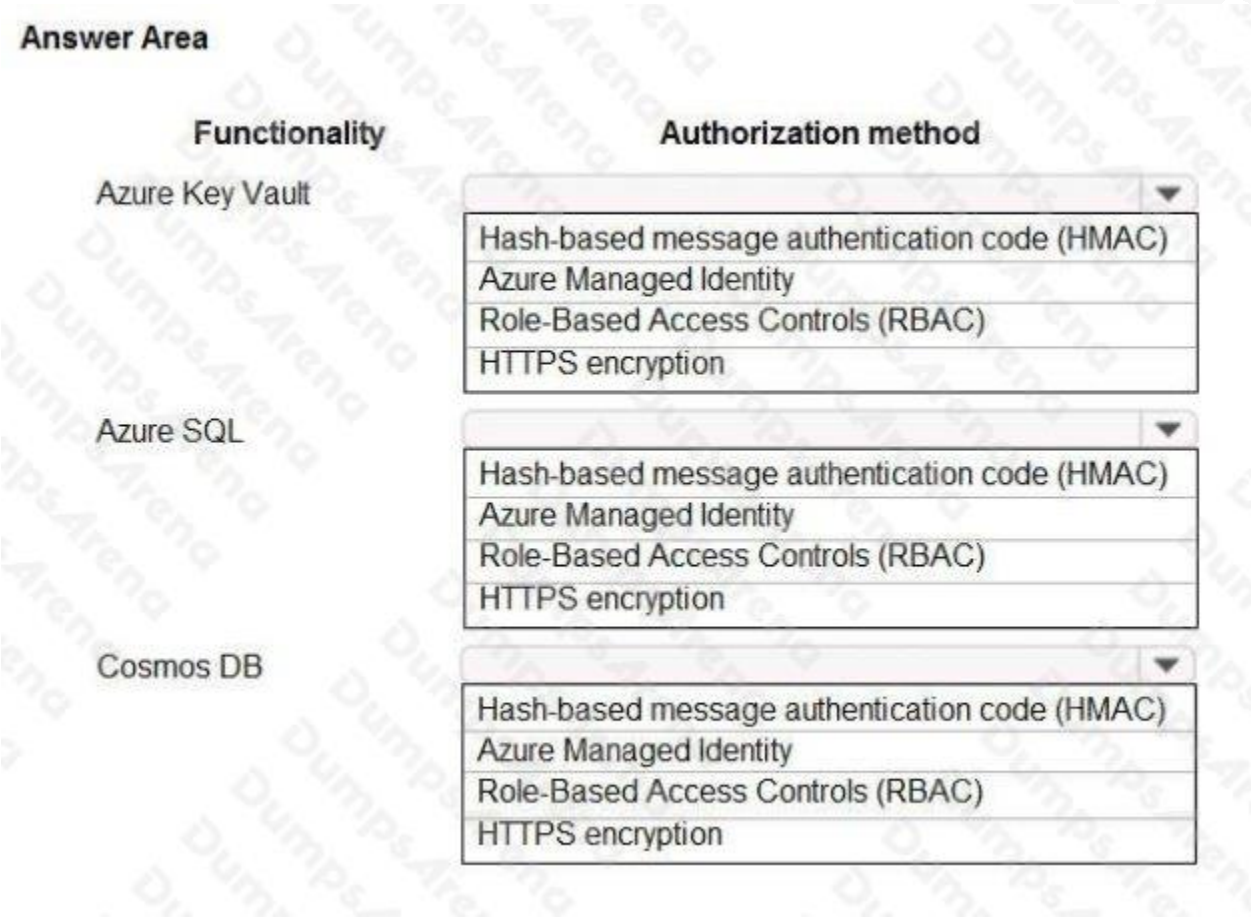
The application uses Azure Key Vault, Azure SQL Database, and Azure Cosmos DB.

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:

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

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 NO: 29 - (Topic 5)

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-AzRoleAssignment 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.

ANSWER: C

QUESTION NO: 30 - (DRAG DROP) - (Topic 5)

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.

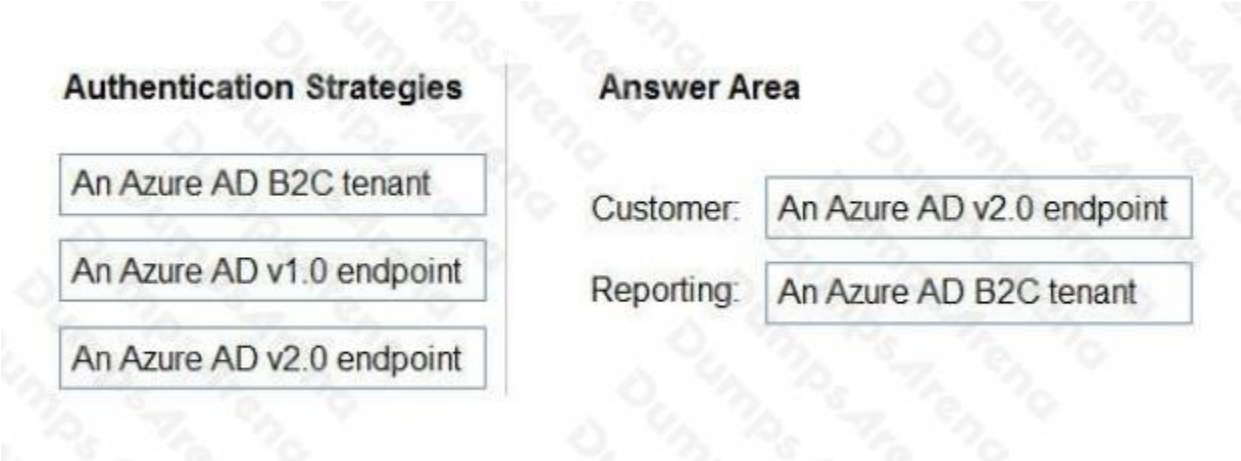
Application name	Requirement
Customer	Users must authenticate by using a personal Microsoft account and multi-factor authenication
Reporting	Users must authenticate by using either Contoso credentials or a personal Microsoft account. You must be able to manage the accounts from Azure AD.

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:

ANSWER:



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 NO: 31 - (HOTSPOT) - (Topic 5)

HOTSPOT

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

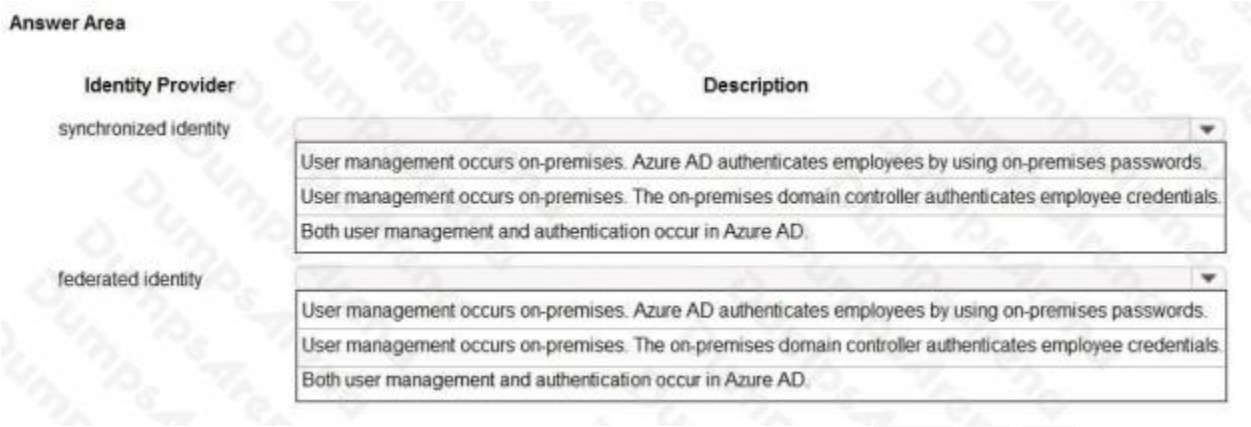
Employees are required to use different accounts when using on-premises or cloud resources. You must recommend a solution that lets employees sign in to all company resources by using a single account. The solution must implement an identity provider.

You need to provide guidance on the different identity providers.

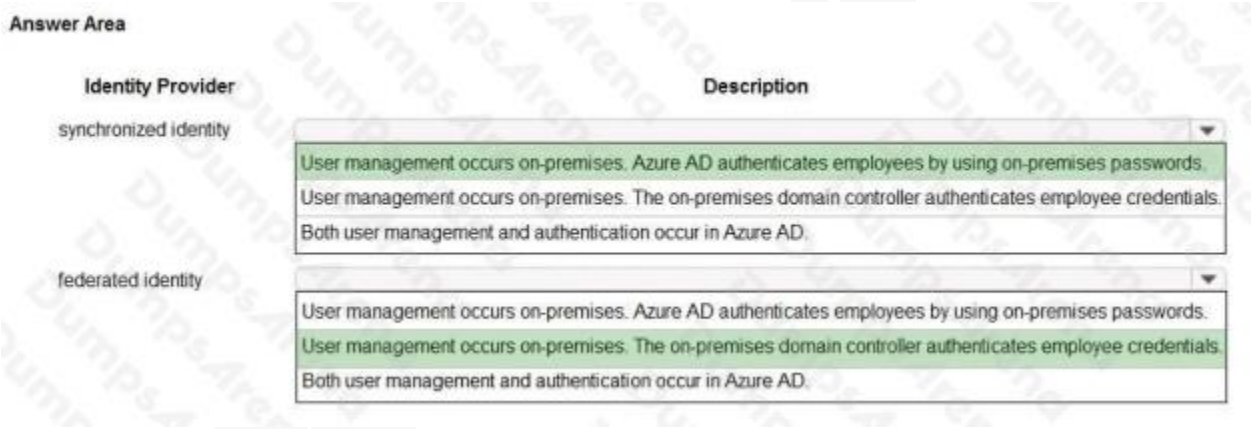
How should you describe each identity provider? To answer, select the appropriate description from each list in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



ANSWER:



Explanation:

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

Azure AD Domain Services for hybrid organizations

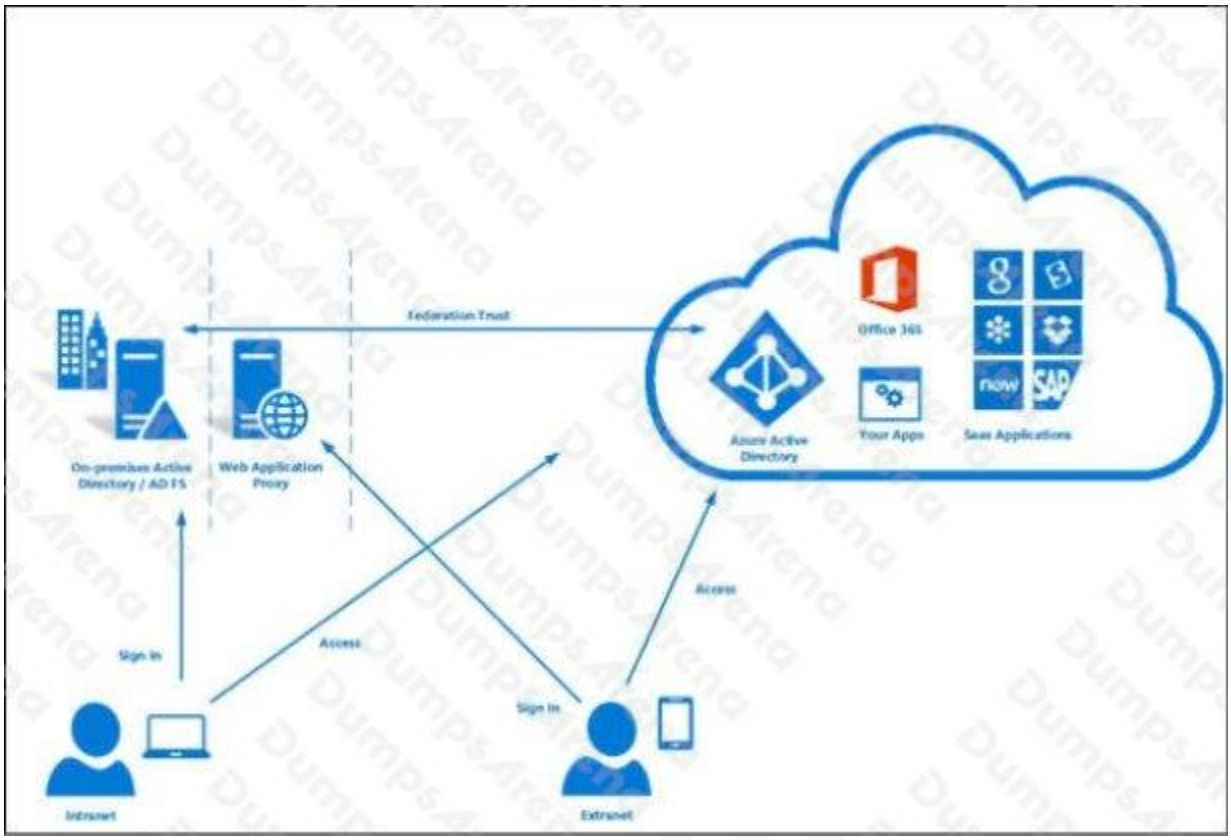
Organizations with a hybrid IT infrastructure consume a mix of cloud resources and on-premises resources. Such organizations synchronize identity information from their on-premises directory to their Azure AD tenant. As hybrid organizations look to migrate more of their on-premises applications to the 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.



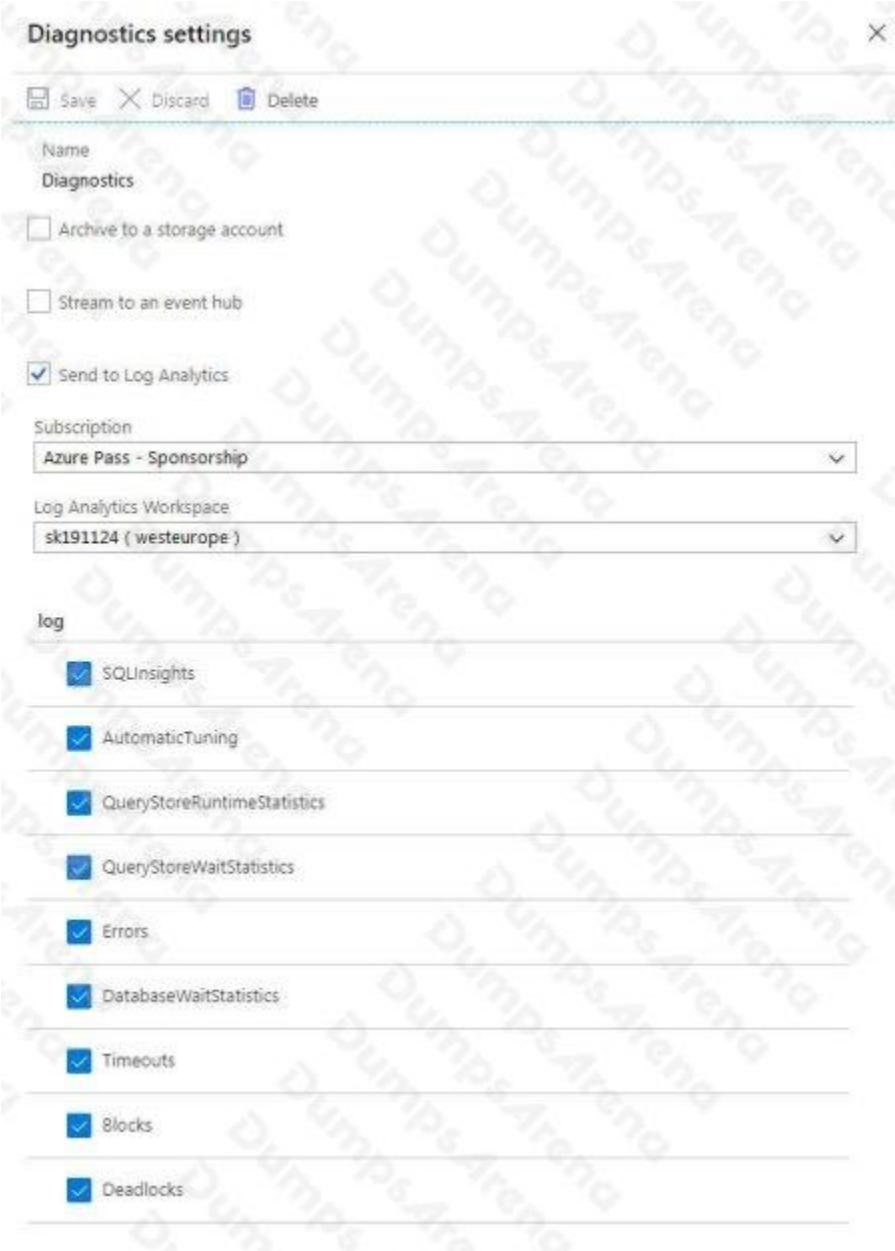
Reference:

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 NO: 32 - (HOTSPOT) - (Topic 5)

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

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

Explanation:

Design Data Storage

QUESTION NO: 33 - (Topic 5)

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

ANSWER: D

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 NO: 34 - (Topic 5)

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

ANSWER: A B D

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 NO: 35 - (Topic 5)

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)

ANSWER: B

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 NO: 36 - (HOTSPOT) - (Topic 5)

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

Topic	Value
HTTP methods	API methods GET only GET and POST only GET, POST, and OPTIONS only
Authorization level	Function Anonymous Admin

ANSWER:

Answer Area

Topic	Value
HTTP methods	API methods GET only GET and POST only GET, POST, and OPTIONS only
Authorization level	Function Anonymous Admin

Explanation:

HTTP 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 NO: 37 - (Topic 5)

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)

ANSWER: B

QUESTION NO: 38 - (DRAG DROP) - (Topic 5)

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:

ANSWER:

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 NO: 39 - (Topic 5)

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)

ANSWER: D

Explanation:

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

QUESTION NO: 40 - (HOTSPOT) - (Topic 5)

HOTSPOT

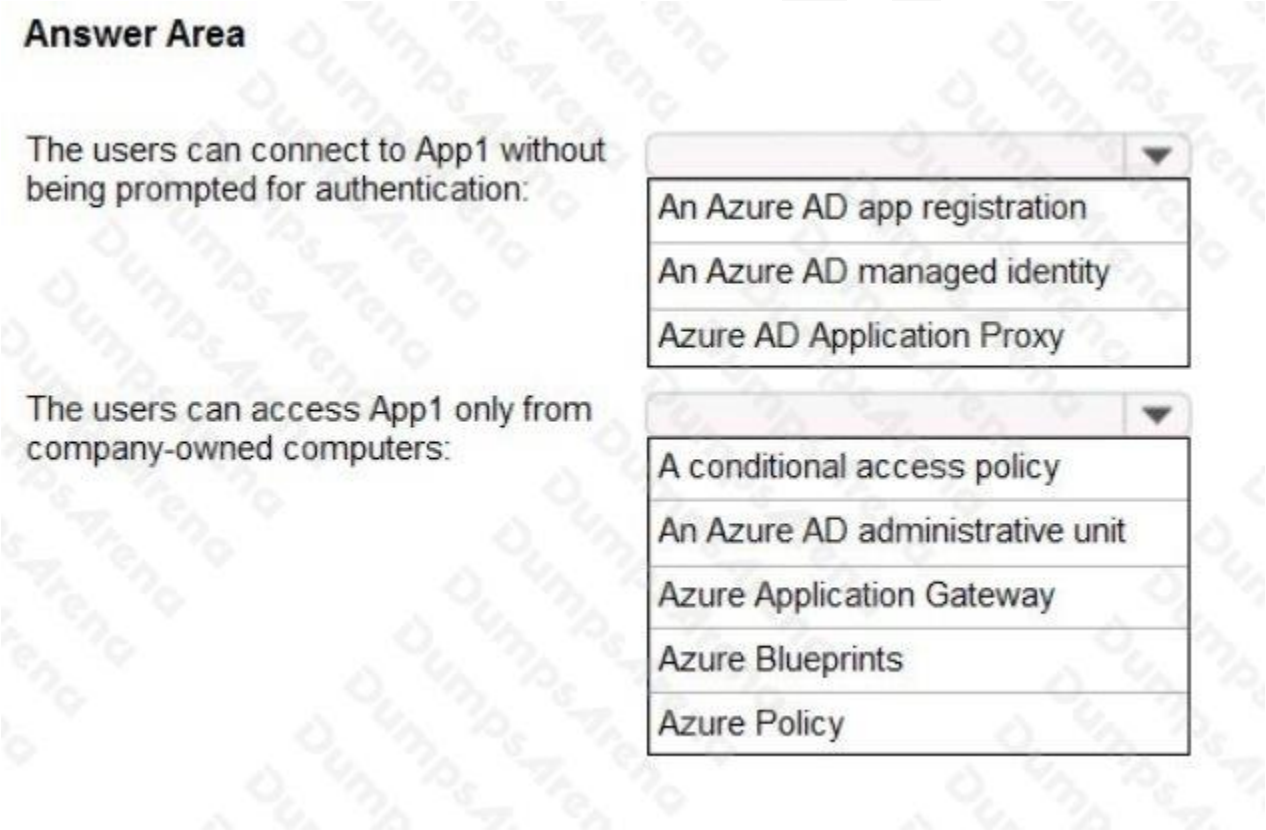
You plan to deploy an Azure web app named App1 that will use Azure Active Directory (Azure AD) authentication.

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:

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

Explanation:

Box 1: An Azure AD app registration

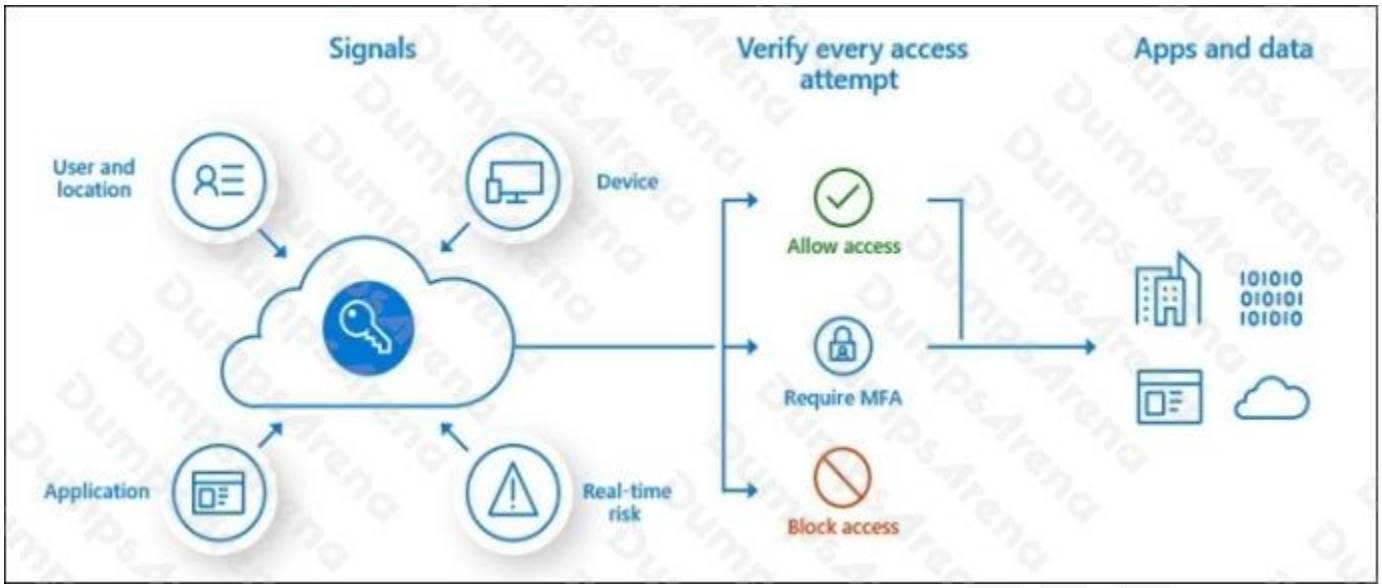
Azure active directory (AD) provides cloud based directory and identity management services.You can use azure AD to manage users of your application and authenticate access to your applications using azure active directory.

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 NO: 41 - (HOTSPOT) - (Topic 5)

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

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

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.

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

QUESTION NO: 42 - (Topic 5)

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)

ANSWER: B

QUESTION NO: 43 - (Topic 5)

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

ANSWER: D

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 NO: 44 - (HOTSPOT) - (Topic 5)

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

ANSWER:

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

Explanation:

QUESTION NO: 45 - (Topic 5)

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

ANSWER: B

Explanation:

Reference:

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

QUESTION NO: 46 - (HOTSPOT) - (Topic 5)

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:

DUMPSARENA

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

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

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 NO: 47 - (Topic 5)

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

ANSWER: B

QUESTION NO: 48 - (Topic 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 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

ANSWER: B

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 NO: 49 - (Topic 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 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

ANSWER: B

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 NO: 50 - (Topic 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 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

ANSWER: B

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 NO: 51 - (HOTSPOT) - (Topic 5)

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:

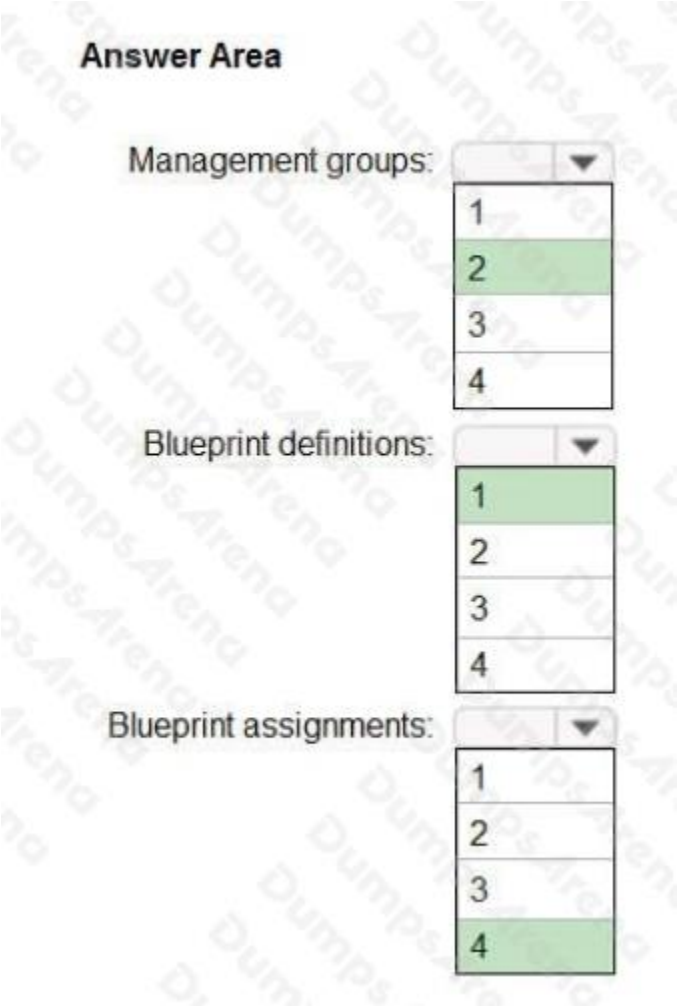
Answer Area

Management groups:
- 1
- 2
- 3
- 4

Blueprint definitions:
- 1
- 2
- 3
- 4

Blueprint assignments:
- 1
- 2
- 3
- 4

ANSWER:



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 NO: 52 - (Topic 5)

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

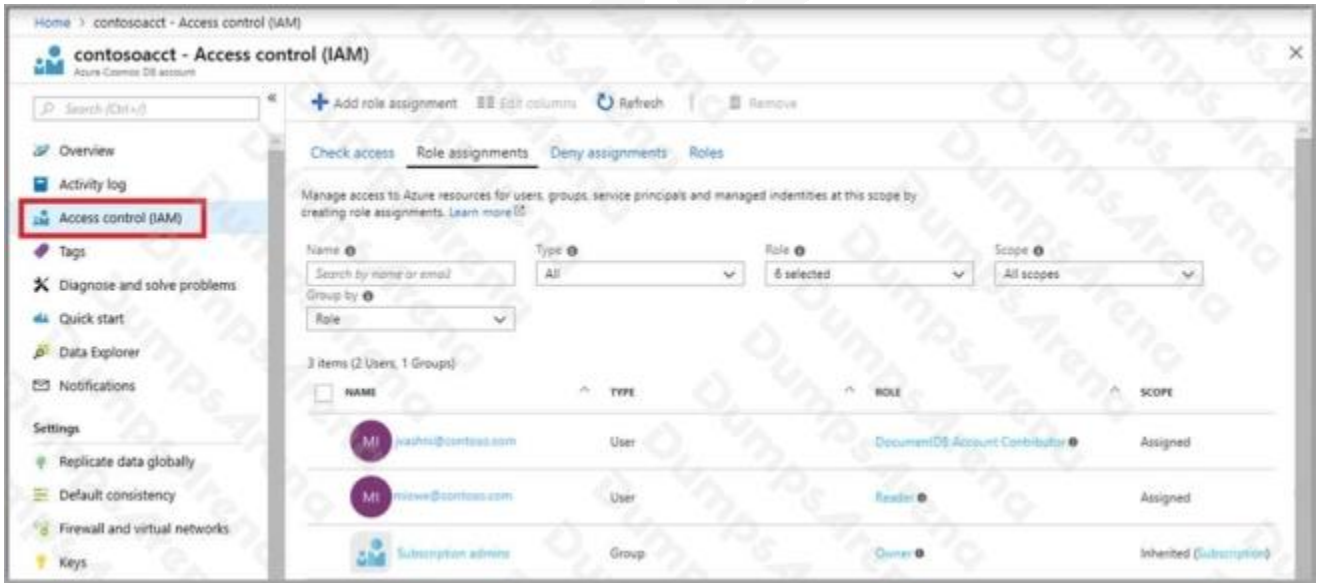
C. a resource token and an Access control (IAM) role assignment

D. master keys and Azure Information Protection policies

ANSWER: C

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 NO: 53 - (Topic 5)

You deploy an Azure virtual machine that runs an ASP.NET application. The application will be accessed from the internet by the users at your company.

You need to recommend a solution to ensure that the users are pre-authenticated by using their Azure Active Directory (Azure AD) account before they can connect to the ASP.NET application.

What should you include in the recommendation?

A. a public Azure Load Balancer

B. Azure Application Gateway

C. Azure Traffic Manager

D. an Azure AD enterprise application

ANSWER: D

Explanation:

You can manage service principals in the Azure portal through the Enterprise Applications experience. Service principals are what govern an application connecting to Azure AD and can be considered the instance of the application in your directory.

Reference:

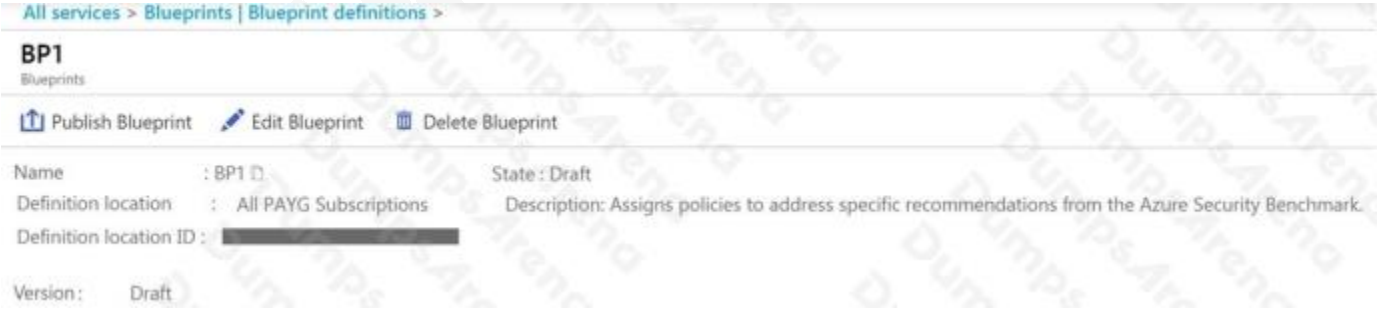
https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-how-applications-are-added

QUESTION NO: 54 - (HOTSPOT) - (Topic 5)

HOTSPOT

You have an Azure blueprint named BP1.

The properties of BP1 are shown in the Properties exhibit. (Click the Properties tab.)



The basic configuration of the blueprint is shown in the Basics exhibit. (Click the Basics tab.)

Basics Artifacts

Add artifacts to the blueprint. Add resource groups to organize where the artifacts should be deployed and assigned.

NAME	ARTIFACT TYPE	PARAMETERS	
Subscription			...
Audit Azure Security Benchmark recommendations and deploy specific supporting VM	Policy assignment	0 out of 12 parameters populated	...
Add artifact...			...
Database Resource Group	Resource group	0 out of 2 parameters populated	...
Add artifact...			...

The artifacts attached to BP1 are shown in the Artifacts exhibit. (Click the Artifacts tab.)

Edit blueprint

Basics Artifacts

Blueprint name

BP1

Blueprint description

Assigns policies to address specific recommendations from the Azure Security Benchmark.

Definition location*

...

The management group or subscription where the blueprint is saved. The definition location determines the scope that the blueprint may be assigned to. Learn more at aka.ms/BlueLocation.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
You can assign BP1 in its current state.	○	○
BP1 has a role assignment defined.	○	○
When BP1 is assigned, you will need to provide a resource group name.	○	○

ANSWER:

Answer Area

Statements	Yes	No
You can assign BP1 in its current state.	○	○
BP1 has a role assignment defined.	○	○
When BP1 is assigned, you will need to provide a resource group name.	○	○

Explanation:

Box 1: No

BP1 is in draft mode.

When a blueprint is first created, it's considered to be in Draft mode. When it's ready to be assigned, it needs to be Published.

Box 2: No

The BP1 artifacts include one Policy assignment and a Resource group, but no Role assignments.

Note: Blueprints are a declarative way to orchestrate the deployment of various resource templates and other artifacts such as:

Role Assignments

Policy Assignments

Azure Resource Manager templates (ARM templates) Resource Groups

Box 3: Yes

Yes, the BP1 artifacts include a Resource group.

Reference:

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

QUESTION NO: 55 - (Topic 5)

Your company wants to use an Azure Active Directory (Azure AD) hybrid identity solution.

You need to ensure that users can authenticate if the internet connection to the on-premises Active Directory is unavailable. The solution must minimize authentication prompts for the users.

What should you include in the solution?

A. password hash synchronization and Azure AD Seamless Single Sign-On (Azure AD Seamless SSO)

B. pass-through authentication and Azure AD Seamless Single Sign-On (Azure AD Seamless SSO)

C. an Active Directory Federation Services (AD FS) server

ANSWER: A

Explanation:

With Password hash synchronization + Seamless SSO the authentication is in the cloud.

Incorrect Answers:

Pass-through Authentication and federation rely on on-premises infrastructure.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/hybrid/choose-ad-authn

QUESTION NO: 56 - (HOTSPOT) - (Topic 5)

HOTSPOT

You need to design an Azure policy that will implement the following functionality:

- For new resources, assign tags and values that match the tags and values of the resource group to which the resources are deployed.

- For existing resources, identify whether the tags and values match the tags and values of the resource group that contains the resources. - For any non-compliant resources, trigger auto-generated remediation tasks to create missing tags and values.

The solution must use the principle of least privilege.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Azure Policy effect to use:

- Append
- EnforceOPAConstraint
- EnforceRegoPolicy
- Modify

Azure Active Directory (Azure AD) object and RBAC role to use for the remediation tasks:

- A managed identity with the Contributor role
- A managed identity with the User Access Administrator role
- A service principal with the Contributor role
- A service principal with the User Access Administrator role

ANSWER:

Answer Area

Azure Policy effect to use:

- Append
- EnforceOPAConstraint
- EnforceRegoPolicy
- Modify

Azure Active Directory (Azure AD) object and RBAC role to use for the remediation tasks:

- A managed identity with the Contributor role
- A managed identity with the User Access Administrator role
- A service principal with the Contributor role
- A service principal with the User Access Administrator role

Explanation:

Box 1: Modify

Modify is used to add, update, or remove properties or tags on a resource during creation or update. A common example is updating tags on resources such as costCenter. Existing noncompliant resources can be remediated with a remediation task. A single Modify rule can have any number of operations.

Incorrect Answers:

- The following effects are deprecated: EnforceOPAConstraint, EnforceRegoPolicy

- Append is used to add additional fields to the requested resource during creation or update. A common example is specifying allowed IPs for a storage resource.

Box 2: A managed identity with the Contributor role

- Managed identity

How remediation security works: When Azure Policy runs the template in the deployIfNotExists policy definition, it does so using a managed identity. Azure Policy creates a managed identity for each assignment, but must have details about what roles to grant the managed identity.

- Contributor role

The Contributor role grants the required access to apply tags to any entity.

Reference: https://docs.microsoft.com/en-us/azure/governance/policy/concepts/effects https://docs.microsoft.com/en-us/azure/governance/policy/how-to/remediate-resources https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/tag-resources

QUESTION NO: 57 - (Topic 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.

Your company has an on-premises Active Directory Domain Services (AD DS) domain and an established Azure Active Directory (Azure AD) environment.

Your company would like users to be automatically signed in to cloud apps when they are on their corporate desktops that are connected to the corporate network.

You need to enable single sign-on (SSO) for company users.

Solution: Install and configure an Azure AD Connect server to use password hash synchronization and select the “Enable single sign-on” option.

Does the solution meet the goal?

A. Yes

B. No

ANSWER: A

Explanation:

Azure Active Directory Seamless Single Sign-On (Azure AD Seamless SSO) automatically signs users in when they are on their corporate devices connected to your corporate network. When enabled, users don't need to type in their passwords to sign in to Azure AD, and usually, even type in their usernames. This feature provides your users easy access to your cloud-based applications without needing any additional on-premises components.

Seamless SSO can be combined with either the Password Hash Synchronization or Pass-through Authentication sign-in methods.

Reference:

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

QUESTION NO: 58 - (Topic 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.

Your company has an on-premises Active Directory Domain Services (AD DS) domain and an established Azure Active Directory (Azure AD) environment.

Your company would like users to be automatically signed in to cloud apps when they are on their corporate desktops that are connected to the corporate network.

You need to enable single sign-on (SSO) for company users.

Solution: Install and configure an Azure AD Connect server to use pass-through authentication and select the “Enable single sign-on” option.

Does the solution meet the goal?

A. Yes

B. No

ANSWER: A

Explanation:

Azure Active Directory Seamless Single Sign-On (Azure AD Seamless SSO) automatically signs users in when they are on their corporate devices connected to your corporate network. When enabled, users don't need to type in their passwords to sign in to Azure AD, and usually, even type in their usernames. This feature provides your users easy access to your cloud-based applications without needing any additional on-premises components.

Seamless SSO can be combined with either the Password Hash Synchronization or Pass-through Authentication sign-in methods.

Reference:

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

QUESTION NO: 59 - (Topic 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.

Your company has an on-premises Active Directory Domain Services (AD DS) domain and an established Azure Active Directory (Azure AD) environment.

Your company would like users to be automatically signed in to cloud apps when they are on their corporate desktops that are connected to the corporate network.

You need to enable single sign-on (SSO) for company users.

Solution: Configure an AD DS server in an Azure virtual machine (VM). Configure bidirectional replication.

Does the solution meet the goal?

A. Yes

B. No

ANSWER: B

Explanation:

Instead install and configure an Azure AD Connect server.

Reference:

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

QUESTION NO: 60 - (Topic 5)

You are designing an Azure web app that will use Azure Active Directory (Azure AD) for authentication.

You need to recommend a solution to provide users from multiple Azure AD tenants with access to App1. The solution must ensure that the users use Azure Multi-Factor Authentication (MFA) when they connect to App1.

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

NOTE: Each correct selection is worth one point.

A. Azure AD conditional access policies

B. Azure AD managed identities

C. an Identity Experience Framework policy

D. an Azure application security group

E. an Endpoint Manager app protection policy

F. Azure AD guest accounts

ANSWER: A F

Explanation:

A: The Conditional Access feature in Azure Active Directory (Azure AD) offers one of several ways that you can use to secure your app and protect a service. Conditional Access enables developers and enterprise customers to protect services in a multitude of ways including:

- Multi-factor authentication
- Allowing only Intune enrolled devices to access specific services
- Restricting user locations and IP ranges

Conditional Access policies are powerful tools, we recommend excluding the following accounts from your policy:

- Service accounts and service principals.

If your organization has these accounts in use in scripts or code, consider replacing them with managed identities.

Incorrect Answers:

B: Managed Identity does not support cross-directory scenarios.

E: Application security groups enable you to configure network security as a natural extension of an application's structure, allowing you to group virtual machines and define network security policies based on those groups.

Note: The correct options should be application registration with Azure, this will allow the authentication of users on the AD to access the application. A default application registration validates that the user has valid login credentials. This can be your Active Directory or in case of a multi-tenant application the directory where the user is originated from.

Reference: https://docs.microsoft.com/en-us/azure/active-directory/develop/v2-conditional-access-dev-guide https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-azure-management https://www.re-mark-able.net/understanding-azure-active-directory-application-registrations/

QUESTION NO: 61 - (Topic 5)

You need to create an Azure Storage account that uses a custom encryption key.

What do you need to implement the encryption?

A. a certificate issued by an integrated certification authority (CA) and stored in Azure Key Vault

B. a managed identity that is configured to access the storage account

C. an Azure Active Directory Premium subscription

D. an Azure key vault in the same Azure region as the storage account

ANSWER: A

Explanation:

You can use your own encryption key to protect the data in your storage account. When you specify a customer-managed key, that key is used to protect and control access to the key that encrypts your data.

You must use either Azure Key Vault or Azure Key Vault Managed Hardware Security Model (HSM) (preview) to store your customer-managed keys.

QUESTION NO: 62 - (HOTSPOT) - (Topic 5)

HOTSPOT

You plan to create an Azure environment that will have a root management group and five 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.

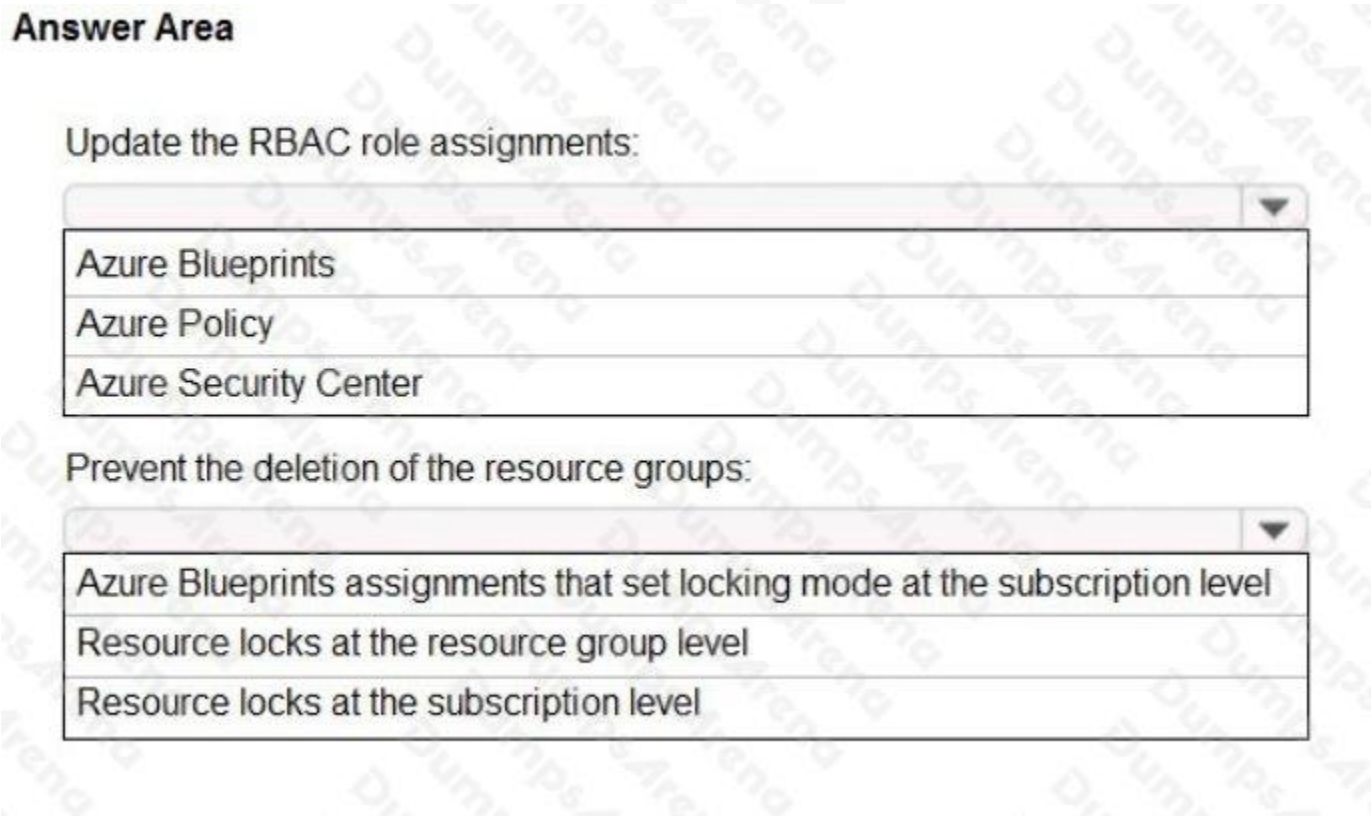
You need to design a solution for the planned environment. The solution must meet the following requirements:

▪ Prevent users who are assigned the Owner role for the subscriptions from deleting the resource groups from their respective subscription. ▪ Ensure that you can update RBAC role assignments across all the subscriptions and resource groups. ▪ Minimize administrative effort.

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:

Answer Area

Update the RBAC role assignments:

- Azure Blueprints
- Azure Policy
- Azure Security Center

Prevent the deletion of the resource groups:

- Azure Blueprints assignments that set locking mode at the subscription level
- Resource locks at the resource group level
- Resource locks at the subscription level

Explanation:

Box 1: Azure Blueprints

Blueprints are a declarative way to orchestrate the deployment of various resource templates and other artifacts such as:

Role Assignments

Policy Assignments

Azure Resource Manager templates (ARM templates) Resource Groups

Incorrect:

A policy is a default allow and explicit deny system focused on resource properties during deployment and for already existing resources.

Box 2: Resource locks at the subscription level

To minimize administrative effort lock at the subscription level.

Note: As an administrator, you can lock a subscription, resource group, or resource to prevent other users in your organization from accidentally deleting or modifying critical resources.

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

QUESTION NO: 63 - (Topic 5)

Your company has the divisions shown in the following table.

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

Sub1 contains an Azure web app that runs an ASP.NET application named App1. App1 uses the Microsoft identity platform (v2.0) to handle user authentication. Users from east.contoso.com can authenticate to App1.

You need to recommend a solution to allow users from west.contoso.com to authenticate to App1.

What should you recommend for the west.contoso.com Azure AD tenant?

A. a conditional access policy

B. pass-through authentication

C. guest accounts

D. an app registration

ANSWER: D

Explanation:

There are several components that make up the Microsoft identity platform:

- OAuth 2.0 and OpenID Connect standard-compliant authentication service
- Application management portal: A registration and configuration experience in the Azure portal, along with the other Azure management capabilities.

You register an application using the App registrations experience in the Azure portal so that your app can be integrated with the Microsoft identity platform and call Microsoft Graph.

Reference: https://docs.microsoft.com/en-us/azure/active-directory/develop/v2-overview https://docs.microsoft.com/en-us/graph/auth-register-app-v2

QUESTION NO: 64 - (Topic 5)

You have an Azure Active Directory (Azure AD) tenant named contoso.com that has a security group named Group1. Group1 is configured for assigned membership. Group1 has 50 members, including 20 guest users.

You need to recommend a solution for evaluating the membership of Group1. The solution must meet the following requirements:

- The evaluation must be repeated automatically every three months.
- Every member must be able to report whether they need to be in Group1.

- Users who report that they do not need to be in Group1 must be removed from Group1 automatically.
- Users who do not report whether they need to be in Group1 must be removed from Group1 automatically.

What should you include in the recommendation?

A. Change the Membership type of Group1 to Dynamic User.

B. Implement Azure AD Privileged Identity Management.

C. Implement Azure AD Identity Protection.

D. Create an access review.

ANSWER: A

Explanation:

In Azure Active Directory (Azure AD), you can create complex attribute-based rules to enable dynamic memberships for groups. Dynamic group membership reduces the administrative overhead of adding and removing users.

When any attributes of a user or device change, the system evaluates all dynamic group rules in a directory to see if the change would trigger any group adds or removes. If a user or device satisfies a rule on a group, they are added as a member of that group. If they no longer satisfy the rule, they are removed.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/groups-dynamic-membership

QUESTION NO: 65 - (Topic 5)

Your company purchases an app named App1.

You need to recommend a solution to ensure that App1 can read and modify access reviews.

What should you recommend?

A. From API Management services, publish the API of App1, and then delegate permissions to the Microsoft Graph API.

B. From the Azure Active Directory admin center, register App1. From the Access control (IAM) blade, delegate permissions.

C. From the Azure Active Directory admin center, register App1, and then delegate permissions to the Microsoft Graph API.

D. From API Management services, publish the API of App1. From the Access control (IAM) blade, delegate permissions.

ANSWER: B

Explanation:

The app must be registered. You can register the application in the Azure Active Directory admin center.

The Azure AD access reviews feature has an API in the Microsoft Graph endpoint.

You can register an Azure AD application and set it up for permissions to call the access reviews API in Graph.

Reference: https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-register-app

QUESTION NO: 66 - (Topic 5)

You have 200 resource groups across 20 Azure subscriptions.

Your company's security policy states that the security administrator must verify all assignments of the Owner role for the subscriptions and resource groups once a month. All assignments that are not approved by the security administrator must be removed automatically. The security administrator must be prompted every month to perform the verification.

What should you use to implement the security policy?

A. Identity Secure Score in Azure Security Center

B. Access reviews in Identity Governance

C. the user risk policy in Azure Active Directory (Azure AD) Identity Protection

D. role assignments in Azure Active Directory (Azure AD) Privileged Identity Management (PIM)

ANSWER: B

Explanation:

Azure Active Directory (Azure AD) access reviews enable organizations to efficiently manage group memberships, access to enterprise applications, and role assignments. User's access can be reviewed on a regular basis to make sure only the right people have continued access.

Reference:

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

QUESTION NO: 67 - (HOTSPOT) - (Topic 5)

HOTSPOT

Your company has 20 web APIs that were developed in-house.

The company is developing 10 web apps that will use the web APIs. The web apps and the APIs are registered in the company's Azure Active Directory (Azure AD) tenant. The web APIs are published by using Azure API Management.

You need to recommend a solution to block unauthorized requests originating from the web apps from reaching the web APIs. The solution must meet the following requirements:

- Use Azure AD-generated claims.
- Minimize configuration end management effort.

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

Grant permissions to allow the web apps to access the web APIs by using:

- Azure AD
- Azure API Management
- The web APIs

Configure a JSON Web Token (JWT) validation policy by using:

- Azure AD
- Azure API Management
- The web APIs

ANSWER:

Answer Area

Grant permissions to allow the web apps to access the web APIs by using:

- Azure AD
- Azure API Management
- The web APIs

Configure a JSON Web Token (JWT) validation policy by using:

- Azure AD
- Azure API Management
- The web APIs

Explanation:

QUESTION NO: 68 - (HOTSPOT) - (Topic 5)

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

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

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

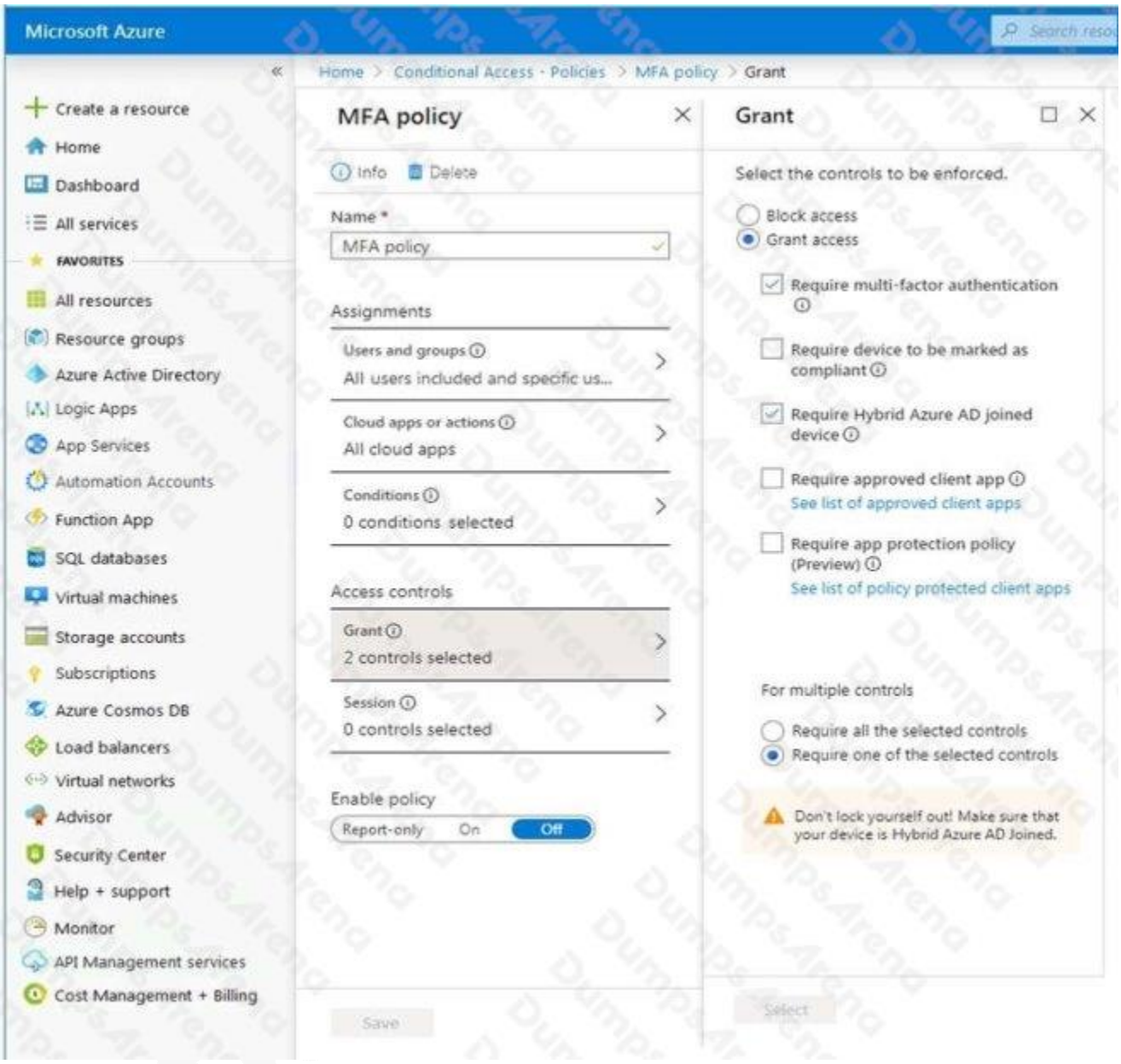
Azure role-based access control (Azure RBAC) is the authorization system you use to manage access to Azure resources. To grant access, you assign roles to users, groups, service principals, or managed identities at a particular scope.

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

QUESTION NO: 69 - (Topic 5)

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.

ANSWER: B

Explanation:

Either the device should be joined to Azure AD or MFA must be used.

QUESTION NO: 70 - (HOTSPOT) - (Topic 5)

HOTSPOT

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

You plan to use Azure Monitor to monitor user sign-ins and generate alerts based on specific user sign-in events.

You need to recommend a solution to trigger the alerts based on the events.

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

Send Azure AD logs to:
- An Azure event hub
- An Azure Log Analytics workspace
- An Azure Storage account

Signal type to use for triggering the alerts:
- Activity log
- Log
- Metric

ANSWER:

Answer Area

Send Azure AD logs to:
- An Azure event hub
- An Azure Log Analytics workspace
- An Azure Storage account

Signal type to use for triggering the alerts:
- Activity log
- Log
- Metric

Explanation:

Box 1: An Azure Log Analytics workspace

To be able to create an alert we send the Azure AD logs to An Azure Log Analytics workspace.

Note: You can forward your AAD logs and events to either an Azure Storage Account, an Azure Event Hub, Log Analytics, or a combination of all of these.

Box 2: Log

Ensure Resource Type is an analytics source like Log Analytics or Application Insights and signal type as Log.

Reference:

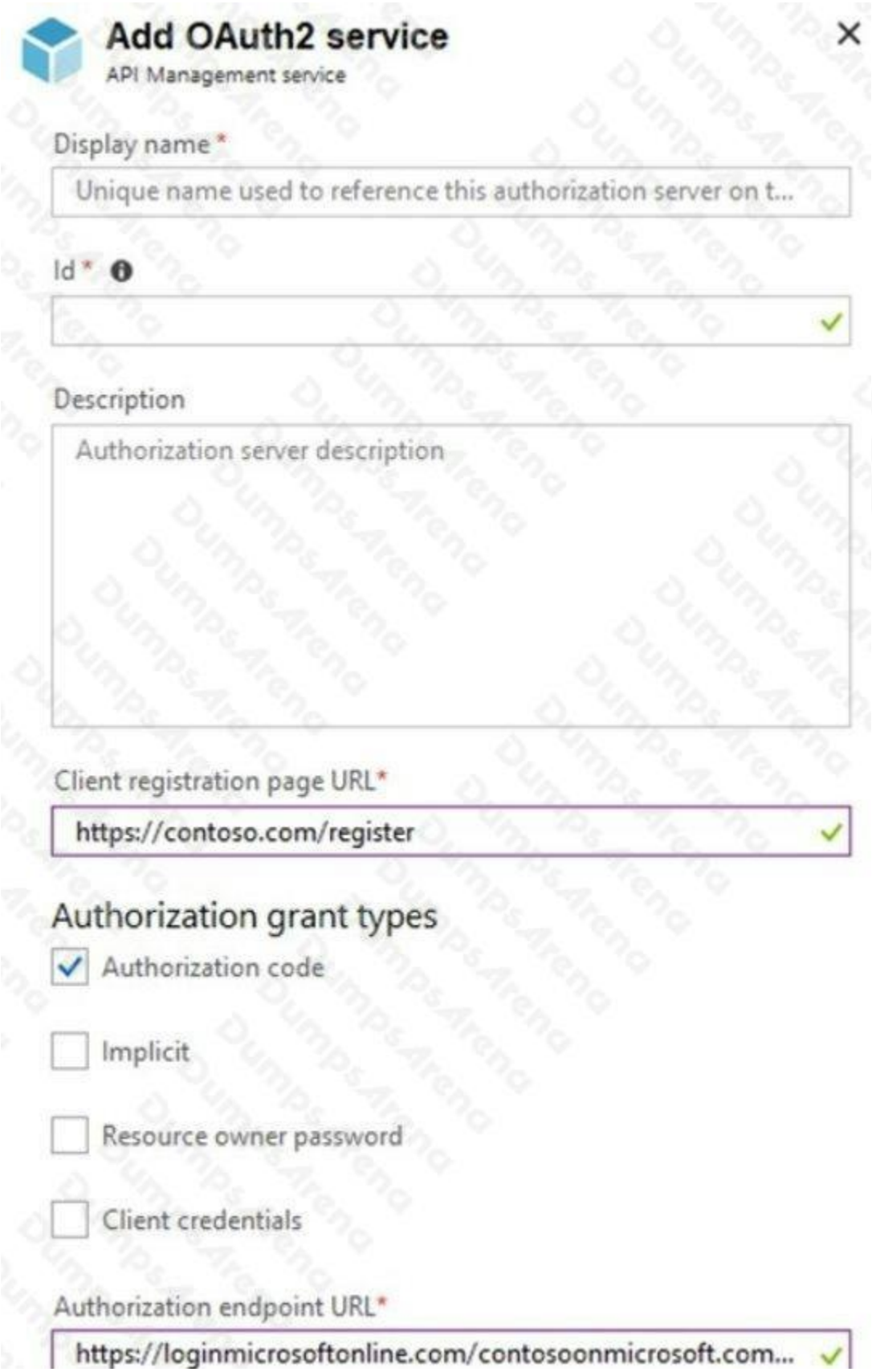
https://4sysops.com/archives/how-to-create-an-azure-ad-admin-login-alert/ https://docs.microsoft.com/en-us/azure/azure-monitor/platform/alerts-log

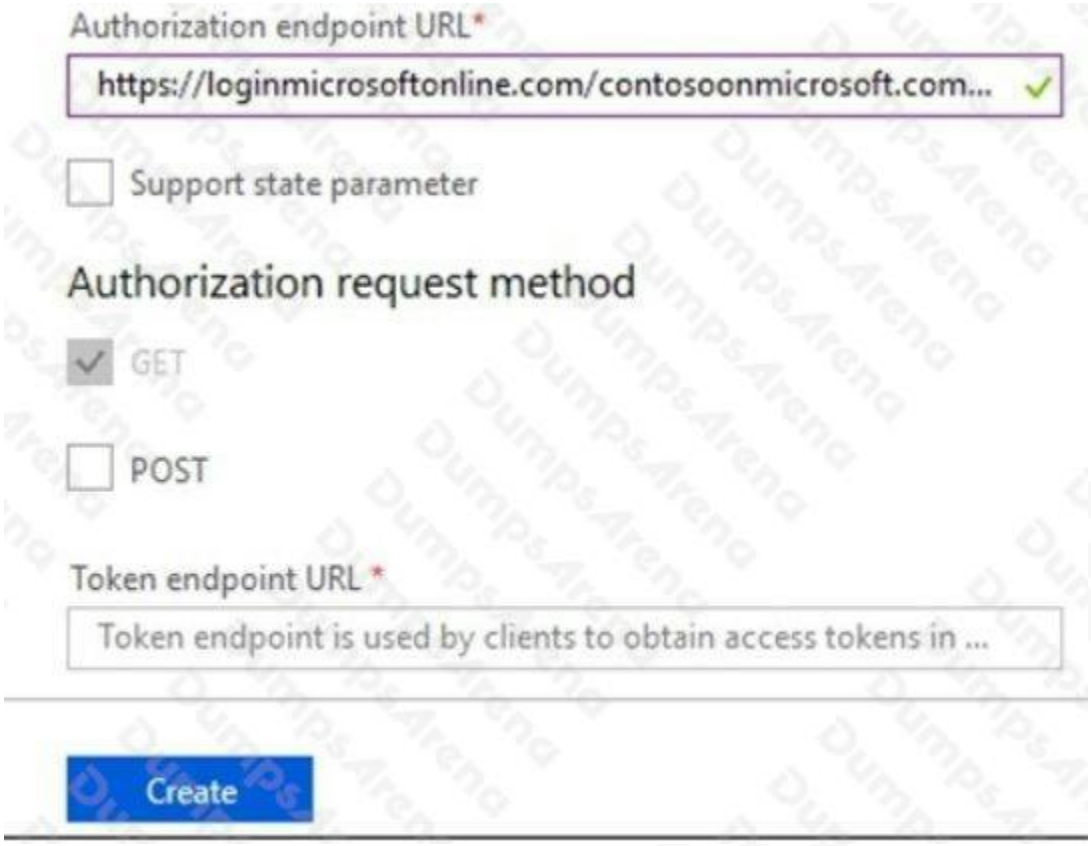
QUESTION NO: 71 - (HOTSPOT) - (Topic 5)

HOTSPOT

You configure OAuth2 authorization in API Management as shown in the following exhibit.

DUMPSARENA


Add OAuth2 service
API Management service
Display name *
Unique name used to reference this authorization server on t...
Id *
Description
Authorization server description
Client registration page URL*
https://contoso.com/register
Authorization grant types
Authorization code
Implicit
Resource owner password
Client credentials
Authorization endpoint URL*
https://loginmicrosoftonline.com/contosoonmicrosoft.com...



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

The selected authorization grant type is for **[answer choice]**.

- Background services
- Headless device authentication
- Web applications

To enable custom data in the grant flow, select **[answer choice]**.

- Client credentials
- Resource owner password
- Support state parameter

ANSWER:

Answer Area

The selected authorization grant type is for **[answer choice]**.

- Background services
- Headless device authentication
- Web applications

To enable custom data in the grant flow, select **[answer choice]**.

- Client credentials
- Resource owner password
- Support state parameter

Explanation:

Box 1: Web applications

The Authorization Code Grant Type is used by both web apps and native apps to get an access token after a user authorizes an app.

Note: The Authorization Code grant type is used by confidential and public clients to exchange an authorization code for an access token.

After the user returns to the client via the redirect URL, the application will get the authorization code from the URL and use it to request an access token.

Incorrect Answers:

Not Headless device authentication:

A headless system is a computer that operates without a monitor, graphical user interface (GUI) or peripheral devices, such as keyboard and mouse.

Headless computers are usually embedded systems in various devices or servers in multi-server data center environments. Industrial machines, automobiles, medical equipment, cameras, household appliances, airplanes, vending machines and toys are among the myriad possible hosts of embedded systems.

Box 2: Client Credentials

How to include additional client data

In case you need to store additional details about a client that don't fit into the standard parameter set the custom data parameter comes to help:

POST /c2id/clients HTTP/1.1

Host: demo.c2id.com

Content-Type: application/json

Authorization: Bearer ztucZS1ZyFKgh0tUEruUtiSTXhnexmd6

{

"redirect_uris" : ["https://myapp.example.com/callback"],

"data" : { "reg_type" : "3rd-party",

"approved" : true,

"author_id" : 792440 }

}

The data parameter permits arbitrary content packaged in a JSON object. To set it you will need the master registration token or a one-time access token with a client-reg:data scope.

Incorrect Answers:

Authorization protocols provide a state parameter that allows you to restore the previous state of your application. The state parameter preserves some state object set by the client in the Authorization request and makes it available to the client in the response.

Reference: https://developer.okta.com/blog/2018/04/10/oauth-authorization-code-grant-type
https://connect2id.com/products/server/docs/guides/client-registration

Design Data Storage

QUESTION NO: 72 - (Topic 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.

Your company has deployed several virtual machines (VMs) on-premises and to Azure. Azure ExpressRoute has been deployed and configured for on-premises to Azure connectivity.

Several VMs are exhibiting network connectivity issues.

You need to analyze the network traffic to determine whether packets are being allowed or denied to the VMs.

Solution: Use Azure Network Watcher to run IP flow verify to analyze the network traffic.

Does the solution meet the goal?

A. Yes

B. No

ANSWER: A

Explanation:

The Network Watcher Network performance monitor is a cloud-based hybrid network monitoring solution that helps you monitor network performance between various points in your network infrastructure. It also helps you monitor network connectivity to service and application endpoints and monitor the performance of Azure ExpressRoute.

Note:

IP flow verify checks if a packet is allowed or denied to or from a virtual machine. The information consists of direction, protocol, local IP, remote IP, local port, and remote port. If the packet is denied by a security group, the name of the rule that

denied the packet is returned. While any source or destination IP can be chosen, IP flow verify helps administrators quickly diagnose connectivity issues from or to the internet and from or to the on-premises environment.

IP flow verify looks at the rules for all Network Security Groups (NSGs) applied to the network interface, such as a subnet or virtual machine NIC. Traffic flow is then verified based on the configured settings to or from that network interface. IP flow verify is useful in confirming if a rule in a Network Security Group is blocking ingress or egress traffic to or from a virtual machine.

Reference: https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-monitoring-overview
https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-ip-flow-verify-overview

QUESTION NO: 73 - (Topic 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.

Your company has deployed several virtual machines (VMs) on-premises and to Azure. Azure ExpressRoute has been deployed and configured for on-premises to Azure connectivity.

Several VMs are exhibiting network connectivity issues.

You need to analyze the network traffic to determine whether packets are being allowed or denied to the VMs.

Solution: Use the Azure Advisor to analyze the network traffic.

Does the solution meet the goal?

A. Yes

B. No

ANSWER: B

Explanation:

Instead use Azure Network Watcher to run IP flow verify to analyze the network traffic.

Note: Advisor is a personalized cloud consultant that helps you follow best practices to optimize your Azure deployments. It analyzes your resource configuration and usage telemetry and then recommends solutions that can help you improve the cost effectiveness, performance, high availability, and security of your Azure resources.

With Advisor, you can:

Get proactive, actionable, and personalized best practices recommendations.

Improve the performance, security, and high availability of your resources, as you identify opportunities to reduce your overall Azure spend. Get recommendations with proposed actions inline.

Reference:

https://docs.microsoft.com/en-us/azure/advisor/advisor-overview

QUESTION NO: 74 - (Topic 5)

You have 500 Azure web apps in the same Azure region. The apps use a premium Azure key vault for authentication.

A developer reports that some authentication requests are being throttled.

You need to recommend a solution to increase the available throughput of the key vault. The solution must minimize costs.

What should you recommend?

A. Change the pricing tier.

B. Configure geo-replication.

C. Configure load balancing for the apps.

D. Increase the number of key vaults in the subscription.

ANSWER: D

Explanation:

To maximize your Key Vault through put rates, here are some recommended guidelines/best practices for maximizing your throughput:

1. Ensure you have throttling in place. Client must honor exponential back-off policies for 429's and ensure you are doing retries as per the guidance below.

2. Divide your Key Vault traffic amongst multiple vaults and different regions. Use a separate vault for each security/availability domain. If you have five apps, each in two regions, then we recommend 10 vaults each containing the secrets unique to app and region.

Reference:

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

QUESTION NO: 75 - (DRAG DROP) - (Topic 5)

DRAG DROP

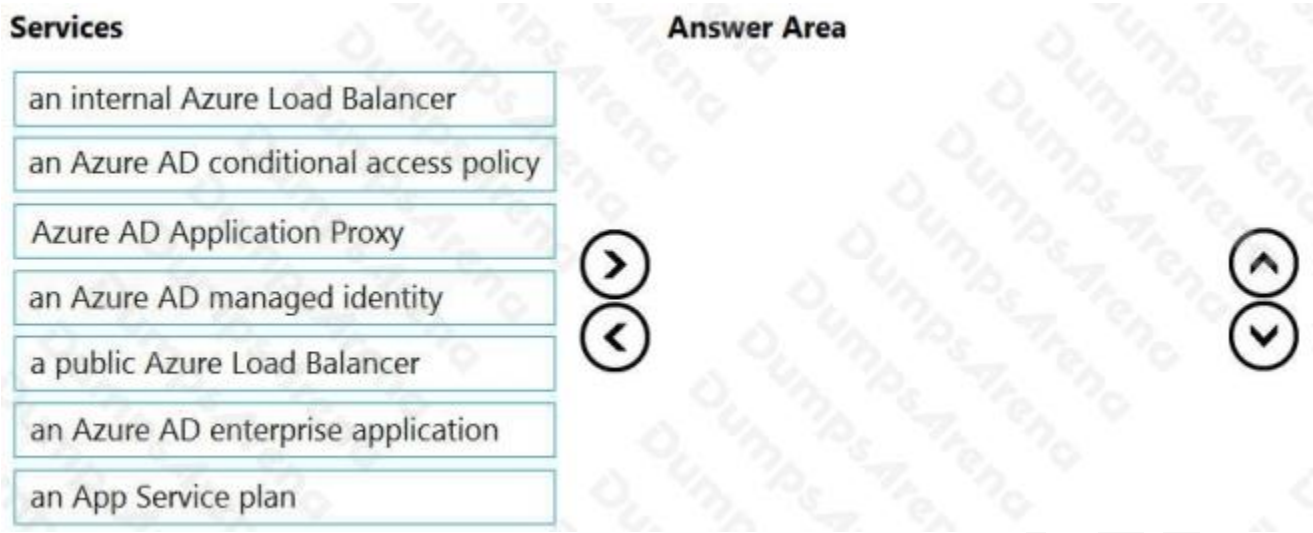
Your on-premises network contains a server named Server1 that runs an ASP.NET application named App1.

You have a hybrid deployment of Azure Active Directory (Azure AD).

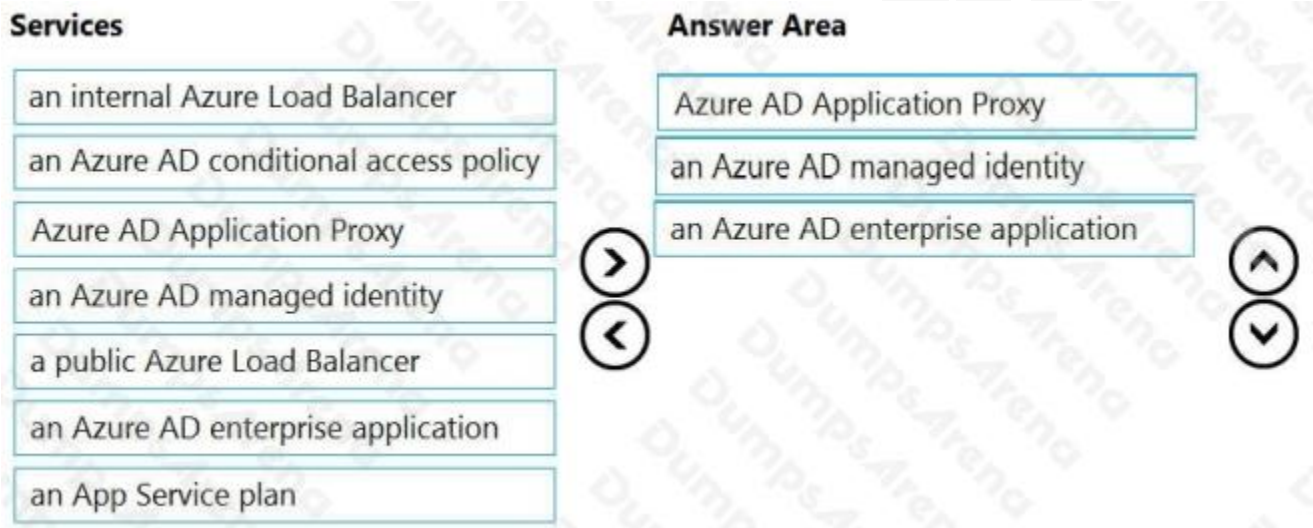
You need to recommend a solution to ensure that users sign in by using their Azure AD account and Azure Multi-Factor Authentication (MFA) when they connect to App1 from the internet.

Which three Azure services should you recommend be deployed and configured in sequence? To answer, move the appropriate services from the list of services to the answer area and arrange them in the correct order.

Select and Place:



ANSWER:



Explanation:

Step 1: Azure AD Application proxy

Azure AD Application Proxy is a prerequisite for a scenario with an on-premises legacy applications published for cloud access,

Note: 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.

Step 2: an Azure AD managed identity

Microsoft's identity solutions span on-premises and cloud-based capabilities. These solutions create a common user identity for authentication and authorization to all resources, regardless of location. We call this hybrid identity.

Step 3: an Azure AD conditional access policy

Conditional Access is the tool used by Azure Active Directory to bring signals together, to make decisions, and enforce organizational policies. Conditional Access is at the heart of the new identity driven control plane.

With hybrid identity to Azure AD and hybrid identity management these scenarios become possible.

Reference:

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

QUESTION NO: 76 - (Topic 5)

A company named Contoso, Ltd. has an Azure Active Directory (Azure AD) tenant that is integrated with Microsoft 365 and an Azure subscription.

Contoso has an on-premises identity infrastructure. The infrastructure includes servers that run Active Directory Domain Services (AD DS), Active Directory Federation Services (AD FS), Azure AD Connect, and Microsoft Identity Manager (MIM).

Contoso has a partnership with a company named Fabrikam, Inc. Fabrikam has an Active Directory forest and a Microsoft 365 tenant. Fabrikam has the same on-premises identity infrastructure components as Contoso.

A team of 10 developers from Fabrikam will work on an Azure solution that will be hosted in the Azure subscription of Contoso. The developers must be added to the Contributor role for a resource group in the Contoso subscription.

You need to recommend a solution to ensure that Contoso can assign the role to the 10 Fabrikam developers. The solution must ensure that the Fabrikam developers use their existing credentials to access resources.

What should you recommend?

A. In the Azure AD tenant of Contoso, enable Azure Active Directory Domain Services (Azure AD DS). Create a one-way forest trust that uses selective authentication between the Active Directory forests of Contoso and Fabrikam.

B. In the Azure AD tenant of Contoso, create cloud-only user accounts for the Fabrikam developers.

C. Configure a forest trust between the on-premises Active Directory forests of Contoso and Fabrikam.

D. In the Azure AD tenant of Contoso, use MIM to create guest accounts for the Fabrikam developers.

ANSWER: C

Explanation:

Trust configurations - Configure trust from managed forests(s) or domain(s) to the administrative forest ▪ A one-way trust is required from production environment to the admin forest.

▪ Selective authentication should be used to restrict accounts in the admin forest to only logging on to the appropriate production hosts.

Reference:

https://docs.microsoft.com/en-us/windows-server/identity/securing-privileged-access/securing-privileged-access-reference-material

QUESTION NO: 77 - (Topic 5)

You are designing an Azure governance solution.

All Azure resources must be easily identifiable based on the following operational information: environment, owner, department, and cost center.

You need to ensure that you can use the operational information when you generate reports for the Azure resources.

What should you include in the solution?

A. an Azure data catalog that uses the Azure REST API as a data source

B. Azure Active Directory (Azure AD) administrative units

C. an Azure management group that uses parent groups to create a hierarchy

D. an Azure policy that enforces tagging rules

ANSWER: D

Explanation:

You use Azure Policy to enforce tagging rules and conventions. By creating a policy, you avoid the scenario of resources being deployed to your subscription that don't have the expected tags for your organization. Instead of manually applying tags or searching for resources that aren't compliant, you create a policy that automatically applies the needed tags during deployment.

Note: Organizing cloud-based resources is a crucial task for IT, unless you only have simple deployments. Use naming and tagging standards to organize your resources for these reasons:

Resource management: Your IT teams will need to quickly locate resources associated with specific workloads, environments, ownership groups, or other important information. Organizing resources is critical to assigning organizational roles and access permissions for resource management.

Reference:

https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/decision-guides/resource-tagging
https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/tag-policies

QUESTION NO: 78 - (HOTSPOT) - (Topic 5)

HOTSPOT

You are designing an access policy for your company.

Occasionally, the developers at the company must stop, start, and restart Azure virtual machines. The development team changes often.

You need to recommend a solution to provide the developers with the required access to the virtual machines. The solution must meet the following requirements:

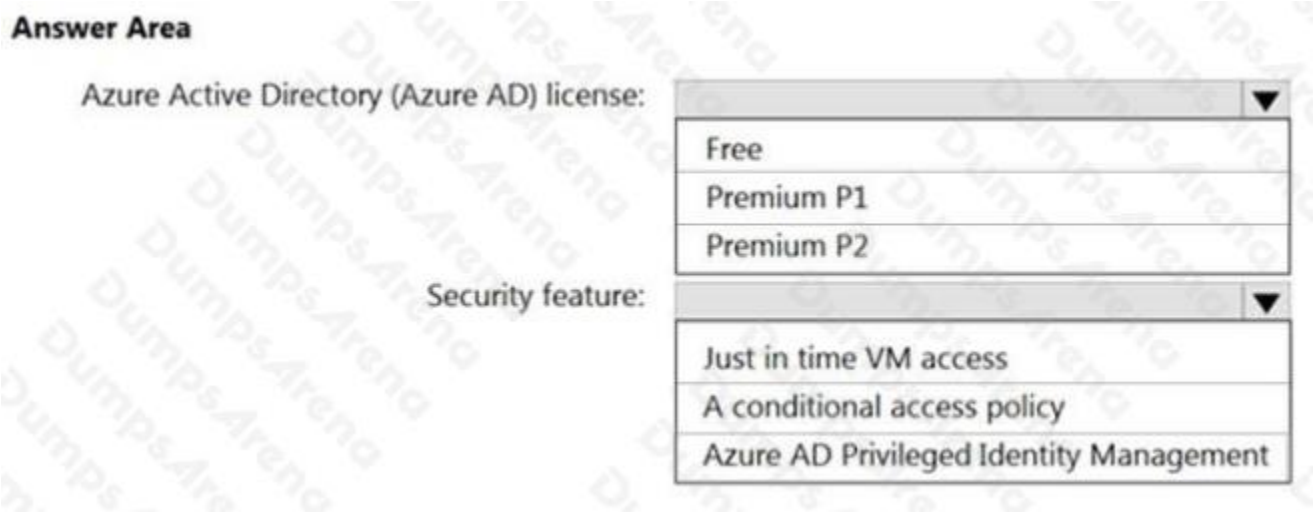
- Provide permissions only when needed.

- Use the principle of least privilege.
- Minimize costs.

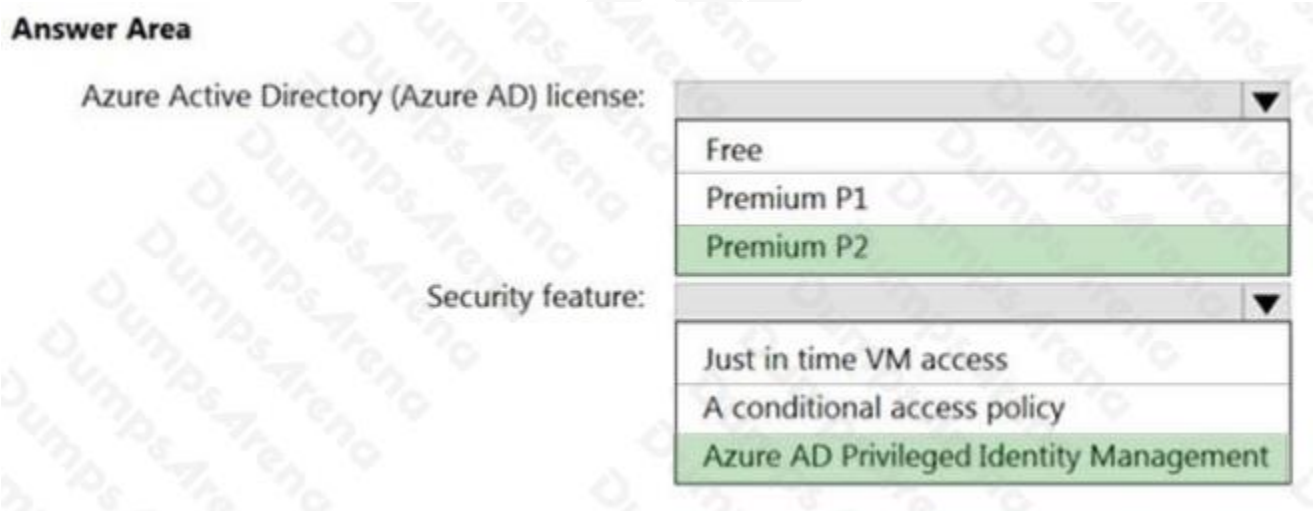
What should you include in the recommendation? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



ANSWER:



Explanation:

QUESTION NO: 79 - (HOTSPOT) - (Topic 5)

HOTSPOT

You have the Free edition of a hybrid Azure Active Directory (Azure AD) tenant. The tenant uses password hash synchronization.

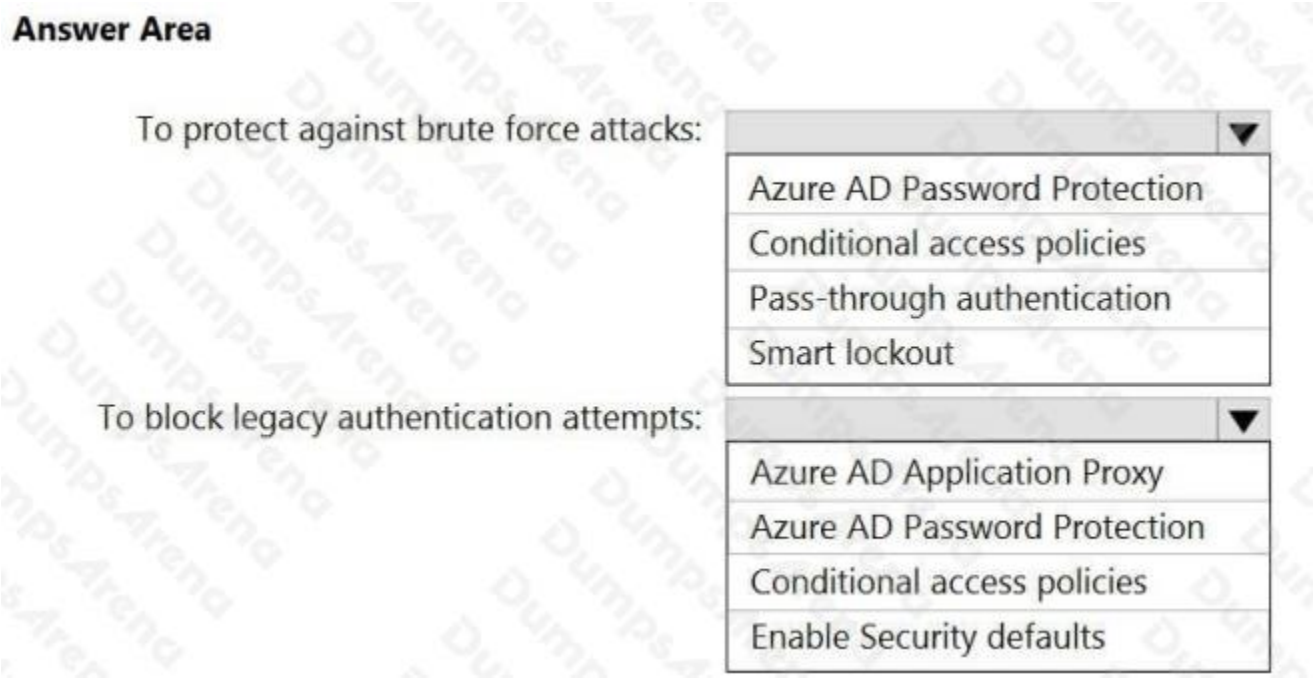
You need to recommend a solution to meet the following requirements:

▪ Prevent Active Directory domain user accounts from being locked out as the result of brute force attacks targeting Azure AD user accounts. ▪ Block legacy authentication attempts to Azure AD integrated apps. ▪ Minimize costs.

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

NOTE: Each correct selection is worth one point.

Hot Area:



ANSWER:

Answer Area

To protect against brute force attacks:

- Azure AD Password Protection
- Conditional access policies
- Pass-through authentication
- Smart lockout

To block legacy authentication attempts:

- Azure AD Application Proxy
- Azure AD Password Protection
- Conditional access policies
- Enable Security defaults

Explanation:

Box 1: Smart lockout

Smart lockout helps lock out bad actors that try to guess your users' passwords or use brute-force methods to get in. Smart lockout can recognize sign-ins that come from valid users and treat them differently than ones of attackers and other unknown sources. Attackers get locked out, while your users continue to access their accounts and be productive.

Box 2: Conditional access policies

If your environment is ready to block legacy authentication to improve your tenant's protection, you can accomplish this goal with Conditional Access.

How can you prevent apps using legacy authentication from accessing your tenant's resources? The recommendation is to just block them with a Conditional Access policy. If necessary, you allow only certain users and specific network locations to use apps that are based on legacy authentication.

Reference: https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-password-smart-lockout
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/block-legacy-authentication

QUESTION NO: 80 - (Topic 5)

You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains several administrative user accounts.

You need to recommend a solution to identify which administrative user accounts have NOT signed in during the previous 30 days.

Which service should you include in the recommendation?

A. Azure AD Privileged Identity Management (PIM)

B. Azure AD Identity Protection

C. Azure Advisor

D. Azure Activity Log

ANSWER: A

QUESTION NO: 81 - (Topic 5)

A company deploys Azure Active Directory (Azure AD) Connect to synchronize identity information from their on-premises Active Directory Domain Services (AD DS) directory to their Azure AD tenant. The identity information that is synchronized includes user accounts, credential hashes for authentication (password sync), and group memberships. The company plans to deploy several Windows and Linux virtual machines (VMs) to support their applications.

The VMs have the following requirements:

- Support domain join, LDAP read, LDAP bind, NTLM and Kerberos authentication, and Group Policy.
- Allow users to sign in to the domain using their corporate credentials and connect remotely to the VM by using Remote Desktop.

You need to support the VM deployment.

Which service should you use?

A. Active Directory Federation Services (AD FS)

B. Azure AD Privileged Identity Management

C. Azure Managed Identity

D. Azure AD Domain Services

ANSWER: D

Explanation:

Azure AD Domain Services provides managed domain services such as domain join, group policy, LDAP, Kerberos/NTLM authentication that are fully compatible with Windows Server Active Directory.

Reference:

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

QUESTION NO: 82 - (HOTSPOT) - (Topic 5)

HOTSPOT

You are designing a software as a service (SaaS) application that will enable Azure Active Directory (Azure AD) users to create and publish online surveys. The SaaS application will have a front-end web app and a back-end web API. The web app will rely on the web API to handle updates to customer surveys.

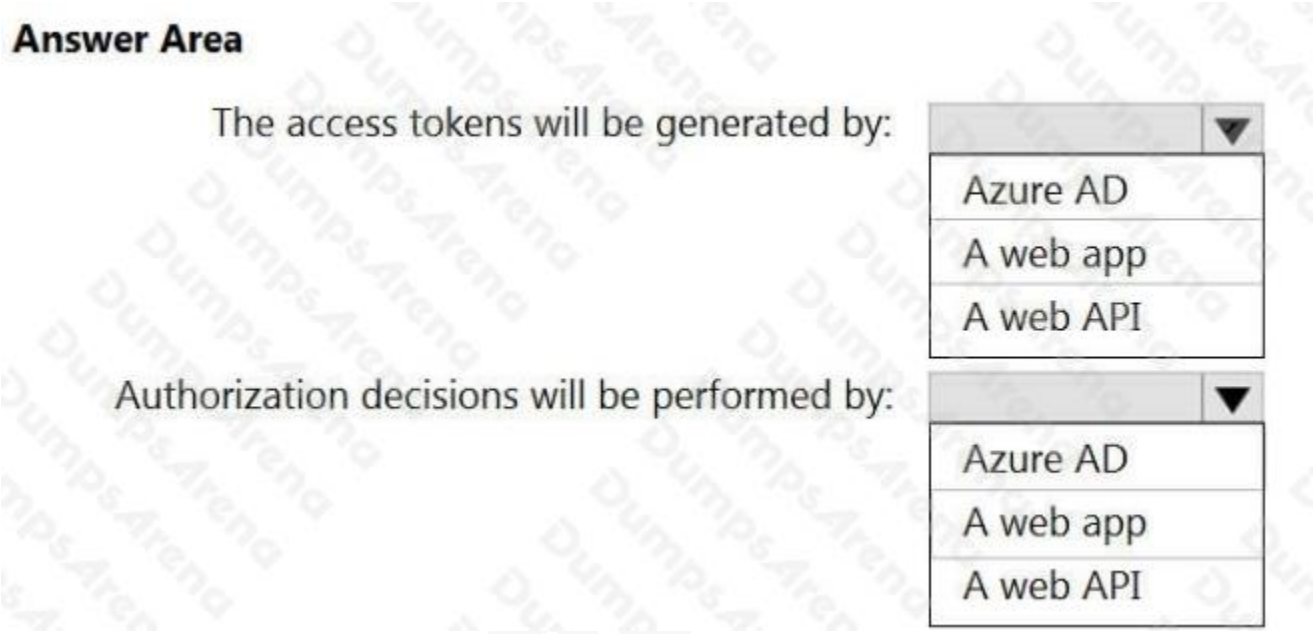
You need to design an authorization flow for the SaaS application. The solution must meet the following requirements:

- To access the back-end web API, the web app must authenticate by using OAuth 2 bearer tokens.
- The web app must authenticate by using the identities of individual users.

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:

Explanation:

Reference: https://docs.microsoft.com/lb-lu/azure/architecture/multitenant-identity/web-api https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-v1-dotnet-webapi

QUESTION NO: 83 - (Topic 5)

You have a hybrid deployment of Azure Active Directory (Azure AD).

You need to recommend a solution to ensure that the Azure AD tenant can be managed only from the computers on your on-premises network.

What should you include in the recommendation?

A. a conditional access policy

B. Azure AD roles and administrators

C. Azure AD Application Proxy

D. Azure AD Privileged Identity Management

ANSWER: A

QUESTION NO: 84 - (Topic 5)

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

ANSWER: D

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 onpremises 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 NO: 85 - (HOTSPOT) - (Topic 5)

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:

DUMPSARENA

Answer Area

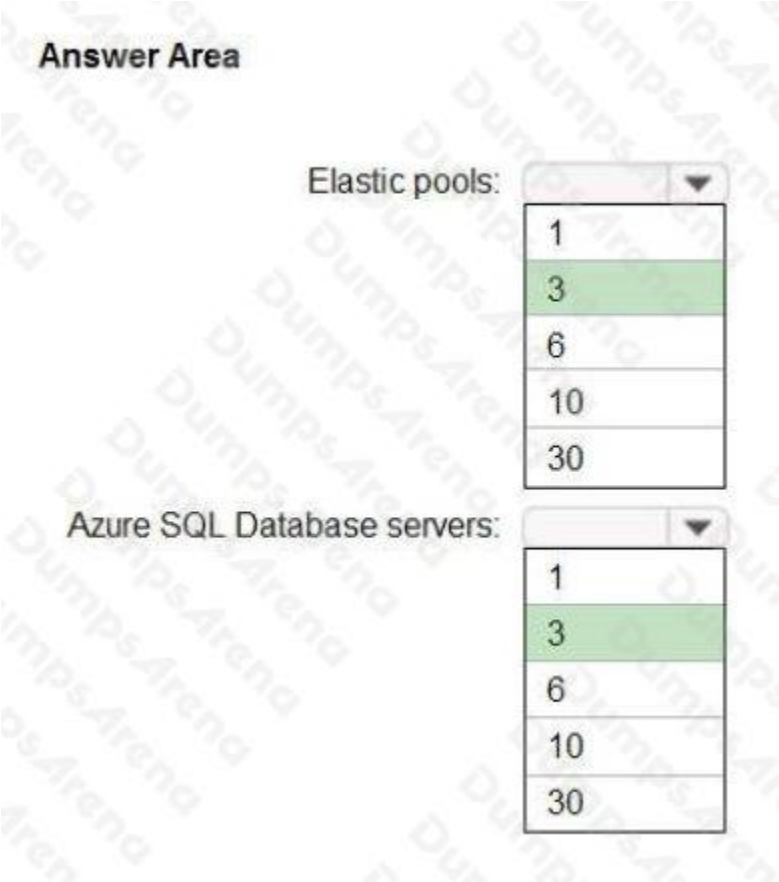
Elastic pools:

- 1
- 3
- 6
- 10
- 30

Azure SQL Database servers:

- 1
- 3
- 6
- 10
- 30

ANSWER:



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.

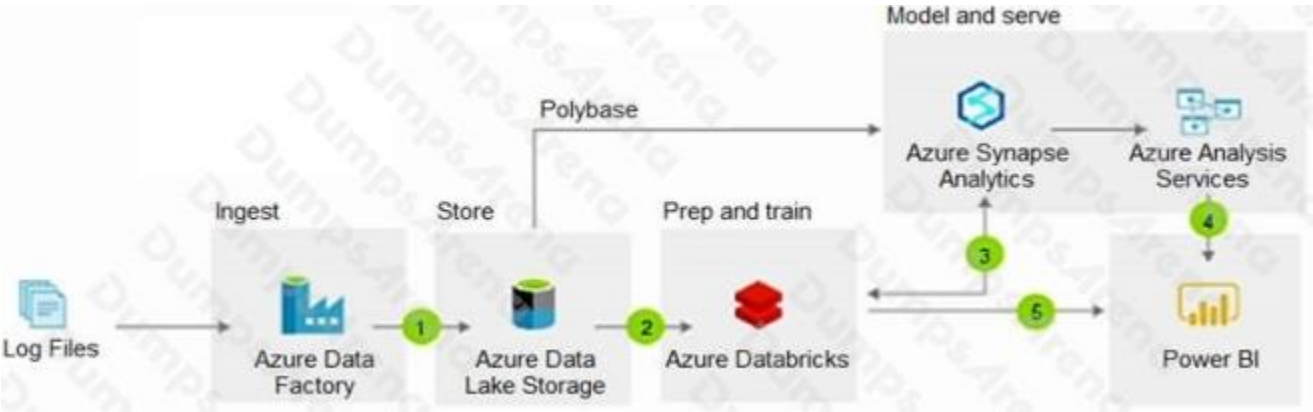
Reference:

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

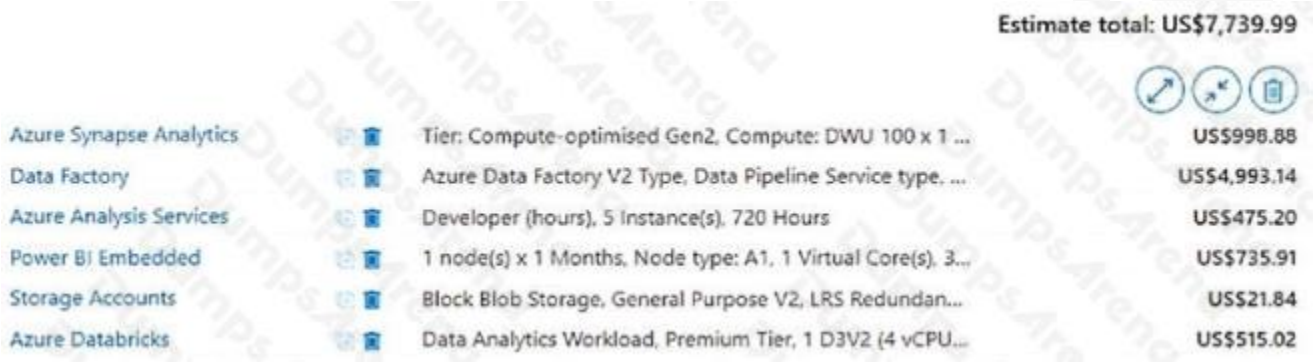
Design Data Storage

QUESTION NO: 86 - (Topic 5)

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.

ANSWER: C

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 NO: 87 - (Topic 5)

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

ANSWER: D

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 NO: 88 - (Topic 5)

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

ANSWER: A

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 NO: 89 - (DRAG DROP) - (Topic 5)

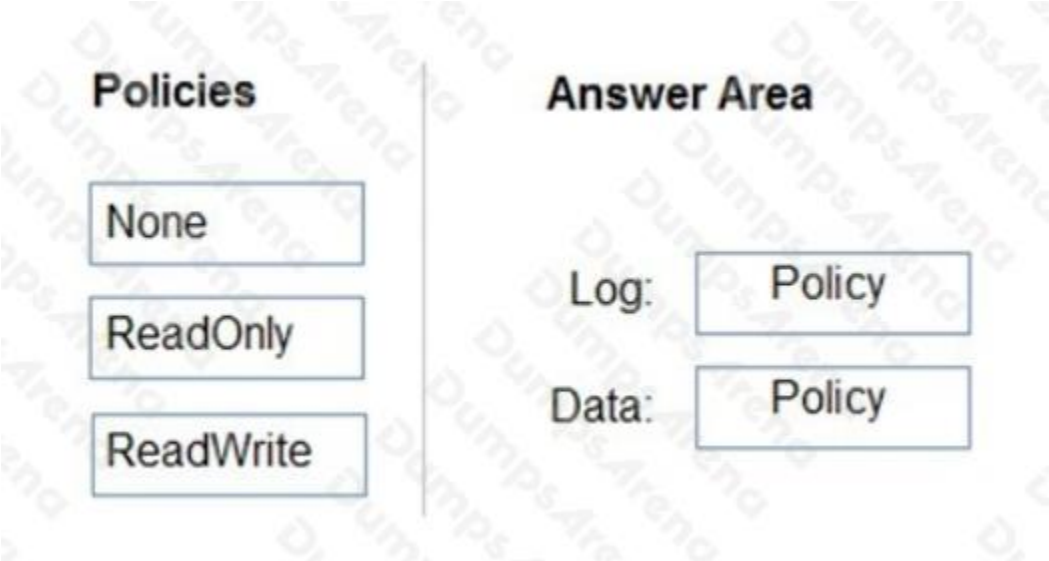
DRAG DROP

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:



ANSWER:

Explanation:

Reference:

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

QUESTION NO: 90 - (Topic 5)

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

ANSWER: D

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 NO: 91 - (Topic 5)

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

ANSWER: C

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

QUESTION NO: 92 - (Topic 5)

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

Name	Type	Location
VNET1	Virtual network	West US
Workspace1	Azure Log Analytics workspace	West US
storage1	Storage account	West US
storage2	Storage account	East US

You need to archive the diagnostic data for VNET1 for 365 days. The solution must minimize costs.

Where should you archive the data?

A. Workspace1

B. storage1

C. storage2

ANSWER: B

Explanation:

Incorrect Answers:

A: When you create a new workspace, it automatically creates several Azure resources that are used by the workspace: ▪ Azure Storage account: Is used as the default datastore for the workspace.

Note: The workspace is the top-level resource for Azure Machine Learning, providing a centralized place to work with all the artifacts you create when you use Azure Machine Learning.

Reference: https://docs.microsoft.com/en-us/azure/machine-learning/concept-workspace

QUESTION NO: 93 - (Topic 5)

You plan to create an Azure Cosmos DB account that uses the SQL API. The account will contain data added by a web application. The web application will send data daily.

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

- Sends email notifications when data is received from the web application
- Minimizes compute cost

What should you include in the recommendation?

A. Deploy an Azure logic app that has a SendGrid connector configured to use an Azure Cosmos DB action.

B. Deploy a function app that is configured to use the Consumption plan and an Azure Event Hubs binding.

C. Deploy a function app that is configured to use the Consumption plan and a SendGrid binding.

D. Deploy an Azure logic app that has a webhook configured to use a SendGrid action.

ANSWER: C

Explanation:

You can send email by using SendGrid bindings in Azure Functions. Azure Functions supports an output binding for SendGrid.

Note: When you're using the Consumption plan, instances of the Azure Functions host are dynamically added and removed based on the number of incoming events.

Reference: https://docs.microsoft.com/en-us/azure/azure-functions/functions-bindings-sendgrid
https://docs.microsoft.com/en-us/azure/azure-functions/functions-scale#consumption-plan

QUESTION NO: 94 - (HOTSPOT) - (Topic 5)

HOTSPOT

You on-premises network contains a file server named Server1 that stores 500 GB of data.

You need to use Azure Data Factory to copy the data from Server1 to Azure Storage.

You add a new data factory.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

From Server1:

- Install an Azure File Sync agent.
- Install a self-hosted integration runtime.
- Install the File Server Resource Manager role service.

From the data factory:

- Create a pipeline.
- Create an import/export job.
- Provision an Azure-SQL Server Integration Services (SSIS) integration runtime.

ANSWER:

Answer Area

From Server1:

- Install an Azure File Sync agent.
- Install a self-hosted integration runtime.
- Install the File Server Resource Manager role service.

From the data factory:

- Create a pipeline.
- Create an import/export job.
- Provision an Azure-SQL Server Integration Services (SSIS) integration runtime.

Explanation:

Box 1: Install a self-hosted integration runtime

The Integration Runtime is a customer-managed data integration infrastructure used by Azure Data Factory to provide data integration capabilities across different network environments.

Box 2: Create a pipeline

With ADF, existing data processing services can be composed into data pipelines that are highly available and managed in the cloud. These data pipelines can be scheduled to ingest, prepare, transform, analyze, and publish data, and ADF manages and orchestrates the complex data and processing dependencies

Reference:

https://docs.microsoft.com/en-us/azure/machine-learning/team-data-science-process/move-sql-azure-adf

QUESTION NO: 95 - (HOTSPOT) - (Topic 5)

HOTSPOT

You have an on-premises file server that stores 2 TB of data files.

You plan to move the data files to Azure Blob storage in the Central Europe region.

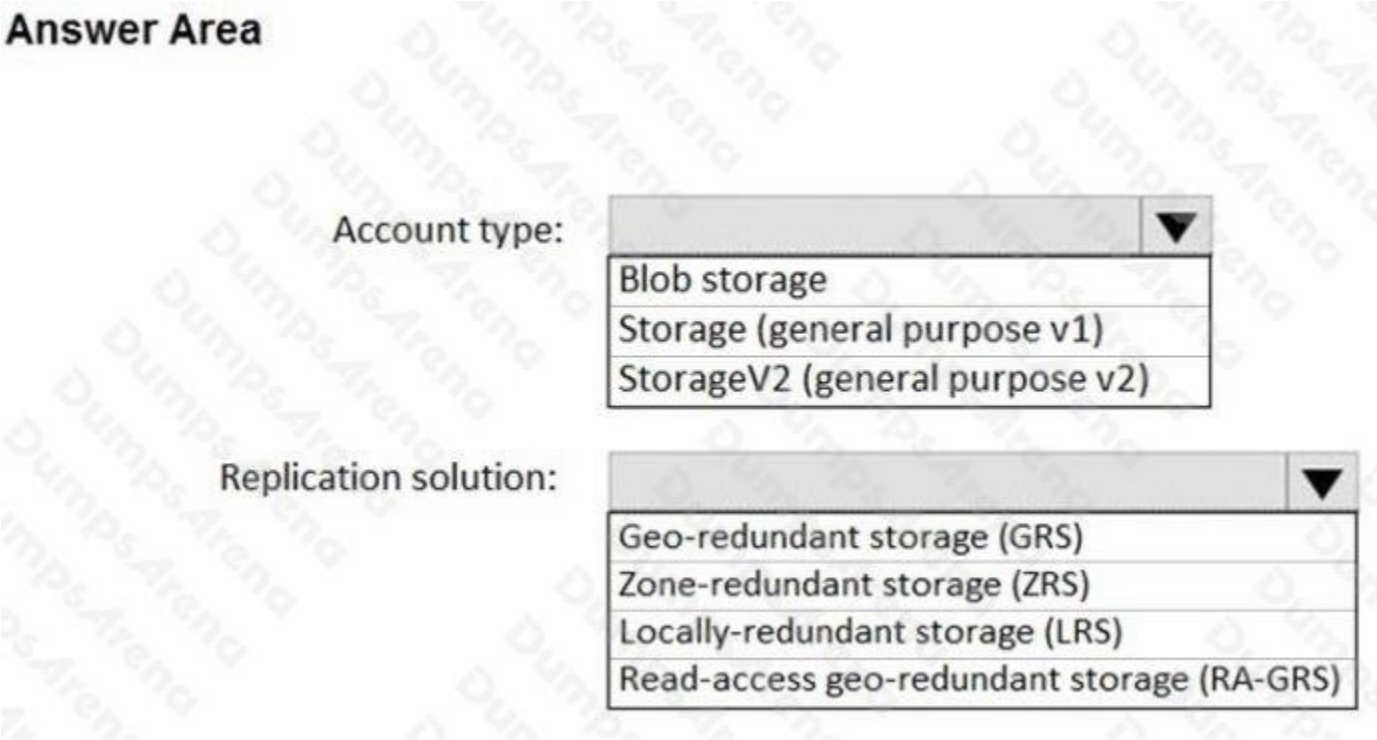
You need to recommend a storage account type to store the data files and a replication solution for the storage account. The solution must meet the following requirements:

- Be available if a single Azure datacenter fails.
- Support storage tiers. ▪ Minimize cost.

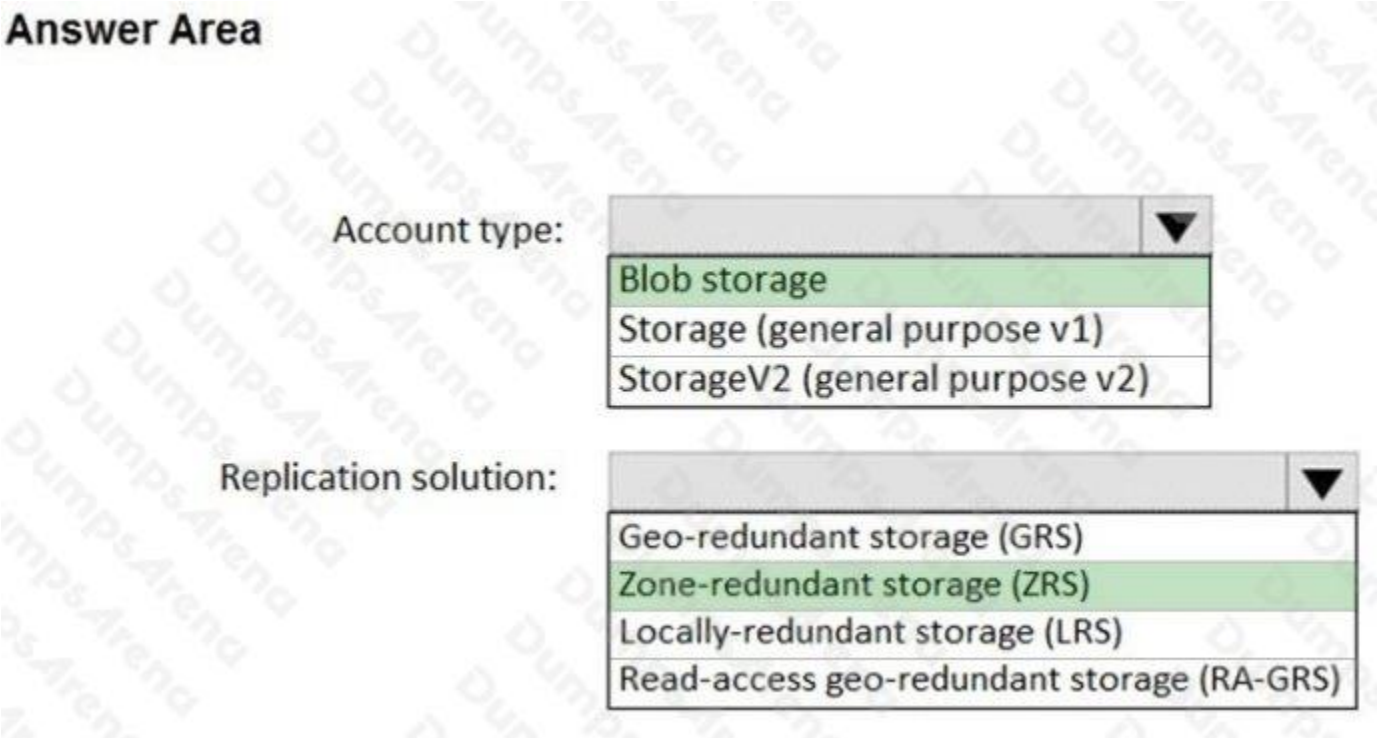
What should you recommend? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



ANSWER:



Explanation:

Box 1: Blob storage

Blob storage supports storage tiers

Note: Azure offers three storage tiers to store data in blob storage: Hot Access tier, Cool Access tier, and Archive tier. These tiers target data at different stages of its lifecycle and offer costeffective storage options for different use cases.

Box 2: Zone-redundant storage (ZRS)

Data in an Azure Storage account is always replicated three times in the primary region. Azure Storage offers two options for how your data is replicated in the primary region:

- Zone-redundant storage (ZRS) copies your data synchronously across three Azure availability zones in the primary region.
- Locally redundant storage (LRS) copies your data synchronously three times within a single physical location in the primary region. LRS is the least expensive replication option, but is not recommended for applications requiring high availability.

Reference:

https://cloud.netapp.com/blog/storage-tiers-in-azure-blob-storage-find-the-best-for-your-data https://docs.microsoft.com/en-us/azure/storage/common/storage-redundancy

QUESTION NO: 96 - (Topic 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 are designing an Azure solution for a company that has four departments. Each department will deploy several Azure app services and Azure SQL databases.

You need to recommend a solution to report the costs for each department to deploy the app services and the databases. The solution must provide a consolidated view for cost reporting that displays cost broken down by department.

Solution: Create a resource group for each resource type. Assign tags to each resource group.

Does this meet the goal?

A. Yes

B. No

ANSWER: A

Explanation:

Tags enable you to retrieve related resources from different resource groups. This approach is helpful when you need to organize resources for billing or management.

Reference:

https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-using-tags

QUESTION NO: 97 - (Topic 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 are designing an Azure solution for a company that has four departments. Each department will deploy several Azure app services and Azure SQL databases.

You need to recommend a solution to report the costs for each department to deploy the app services and the databases. The solution must provide a consolidated view for cost reporting that displays cost broken down by department.

Solution: Create a new subscription for each department.

Does this meet the goal?

A. Yes

B. No

ANSWER: B

Explanation:

Instead, create a resources group for each resource type. Assign tags to each resource

Note: Tags enable you to retrieve related resources from different resource groups. This approach is helpful when you need to organize resources for billing or management.

Reference:

https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-using-tags

QUESTION NO: 98 - (Topic 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 are designing an Azure solution for a company that has four departments. Each department will deploy several Azure app services and Azure SQL databases.

You need to recommend a solution to report the costs for each department to deploy the app services and the databases. The solution must provide a consolidated view for cost reporting that displays cost broken down by department.

Solution: Place all resources in the same resource group. Assign tags to each resource.

Does the solution meet the goal?

A. Yes

B. No

ANSWER: B

Explanation:

Instead, create a resources group for each resource type. Assign tags to each resource

Note: Tags enable you to retrieve related resources from different resource groups. This approach is helpful when you need to organize resources for billing or management.

Reference:

https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-using-tags

QUESTION NO: 99 - (HOTSPOT) - (Topic 5)

HOTSPOT

You have an Azure SQL database named DB1.

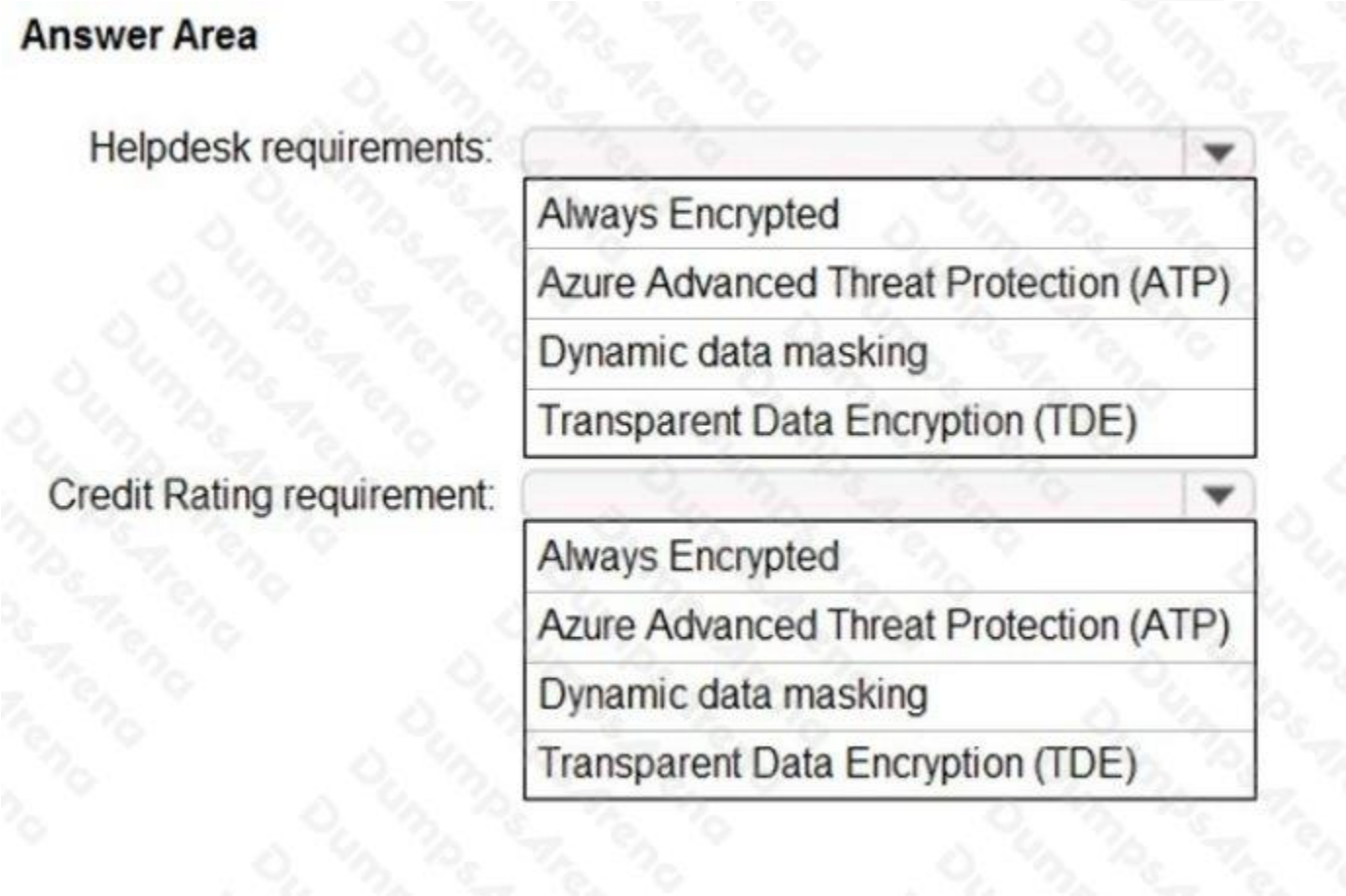
You need to recommend a data security solution for DB1. The solution must meet the following requirements:

- When helpdesk supervisors query DB1, they must see the full number of each credit card.
- When helpdesk operators query DB1, they must see only the last four digits of each credit card number.
- A column named Credit Rating must never appear in plain text within the database system, and only client applications must be able to decrypt the Credit Rating column.

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:

Answer Area

Helpdesk requirements:

- Always Encrypted
- Azure Advanced Threat Protection (ATP)
- Dynamic data masking
- Transparent Data Encryption (TDE)

Credit Rating requirement:

- Always Encrypted
- Azure Advanced Threat Protection (ATP)
- Dynamic data masking
- Transparent Data Encryption (TDE)

Explanation:

Box 1: Dynamic data masking

Dynamic data masking helps prevent unauthorized access to sensitive data by enabling customers to designate how much of the sensitive data to reveal with minimal impact on the application layer. It's a policy-based security feature that hides the sensitive data in the result set of a query over designated database fields, while the data in the database is not changed.

Box 2: Always encrypted

Data stored in the database is protected even if the entire machine is compromised, for example by malware. Always Encrypted leverages client-side encryption: a database driver inside an application transparently encrypts data, before sending the data to the database. Similarly, the driver decrypts encrypted data retrieved in query results.

Reference:

https://azure.microsoft.com/en-us/blog/transparent-data-encryption-or-always-encrypted/

QUESTION NO: 100 - (Topic 5)

You are designing a data protection strategy for Azure virtual machines. All the virtual machines use managed disks.

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

- The use of encryption keys is audited.

- All the data is encrypted at rest always.
- You manage the encryption keys, not Microsoft.

What should you include in the recommendation?

A. client-side encryption

B. Azure Storage Service Encryption

C. Azure Disk Encryption

D. Encrypting File System (EFS)

ANSWER: C

Explanation:

Reference:

https://docs.microsoft.com/en-us/azure/security/azure-security-disk-encryption-overview

QUESTION NO: 101 - (Topic 5)

You have an on-premises application named App1 that uses an Oracle database.

You plan to use Azure Databricks to transform and load data from App1 to an Azure Synapse Analytics instance.

You need to ensure that the App1 data is available to Databricks.

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

NOTE: Each correct selection is worth one point.

A. Azure Data Box Gateway

B. Azure Data Lake Storage

C. Azure Import/Export service

D. Azure Data Factory

E. Azure Data Box Edge

ANSWER: B D

Explanation:

Automate data movement using Azure Data Factory, then load data into Azure Data Lake Storage, transform and clean it using Azure Databricks, and make it available for analytics using Azure Synapse

Analytics. Modernize your data warehouse in the cloud for unmatched levels of

Note: Integrate data silos with Azure Data Factory, a service built for all data integration needs and skill levels. Easily construct ETL and ELT processes code-free within the intuitive visual environment, or write your own code. Visually integrate data sources using more than 90+ natively built and maintenance-free connectors at no added cost. Focus on your data—the serverless integration service does the rest.

Reference:

https://azure.microsoft.com/en-us/services/databricks/#capabilities https://azure.microsoft.com/en-us/services/data-factory/

QUESTION NO: 102 - (Topic 5)

You have 100 devices that write performance data to Azure Blob storage.

You plan to store and analyze the performance data in an Azure SQL database.

You need to recommend a solution to move the performance data to the SQL database.

What should you include in the recommendation?

A. Azure Database Migration Service

B. Azure Data Factory

C. Azure Data Box

D. Data Migration Assistant

ANSWER: B

Explanation:

You can copy data from Azure Blob to Azure SQL Database using Azure Data Factory.

Reference:

https://docs.microsoft.com/en-us/azure/data-factory/tutorial-copy-data-dot-net

QUESTION NO: 103 - (HOTSPOT) - (Topic 5)

HOTSPOT

You have a web application that uses a MongoDB database. You plan to migrate the web application to Azure.

You must migrate to Cosmos DB while minimizing code and configuration changes.

You need to design the Cosmos DB configuration.

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

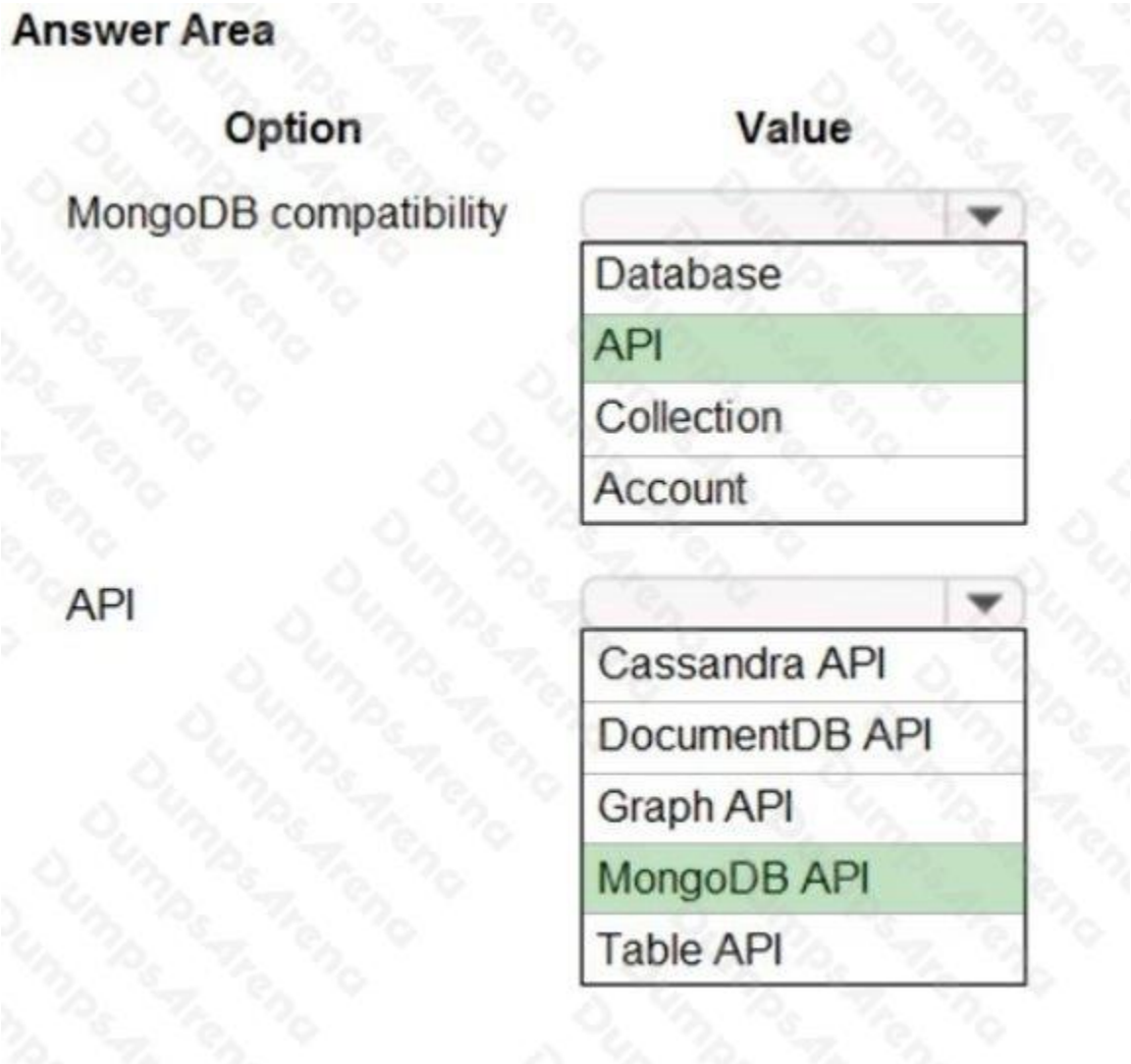
NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Option	Value
MongoDB compatibility	Database API Collection Account
API	Cassandra API DocumentDB API Graph API MongoDB API Table API

ANSWER:



Explanation:

MongoDB compatibility: API

API: MongoDB API

Azure Cosmos DB comes with multiple APIs:

- SQL API, a JSON document database service that supports SQL queries. This is compatible with the former Azure DocumentDB.
- MongoDB API, compatible with existing Mongo DB libraries, drivers, tools and applications.
- Cassandra API, compatible with existing Apache Cassandra libraries, drivers, tools, and applications.
- Azure Table API, a key-value database service compatible with existing Azure Table Storage.
- Gremlin (graph) API, a graph database service supporting Apache Tinkerpop's graph traversal language, Gremlin.

Reference: https://docs.microsoft.com/en-us/azure/cosmos-db/create-mongodb-dotnet

QUESTION NO: 104 - (Topic 5)

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

ANSWER: B

Explanation:

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

QUESTION NO: 105 - (Topic 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 Azure Storage account that contains two 1-GB data files named File1 and File2. The data files are set to use the archive access tier.

You need to ensure that File1 is accessible immediately when a retrieval request is initiated.

Solution: For File1, you set Access tier to Hot.

Does this meet the goal?

A. Yes

B. No

ANSWER: A

Explanation:

The hot access tier has higher storage costs than cool and archive tiers, but the lowest access costs. Example usage scenarios for the hot access tier include:

- Data that's in active use or expected to be accessed (read from and written to) frequently. - Data that's staged for processing and eventual migration to the cool access tier.

Reference:

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

QUESTION NO: 106 - (Topic 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 Azure Storage account that contains two 1-GB data files named File1 and File2. The data files are set to use the archive access tier.

You need to ensure that File1 is accessible immediately when a retrieval request is initiated.

Solution: You add a new file share to the storage account.

Does this meet the goal?

A. Yes

B. No

ANSWER: B

QUESTION NO: 107 - (Topic 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 Azure Storage account that contains two 1-GB data files named File1 and File2. The data files are set to use the archive access tier.

You need to ensure that File1 is accessible immediately when a retrieval request is initiated.

Solution: You move File1 to a new storage account. For File1, you set Access tier to Archive.

Does this meet the goal?

A. Yes

B. No

ANSWER: B

Explanation:

Instead use the hot access tier.

The hot access tier has higher storage costs than cool and archive tiers, but the lowest access costs. Example usage scenarios for the hot access tier include:

▪ Data that's in active use or expected to be accessed (read from and written to) frequently. ▪ Data that's staged for processing and eventual migration to the cool access tier.

Reference:

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

QUESTION NO: 108 - (Topic 5)

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

ANSWER: A

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 NO: 109 - (HOTSPOT) - (Topic 5)

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

ANSWER:

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

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 NO: 110 - (Topic 5)

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

ANSWER: C

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 NO: 111 - (Topic 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 are designing an Azure solution for a company that has four departments. Each department will deploy several Azure app services and Azure SQL databases.

You need to recommend a solution to report the costs for each department to deploy the app services and the databases. The solution must provide a consolidated view for cost reporting that displays cost broken down by department.

Solution: Create a separate resource group for each department. Place the resources for each department in its respective resource group.

Does this meet the goal?

A. Yes

B. No

ANSWER: B

Explanation:

Instead create a resources group for each resource type. Assign tags to each resource group.

Note: Tags enable you to retrieve related resources from different resource groups. This approach is helpful when you need to organize resources for billing or management.

Reference:

https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-using-tags

QUESTION NO: 112 - (Topic 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

ANSWER: B

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 NO: 113 - (Topic 5)

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

ANSWER: C

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 NO: 114 - (HOTSPOT) - (Topic 5)

HOTSPOT

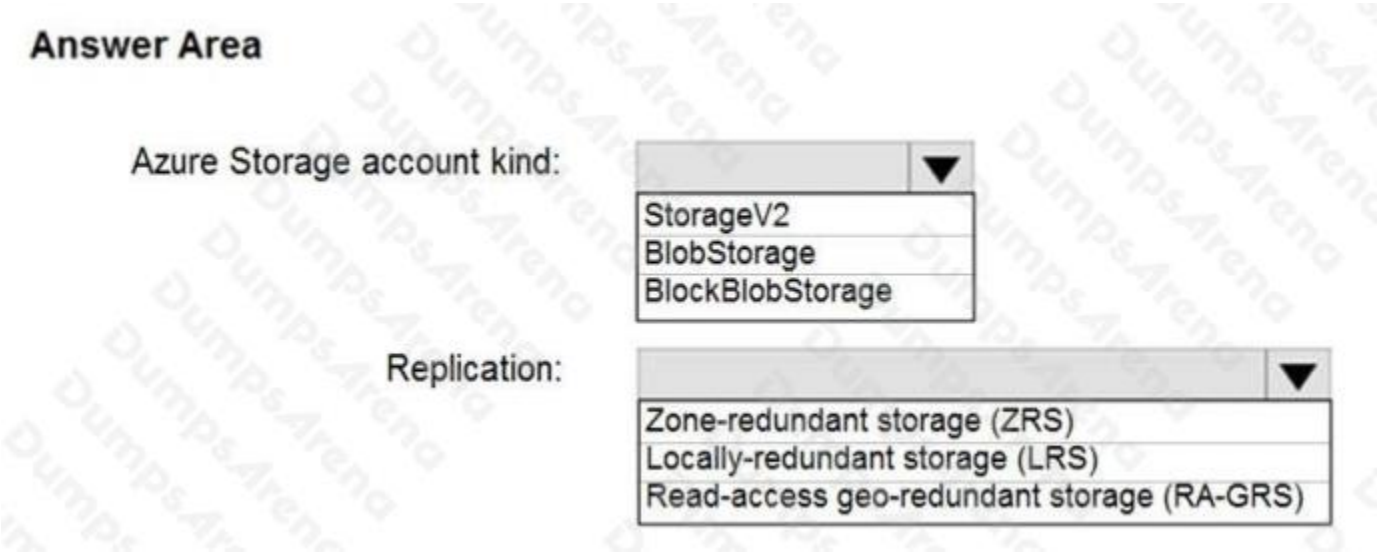
You plan to develop a new app that will store business critical data. The app must meet the following requirements:

- Prevent new data from being modified for one year.
- Minimize read latency.
- Maximize data resiliency.

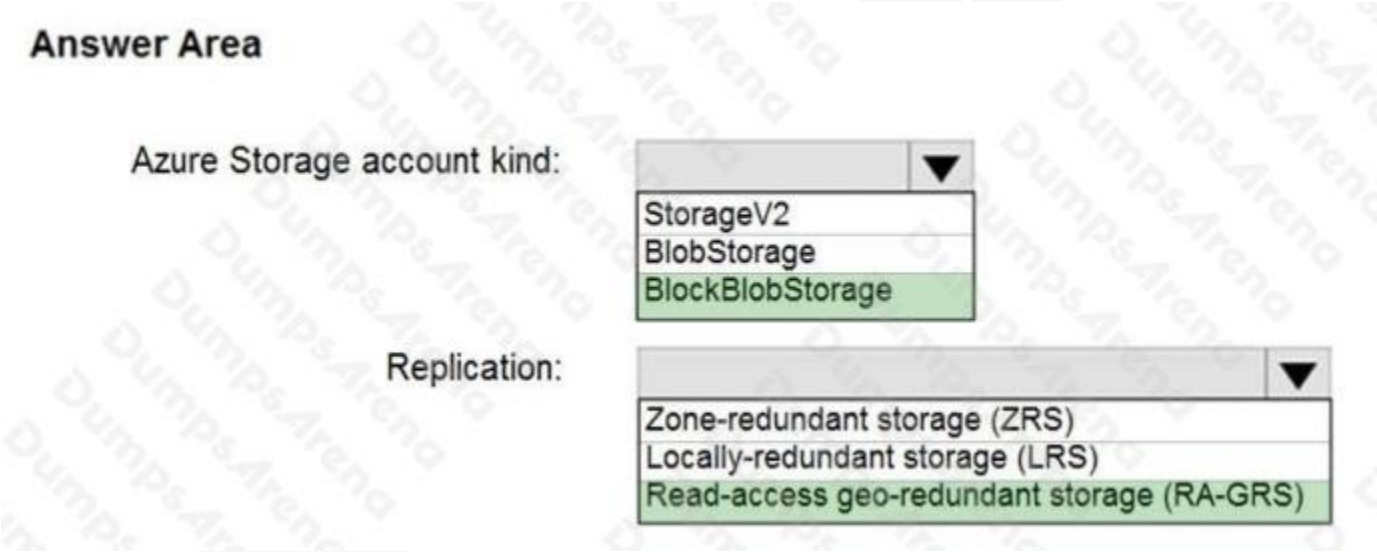
You need to recommend a storage solution for the app.

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

Hot Area:



ANSWER:



Explanation:

Box 1:

BlockBlobStorage

Storage accounts with premium performance characteristics for block blobs and append blobs.

Box 2:

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

https://docs.microsoft.com/en-us/azure/storage/common/storage-redundancy?toc=/azure/storage/ blobs/toc.json

QUESTION NO: 115 - (Topic 5)

You have an application named App1. App1 generates log files that must be archived for five years. The log files must be readable by App1 but must not be modified.

Which storage solution should you recommend for archiving?

A. Ingest the log files into an Azure Log Analytics workspace

B. Use an Azure Blob storage account and a time-based retention policy

C. Use an Azure Blob storage account configured to use the Archive access tier

D. Use an Azure file share that has access control enabled

ANSWER: B

Explanation:

Immutable storage for Azure Blob storage enables users to store business-critical data objects in a WORM (Write Once, Read Many) state.

Immutable storage supports:

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.

Reference:

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

QUESTION NO: 116 - (Topic 5)

You have 100 Microsoft SQL Server Integration Services (SSIS) packages that are configured to use 10 on-premises SQL Server databases as their destinations.

You plan to migrate the 10 on-premises databases to Azure SQL Database.

You need to recommend a solution to host the SSIS packages in Azure. The solution must ensure that the packages can target the SQL Database instances as their destinations.

What should you include in the recommendation?

A. SQL Server Migration Assistant (SSMA)

B. Data Migration Assistant

C. Azure Data Catalog

D. Azure Data Factory

ANSWER: B

QUESTION NO: 117 - (HOTSPOT) - (Topic 5)

HOTSPOT

You are planning an Azure Storage solution for sensitive data. The data will be accessed daily. The data set is less than 10 GB.

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

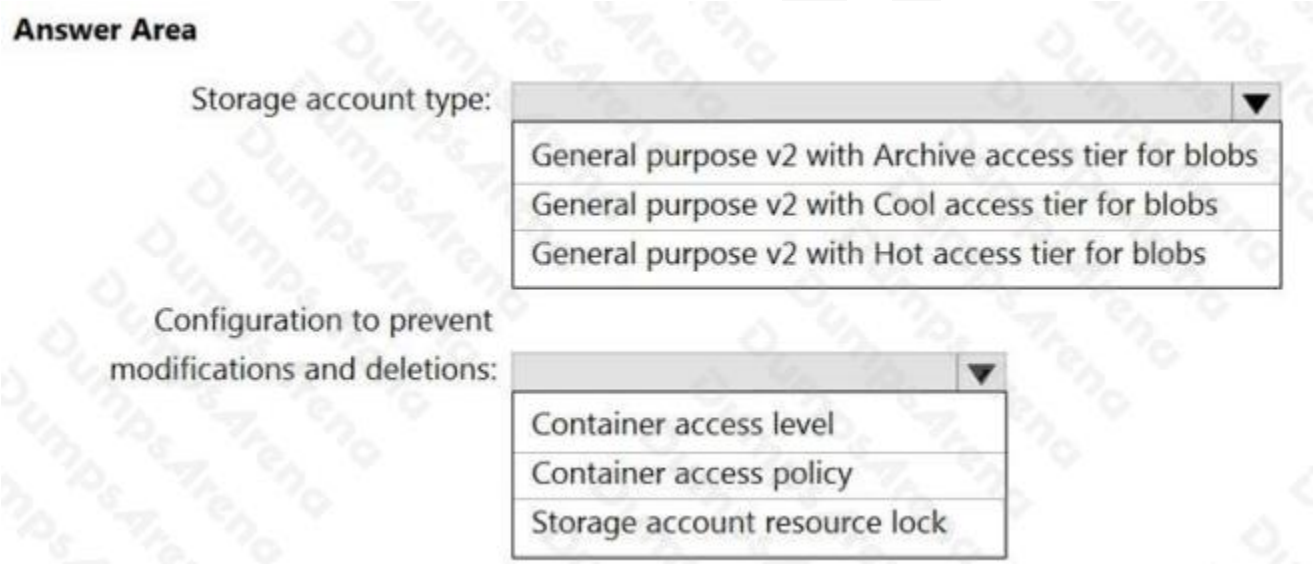
- All the data written to storage must be retained for five years.

- Once the data is written, the data can only be read. Modifications and deletion must be prevented. - After five years, the data can be deleted, but never modified. - Data access charges must be minimized.

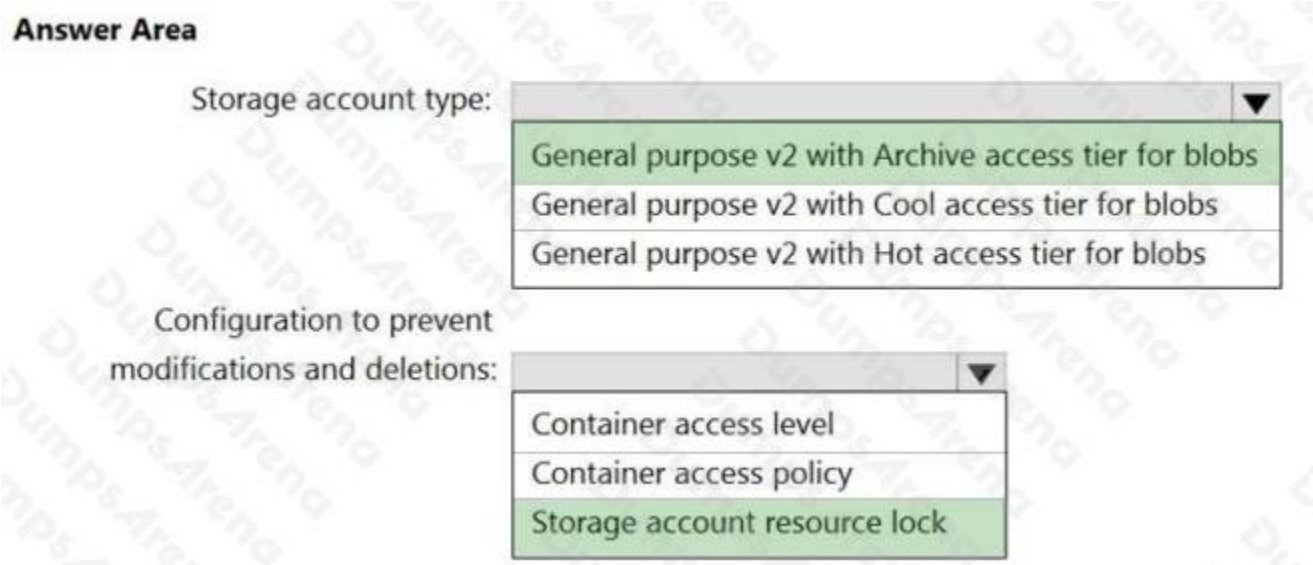
What should you recommend? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



ANSWER:



Explanation:

Box 1: General purpose v2 with Archive acce3ss tier for blobs

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. Cool - Optimized for storing data that is infrequently accessed and stored for at least 30 days. Hot - Optimized for storing data that is accessed frequently.

Box 2: Storage account resource lock

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

Note: You can set the lock level to CanNotDelete or ReadOnly. In the portal, the locks are called Delete and Read-only respectively.

- CanNotDelete means authorized users can still read and modify a resource, but they can't delete the resource.
- ReadOnly means authorized users can read a resource, but they can't delete or update the resource. Applying this lock is similar to restricting all authorized users to the permissions granted by the Reader role.

Reference:

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

QUESTION NO: 118 - (Topic 5)

You have an Azure subscription. The subscription contains an app that is hosted in the East US, Central Europe, and East Asia regions.

You need to recommend a data-tier solution for the app. The solution must meet the following requirements:

- Support multiple consistency levels.
- Be able to store at least 1 TB of data.
- Be able to perform read and write operations in the Azure region that is local to the app instance.

What should you include in the recommendation?

A. an Azure Cosmos DB database

B. a Microsoft SQL Server Always On availability group on Azure virtual machines

C. an Azure SQL database in an elastic pool

D. Azure Table storage that uses geo-redundant storage (GRS) replication

ANSWER: A

Explanation:

Azure Cosmos DB approaches data consistency as a spectrum of choices. This approach includes more options than the two extremes of strong and eventual consistency. You can choose from five welldefined levels on the consistency spectrum.

With Cosmos DB any write into any region must be replicated and committed to all configured regions within the account.

Incorrect Answers:

D: Not able to do local writes.

Reference: https://docs.microsoft.com/en-us/azure/cosmos-db/consistency-levels-tradeoffs

QUESTION NO: 119 - (Topic 5)

You need to recommend a data storage strategy for WebApp1.

What should you include in the recommendation?

A. a vCore-based Azure SQL database

B. an Azure virtual machine that runs SQL Server

C. an Azure SQL Database elastic pool

D. a fixed-size DTU Azure SQL database

ANSWER: A

QUESTION NO: 120 - (DRAG DROP) - (Topic 5)

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.

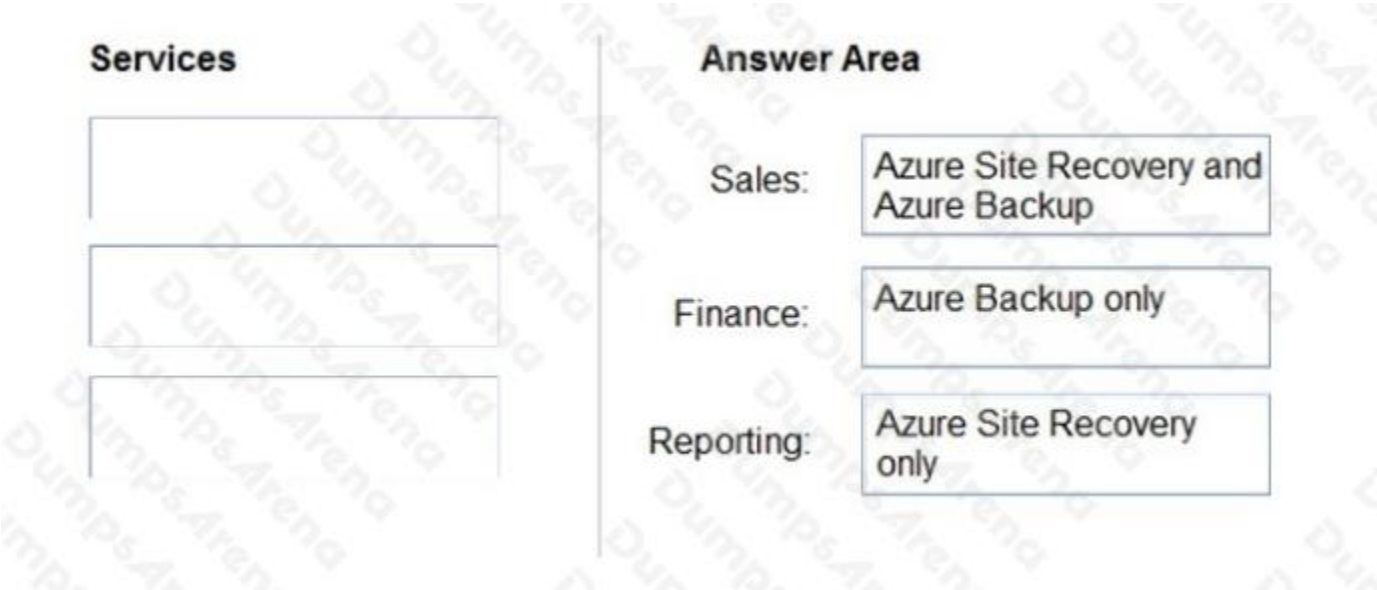
You need to recommend which Azure services meet the business continuity and disaster recovery objectives. The solution must minimize costs.

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:

ANSWER:



Explanation:

QUESTION NO: 121 - (Topic 5)

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.

ANSWER: D

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:

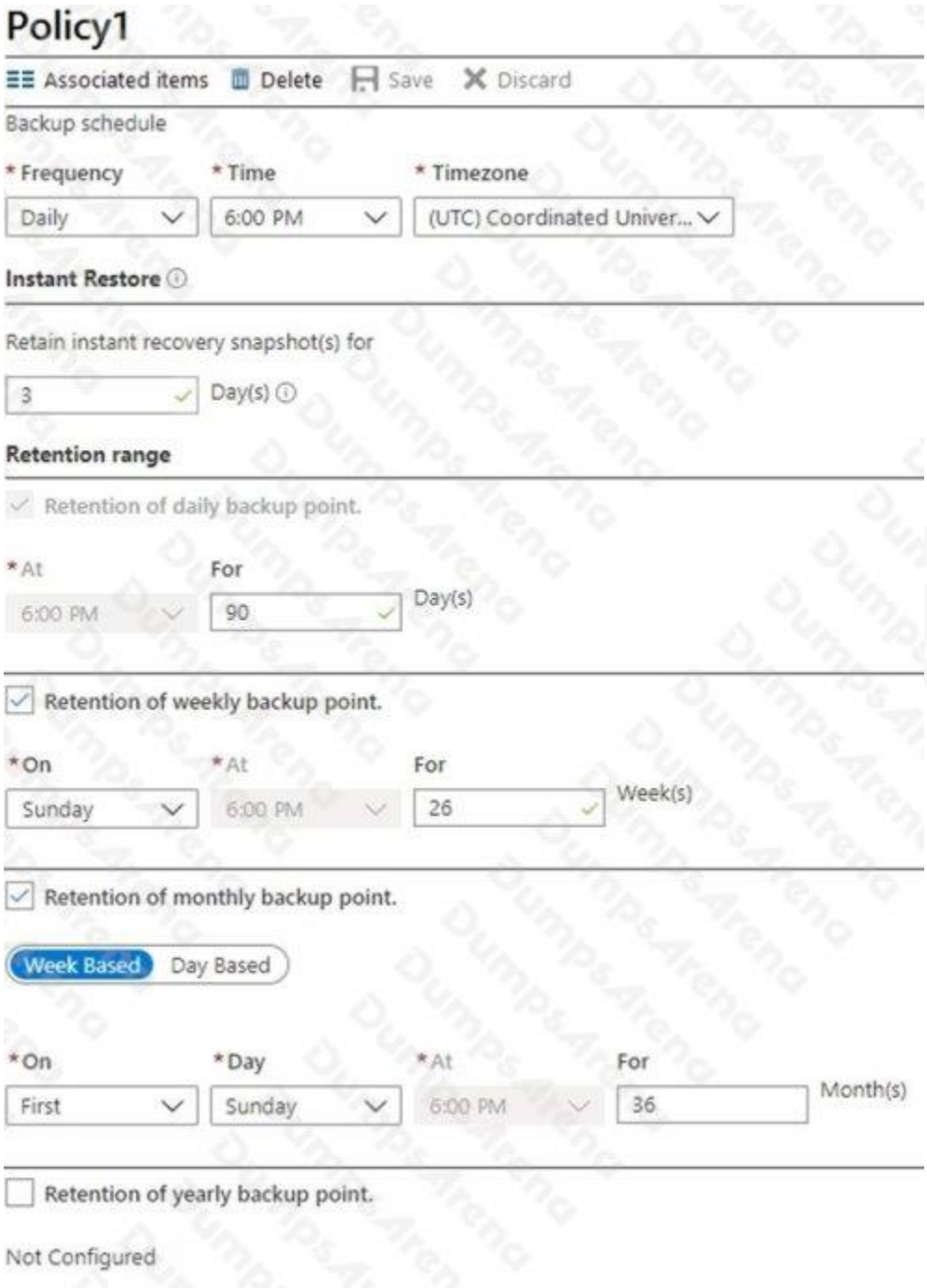
https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blob-immutable-storage

QUESTION NO: 122 - (HOTSPOT) - (Topic 5)

HOTSPOT

You plan to deploy the backup policy shown in the following exhibit.

DUMPSARENA



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

Virtual machines that are backed up by using the policy can be recovered for up to a maximum of **[answer choice]**.

- 90 days
- 26 weeks
- 36 months
- 45 months

The minimum recovery point objective (RPO) for virtual machines that are backed up by using the policy is **[answer choice]**.

- 1 hour
- 1 day
- 1 week
- 1 month
- 1 year

ANSWER:

Answer Area

Virtual machines that are backed up by using the policy can be recovered for up to a maximum of **[answer choice]**.

- 90 days
- 26 weeks
- 36 months
- 45 months

The minimum recovery point objective (RPO) for virtual machines that are backed up by using the policy is **[answer choice]**.

- 1 hour
- 1 day
- 1 week
- 1 month
- 1 year

Explanation:

QUESTION NO: 123 - (HOTSPOT) - (Topic 5)

HOTSPOT

You have an Azure web app named App1 and an Azure key vault named KV1.

App1 stores database connection strings in KV1.

App1 performs the following types of requests to KV1:

- Get
- List
- Wrap
- Delete
- Unwrap

- Backup
- Decrypt
- Encrypt

You are evaluating the continuity of service for App1.

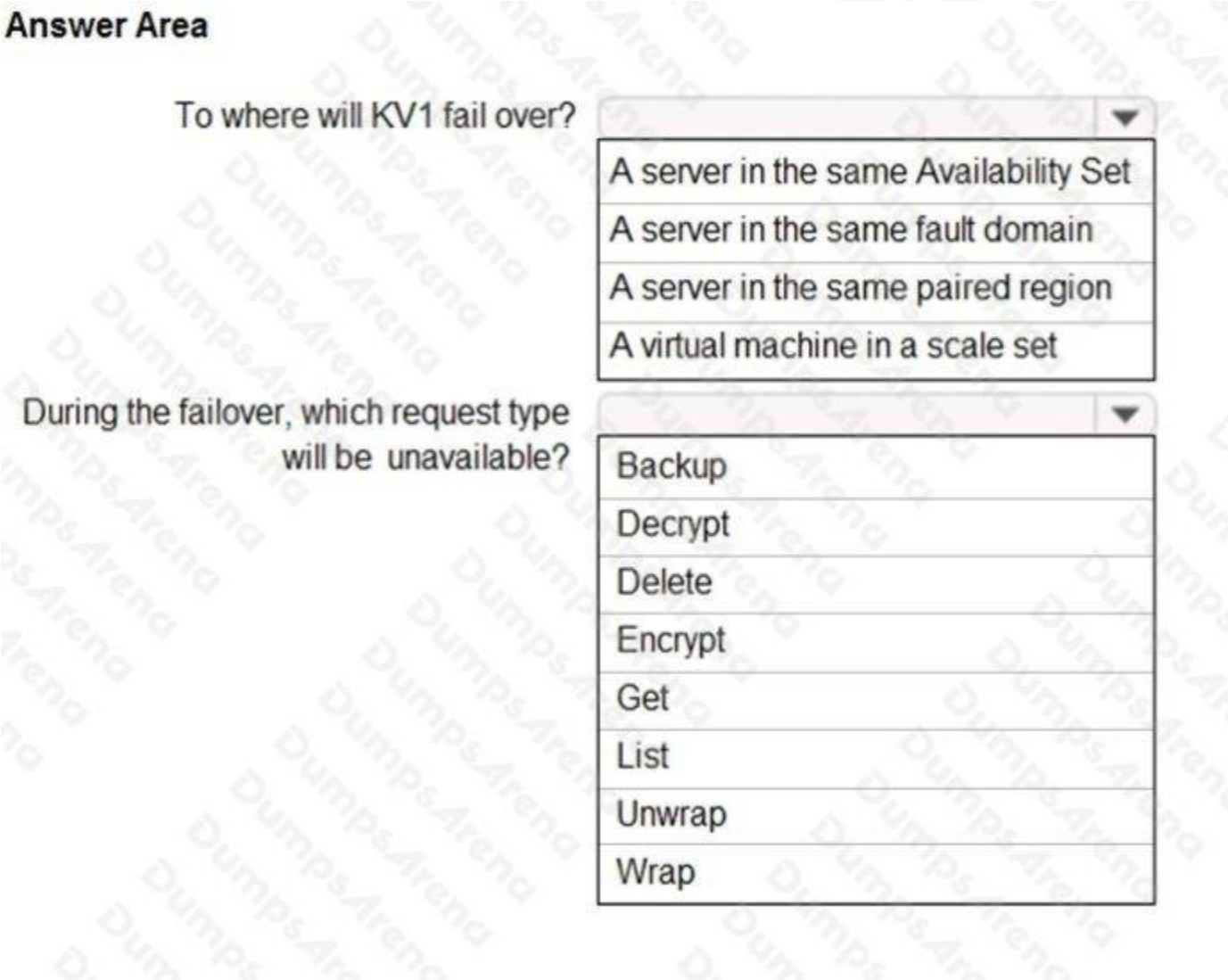
You need to identify the following if the Azure region that hosts KV1 becomes unavailable:

- To where will KV1 fail over?
- During the failover, which request type will be unavailable?

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

NOTE: Each correct selection is worth one point.

Hot Area:



ANSWER:

Answer Area

To where will KV1 fail over?

- A server in the same Availability Set
- A server in the same fault domain
- A server in the same paired region
- A virtual machine in a scale set

During the failover, which request type will be unavailable?

- Backup
- Decrypt
- Delete
- Encrypt
- Get
- List
- Unwrap
- Wrap

Explanation:

Box 1: A server in the same paired region

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 to maintain high durability of your keys and secrets.

Box 2: Delete

During failover, your key vault is in read-only mode. Requests that are supported in this mode are: ▪ List certificates

▪ Get certificates ▪ List secrets

▪ Get secrets

▪ List keys

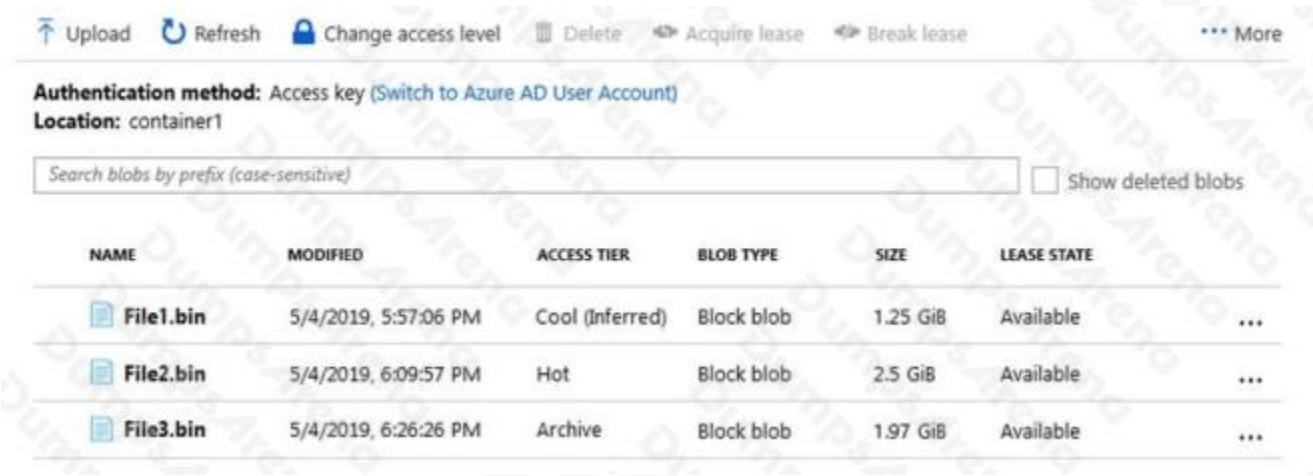
▪ Get (properties of) keys

- Encrypt
- Decrypt ▪ Wrap ▪ Unwrap
- Verify
- Sign
- Backup

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

QUESTION NO: 124 - (Topic 5)

You have an Azure Storage account that contains the data shown in the following exhibit.



You need to identify which files can be accessed immediately from the storage account.

Which files should you identify?

A. File1.bin only

B. File2.bin only

C. File3.bin only

D. File1.bin and File2.bin only

E. File1.bin, File2.bin, and File3.bin

ANSWER: D

Explanation:

Hot - Optimized for storing data that is accessed frequently.

Cool - Optimized for storing data that is infrequently accessed and stored for at least 30 days.

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). Note: Lease state of the blob. Possible values: available|leased|expired|breaking|broken

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

QUESTION NO: 125 - (HOTSPOT) - (Topic 5)

HOTSPOT

You have a virtual machine scale set named SS1.

You configure autoscaling as shown in the following exhibit.

You configure the scale out and scale in rules to have a duration of 10 minutes and a cool down time of 10 minutes.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

If SS1 scales to nine virtual machines, what is the minimum amount of time before SS1 will scale out?

- 10 minutes
- 20 minutes
- 30 minutes
- 60 minutes

If SS1 scales to nine virtual machines, and then the average processor utilization is 30 percent for one hour, how many virtual machines will be in SS1?

- 1
- 3
- 6
- 9
- 12
- 15

ANSWER:

Answer Area

If SS1 scales to nine virtual machines, what is the minimum amount of time before SS1 will scale out?

- 10 minutes
- 20 minutes
- 30 minutes
- 60 minutes

If SS1 scales to nine virtual machines, and then the average processor utilization is 30 percent for one hour, how many virtual machines will be in SS1?

- 1
- 3
- 6
- 9
- 12
- 15

Explanation:

Box 1: 20 Minutes.

10 minutes cool down time after the last scale-up plus 10 minutes duration equals 20 minutes.

Box 2: 9

30% does not match the scale in requirement of less than 25% so the number of virtual machines will not change.

QUESTION NO: 126 - (HOTSPOT) - (Topic 5)

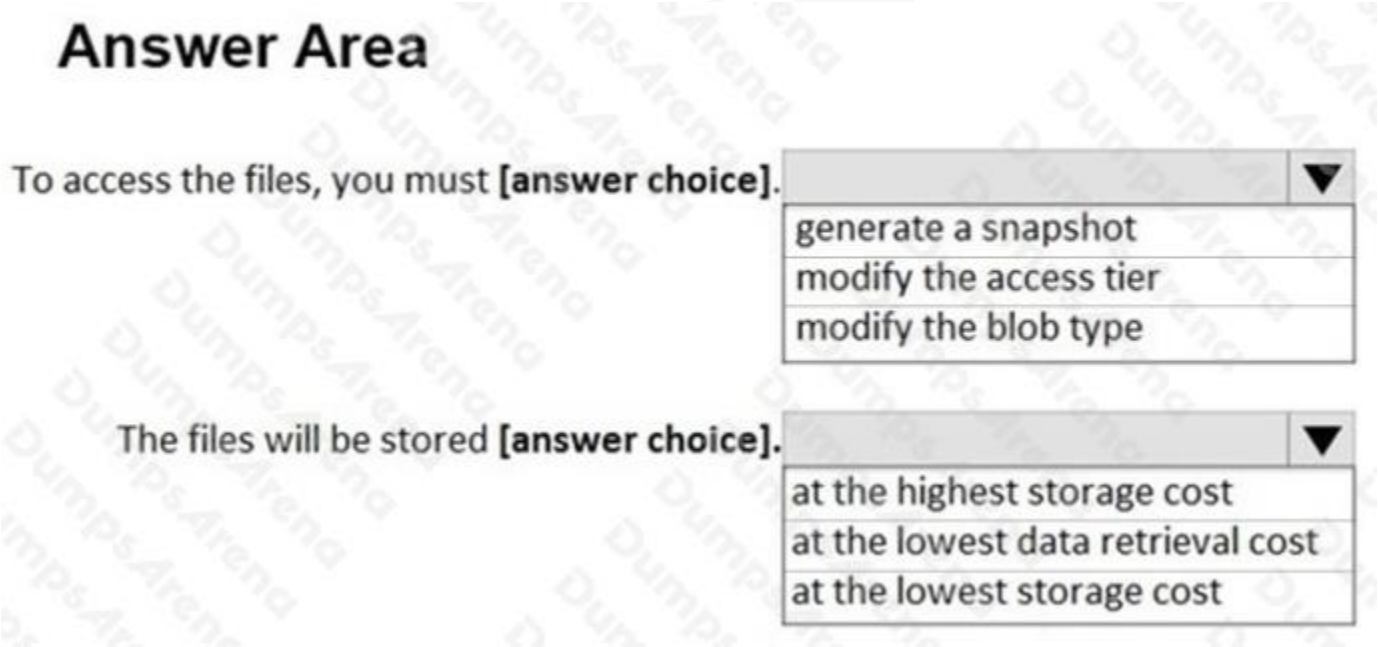
HOTSPOT

You plan to create a storage account and to save the files as shown in the following exhibit.

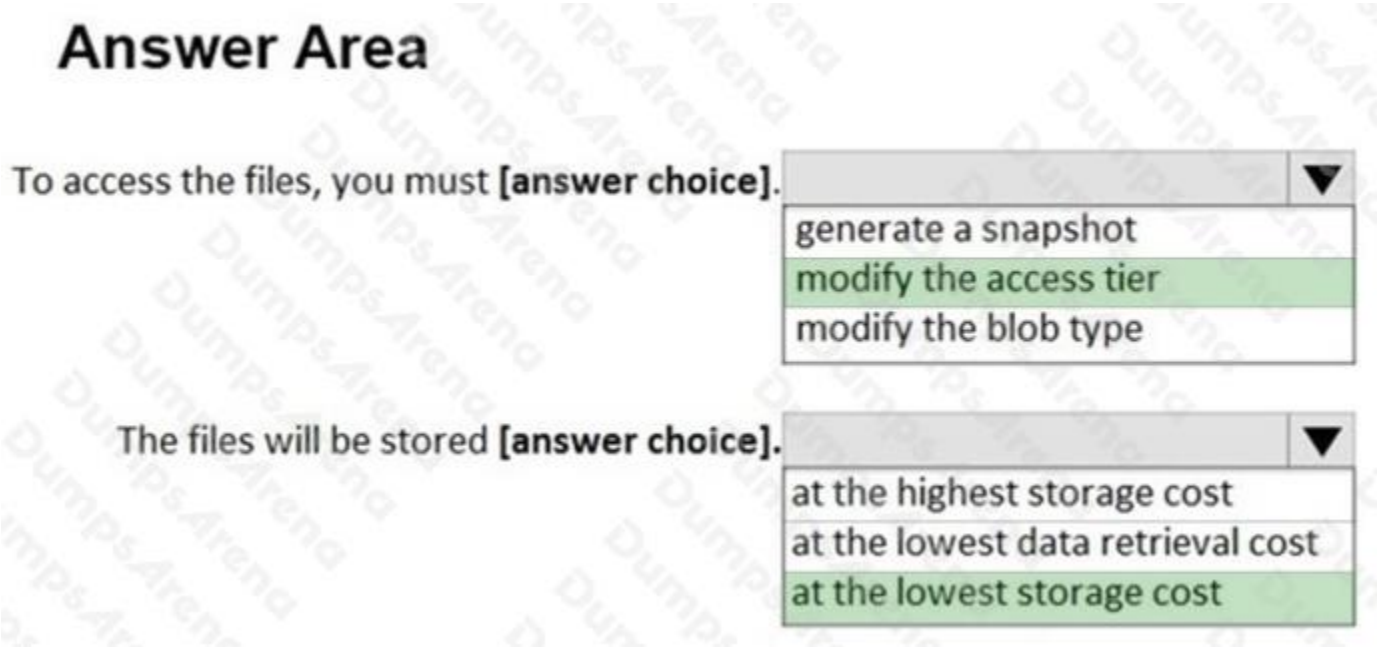
Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Hot Area:



ANSWER:



Explanation:

Reference:

https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blob-storage-tiers#archive-access-tier-preview

QUESTION NO: 127 - (HOTSPOT) - (Topic 5)

HOTSPOT

You need to recommend an Azure Storage account configuration for two applications named Application1 and Application2. The configuration must meet the following requirements:

- Storage for Application1 must provide the highest possible transaction rates and the lowest possible latency.
- Storage for Application2 must provide the lowest possible storage costs per GB. ▪ Storage for both applications must be optimized for uploads and downloads.
- Storage for both applications must be available in an event of datacenter failure.

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

Application1:

- BlobStorage with Standard performance, Hot access tier, and Read-access geo-redundant storage (RA-GRS) replication
- BlockBlobStorage with Premium performance and Zone-redundant storage (ZRS) replication
- General purpose v1 with Premium performance and Locally-redundant storage (LRS) replication
- General purpose v2 with Standard performance, Hot access tier, and Locally-redundant storage (LRS) replication

Application2:

- BlobStorage with Standard performance, Cool access tier, and Geo-redundant storage (GRS) replication
- BlockBlobStorage with Premium performance and Zone-redundant storage (ZRS) replication
- General purpose v1 with Standard performance and Read-access geo-redundant storage (RA-GRS) replication
- General purpose v2 with Standard performance, Cool access tier, and Read-access geo-redundant storage (RA-GRS) replication

ANSWER:

Answer Area

Application1:

- BlobStorage with Standard performance, Hot access tier, and Read-access geo-redundant storage (RA-GRS) replication
- BlockBlobStorage with Premium performance and Zone-redundant storage (ZRS) replication
- General purpose v1 with Premium performance and Locally-redundant storage (LRS) replication
- General purpose v2 with Standard performance, Hot access tier, and Locally-redundant storage (LRS) replication

Application2:

- BlobStorage with Standard performance, Cool access tier, and Geo-redundant storage (GRS) replication
- BlockBlobStorage with Premium performance and Zone-redundant storage (ZRS) replication
- General purpose v1 with Standard performance and Read-access geo-redundant storage (RA-GRS) replication
- General purpose v2 with Standard performance, Cool access tier, and Read-access geo-redundant storage (RA-GRS) replication

Explanation:

Box 1: BloblBlobStorage with Premium performance and Zone-redundant storage (ZRS) replication.

BlockBlobStorage accounts: Storage accounts with premium performance characteristics for block blobs and append blobs. Recommended for scenarios with high transactions rates, or scenarios that use smaller objects or require consistently low storage latency.

Premium: optimized for high transaction rates and single-digit consistent storage latency.

Box 2: General purpose v2 with Standard performance..

General-purpose v2 accounts: Basic storage account type for blobs, files, queues, and tables. Recommended for most scenarios using Azure Storage.

Incorrect Answers:

▪ Locally redundant storage (LRS) copies your data synchronously three times within a single physical location in the primary region ▪ Standard: optimized for high capacity and high throughput

▪ General-purpose v1 accounts: Legacy account type for blobs, files, queues, and tables. Use general-purpose v2 accounts instead when possible. ▪ BlobStorage accounts: Legacy Blob-only storage accounts. Use general-purpose v2 accounts instead when possible.

Reference: https://docs.microsoft.com/en-us/azure/storage/common/storage-account-overview https://docs.microsoft.com/en-us/azure/storage/common/storage-redundancy

QUESTION NO: 128 - (Topic 5)

Your company has 300 virtual machines hosted in a VMware environment. The virtual machines vary in size and have various utilization levels.

You plan to move all the virtual machines to Azure.

You need to recommend how many and what size Azure virtual machines will be required to move the current workloads to Azure. The solution must minimize administrative effort.

What should you use to make the recommendation?

A. Azure Pricing calculator

B. Azure Cost Management

C. Azure Advisor

D. Azure Migrate

ANSWER: D

QUESTION NO: 129 - (Topic 5)

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

ANSWER: C

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 NO: 130 - (Topic 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 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

ANSWER: B

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.

3. Either

▪ To enable legal holds, select Add Policy. Select Legal hold from the drop-down menu, or ▪ 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 NO: 131 - (Topic 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 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

ANSWER: B

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 NO: 132 - (Topic 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 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

ANSWER: B

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 NO: 133 - (Topic 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

ANSWER: B

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 NO: 134 - (Topic 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 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

ANSWER: B

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 NO: 135 - (Topic 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 a Recovery Services vault, and then using Azure Site Recovery.

Does this meet the goal?

A. Yes

B. No

ANSWER: A

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 NO: 136 - (Topic 5)

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.

ANSWER: D

Explanation:

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

DUMPSARENA

	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 NO: 137 - (Topic 5)

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

ANSWER: C

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 NO: 138 - (Topic 5)

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

ANSWER: A

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 NO: 139 - (DRAG DROP) - (Topic 5)

DRAG DROP

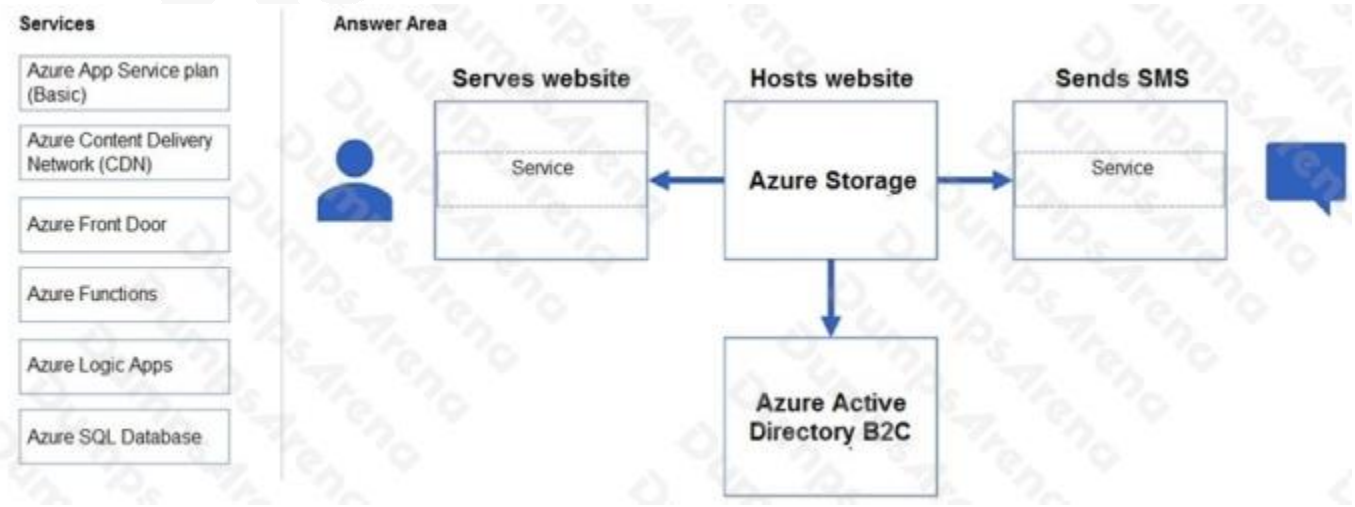
The developers at your company are building a static web app to support users sending text messages. The app must meet the following requirements:

- 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.

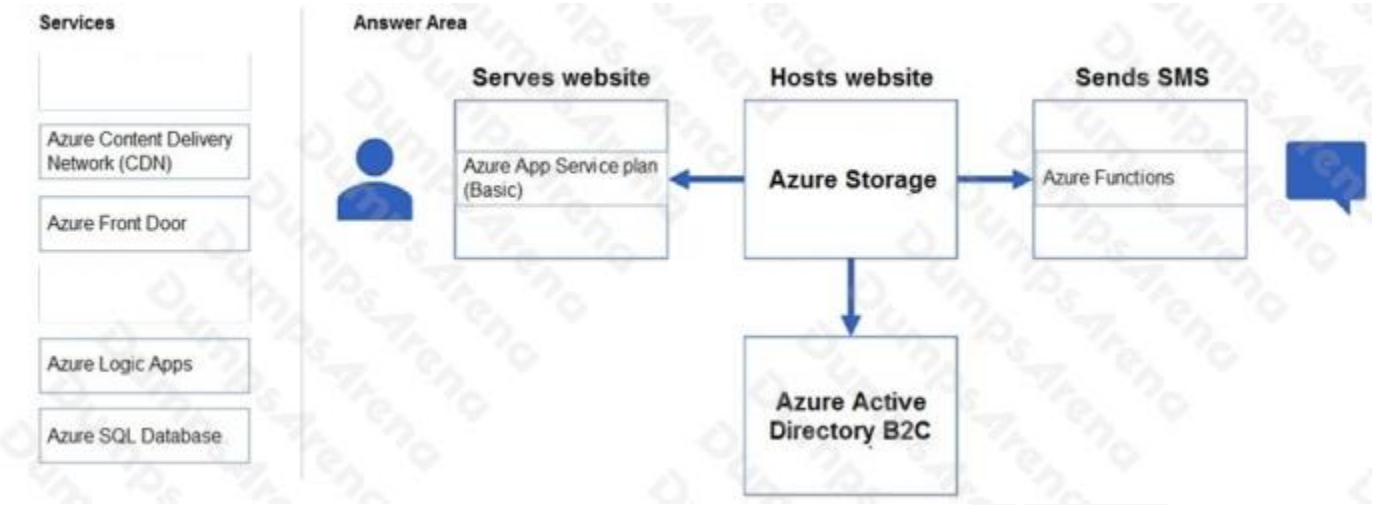
Which Azure service should you use to complete the architecture? To answer, drag the appropriate services to the correct locations. Each service may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:



ANSWER:



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 NO: 140 - (Topic 5)

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 Managed Instance Business Critical

C. Azure SQL Database Business Critical

D. Azure SQL Database Basic

ANSWER: A

Explanation:

Standard geo-replication is available with Standard and General Purpose databases in the current Azure Management Portal and standard APIs.

Incorrect Answers:

B, C: 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 NO: 141 - (Topic 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 using Azure Migrate.

Does this meet the goal?

A. Yes

B. No

ANSWER: B

Explanation:

To ensure that the virtual machines remain available during the migration, use Azure Site Recovery.

Reference:

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

QUESTION NO: 142 - (Topic 5)

The accounting department at your company migrates to a new financial accounting software. The accounting department must keep file-based database backups for seven years for compliance purposes. It is unlikely that the backups will be used to recover data.

You need to move the backups to Azure. The solution must minimize costs.

Where should you store the backups?

A. Azure Blob storage that uses the Archive tier

B. Azure SQL Database

C. Azure Blob storage that uses the Cool tier

D. a Recovery Services vault

ANSWER: A

Explanation:

Azure Front Door enables you to define, manage, and monitor the global routing for your web traffic by optimizing for best performance and instant global failover for high availability. With Front Door, you can transform your global (multi-region) consumer and enterprise applications into robust, high-performance personalized modern applications, APIs, and content that reaches a global audience with Azure.

Front Door works at Layer 7 or HTTP/HTTPS layer and uses anycast protocol with split TCP and Microsoft's global network for improving global connectivity.

Incorrect Answers:

B: Azure Traffic Manager uses DNS (layer 3) to shape traffic. SSL works at Layer 6.

Azure Traffic Manager can direct customers to their closest AKS cluster and application instance. For the best performance and redundancy, direct all application traffic through Traffic Manager before it goes to your AKS cluster.

Reference:

https://docs.microsoft.com/en-us/azure/frontdoor/front-door-overview

QUESTION NO: 143 - (Topic 5)

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

ANSWER: C

Explanation:

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

QUESTION NO: 144 - (Topic 5)

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

ANSWER: D

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 NO: 145 - (Topic 5)

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)

ANSWER: C

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 NO: 146 - (Topic 5)

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.

ANSWER: B C

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 NO: 147 - (Topic 5)

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

ANSWER: A

Explanation:

Asynchronous messaging can be implemented in a variety of different ways: with queues, topics, and subscriptions. Azure Service Bus supports asynchronism via a store and forward mechanism.

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 https://docs.microsoft.com/en-us/azure/service-bus-messaging/service-bus-async-messaging https://docs.microsoft.com/en-us/azure/architecture/guide/technology-choices/messaging

QUESTION NO: 148 - (Topic 5)

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

ANSWER: D

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 NO: 149 - (Topic 5)

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

ANSWER: C

QUESTION NO: 150 - (Topic 5)

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

ANSWER: C

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 NO: 151 - (Topic 5)

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

ANSWER: D

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 NO: 152 - (HOTSPOT) - (Topic 5)

HOTSPOT

Your company deploys an Azure App Service Web App.

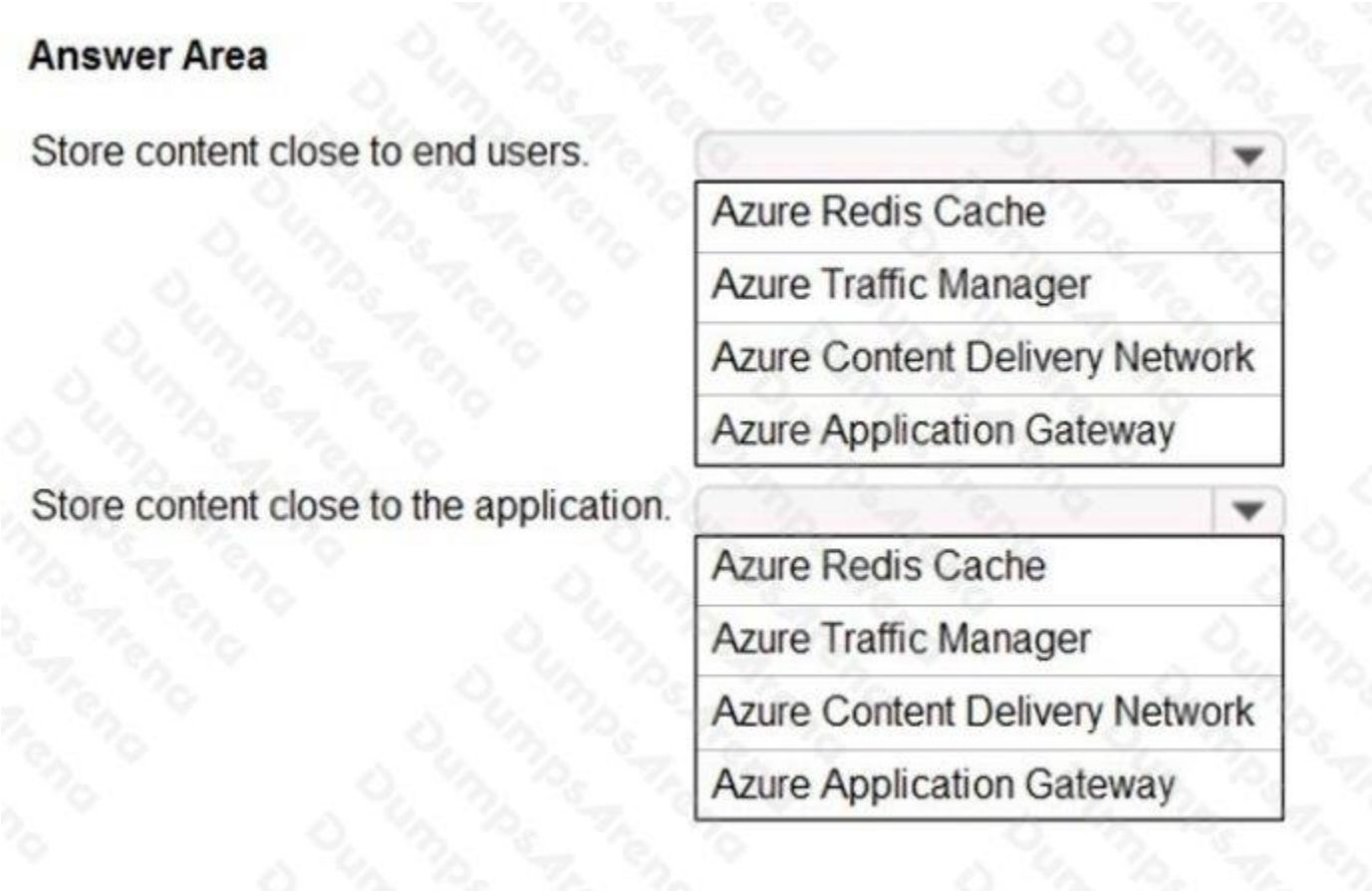
During testing the application fails under load. The application cannot handle more than 100 concurrent user sessions. You enable the Always On feature. You also configure auto-scaling to increase instance counts from two to 10 based on HTTP queue length.

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:

Answer Area

Store content close to end users.

- Azure Redis Cache
- Azure Traffic Manager
- Azure Content Delivery Network
- Azure Application Gateway

Store content close to the application.

- Azure Redis Cache
- Azure Traffic Manager
- Azure Content Delivery Network
- Azure Application Gateway

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 NO: 153 - (Topic 5)

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

ANSWER: A

QUESTION NO: 154 - (DRAG DROP) - (Topic 5)

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)

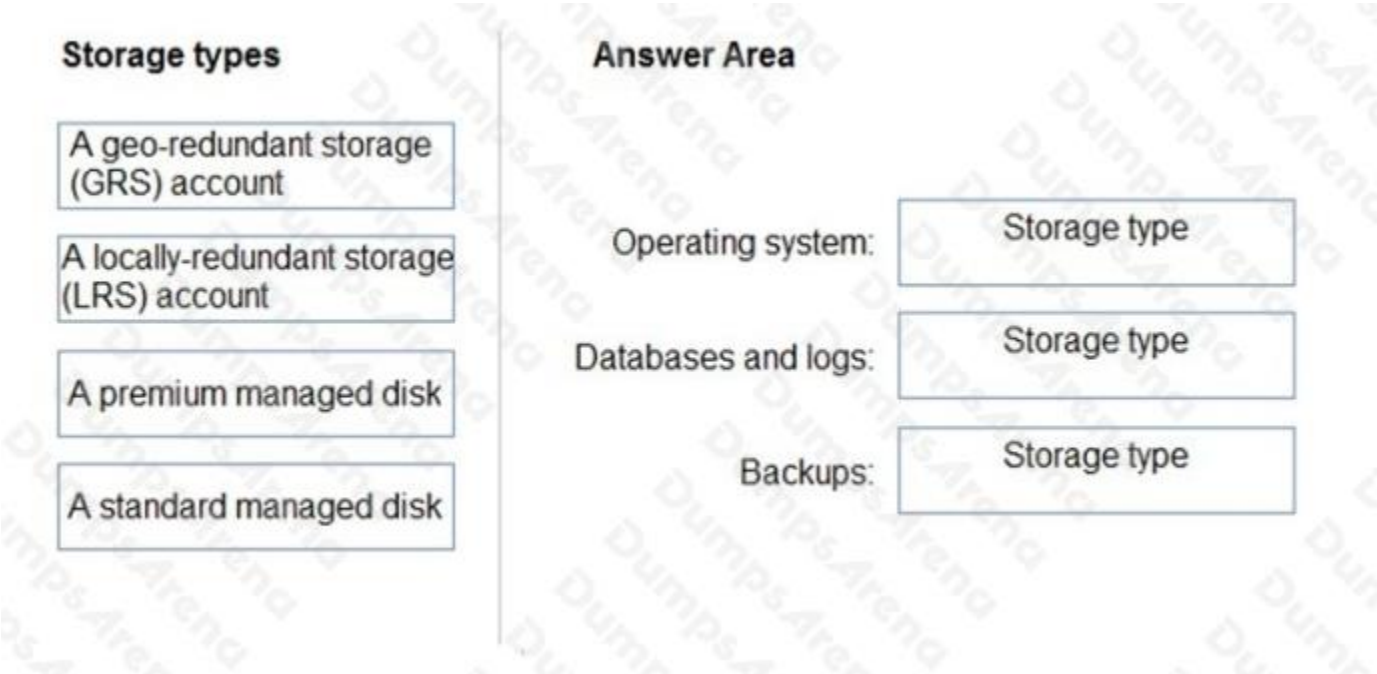
You identify the storage priorities for various data types as shown in the following table.

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

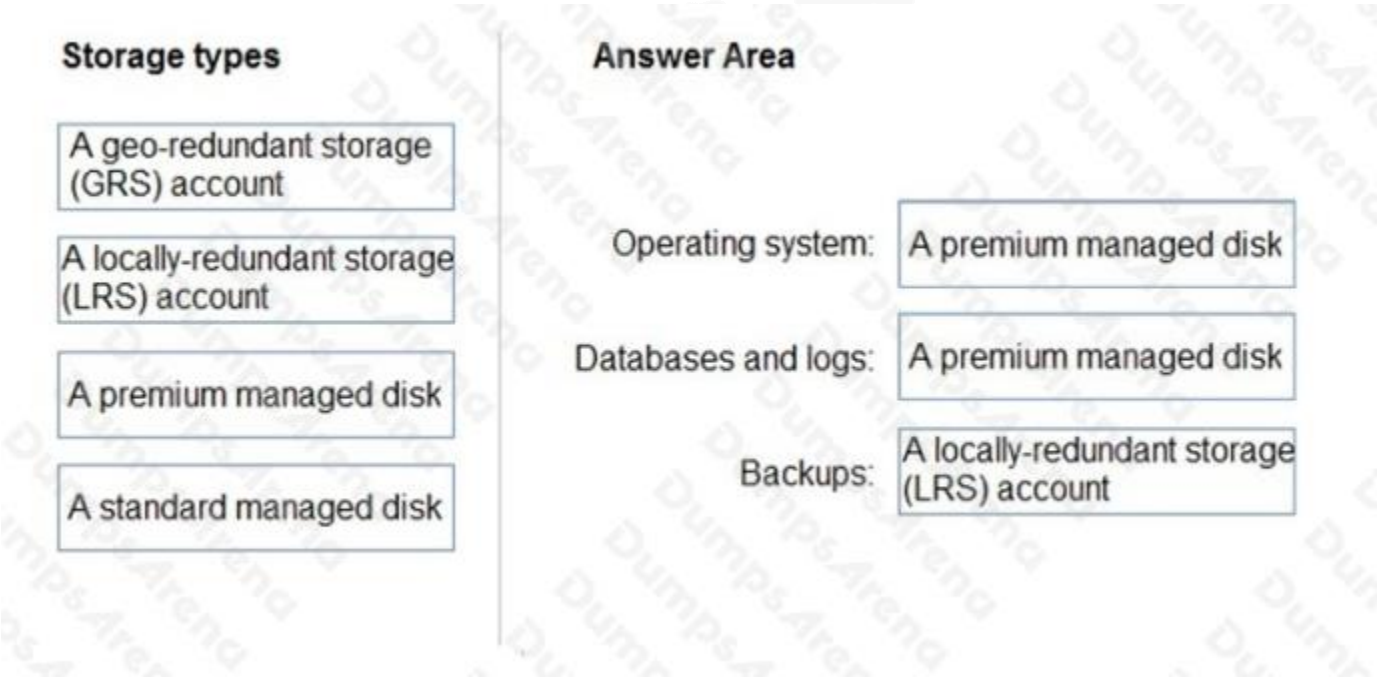
Which storage type should you recommend for each data type? To answer, drag the appropriate storage types to the correct data types. Each storage type may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:



ANSWER:



Explanation:

QUESTION NO: 155 - (Topic 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.

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

ANSWER: B

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/

QUESTION NO: 156 - (Topic 5)

You have an application that sends events to an Azure event hub by using HTTP requests over the internet.

You plan to increase the number of application instances.

You need to recommend a solution to reduce the overhead associated with sending events to the hub.

What should you recommend?

A. Configure the application to send events by using the AMQP protocol

B. Reduce the retention period of the event hub.

C. Replace the event hub with an Azure Service Bus instance.

D. Configure the application to send events by using the HTTPS protocol.

ANSWER: A

Explanation:

Compared to HTTP, AMQP is easy to scale.

Note: Facts pro-AMQP

Delivering messages with AMQP gives you reliability and being asynchronous allows you to not worry about the delivery at all.

Incorrect Answres:

B: Changing the retention period would not reduce the overhead.

C: Azure event hub has a low latency compared to Azure Service Bus.

D: Overhead increases with HTTPS compared to HTTP.

Reference:

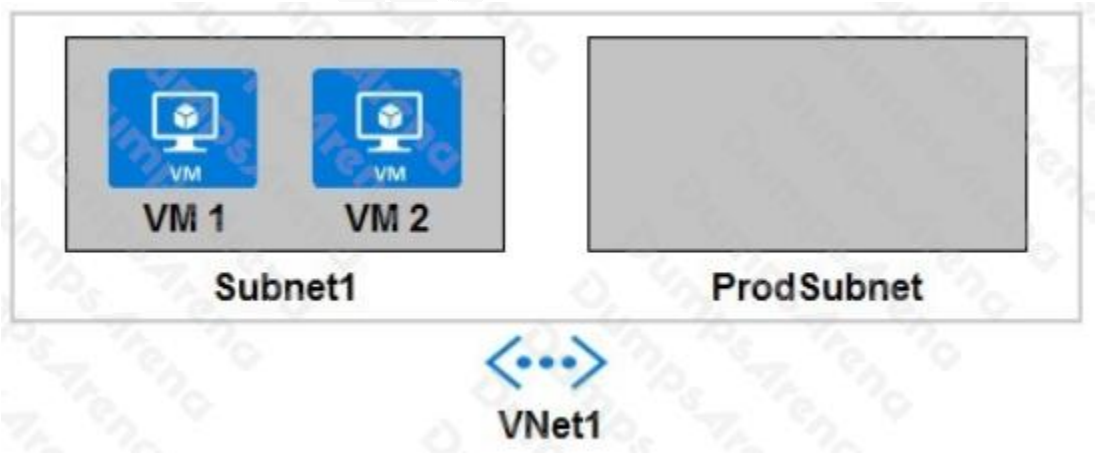
https://dev.to/fedejsoren/amqp-vs-http

QUESTION NO: 157 - (HOTSPOT) - (Topic 5)

HOTSPOT

Your company develops a web service that is deployed to an Azure virtual machine named VM1. The web service allows an API to access real-time data from VM1.

The current virtual machine deployment is shown in the Deployment exhibit. (Click the Deployment tab).



The chief technology officer (CTO) sends you the following email message: “Our developers have deployed the web service to a virtual machine named VM1. Testing has shown that the API is accessible from VM1 and VM2. Our partners must be able to connect to the API over the Internet. Partners will use this data in applications that they develop.” You deploy an

Azure API Management (APIM) service. The relevant API Management configuration is shown in the API exhibit. (Click the API tab.)

Virtual network: Off | **External** | Internal

LOCATION	VIRTUAL NETWORK	SUBNET
West Europe	VNet1	ProdSubnet

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
The API is available to partners over the Internet.	○	○
The APIM instance can access real-time data from VM1.	○	○
A VPN gateway is required for partner access.	○	○

ANSWER:

Answer Area

Statements	Yes	No
The API is available to partners over the Internet.	○	○
The APIM instance can access real-time data from VM1.	○	○
A VPN gateway is required for partner access.	○	○

Explanation:

Reference: https://docs.microsoft.com/en-us/azure/api-management/api-management-using-with-vnet

QUESTION NO: 158 - (DRAG DROP) - (Topic 5)

DRAG DROP

You have an Azure subscription. The subscription contains Azure virtual machines that run Windows Server 2016 and Linux.

You need to use Azure Monitor to design an alerting strategy for security-related events.

Which Azure Monitor Logs tables should you query? To answer, drag the appropriate tables to the correct log types. 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:

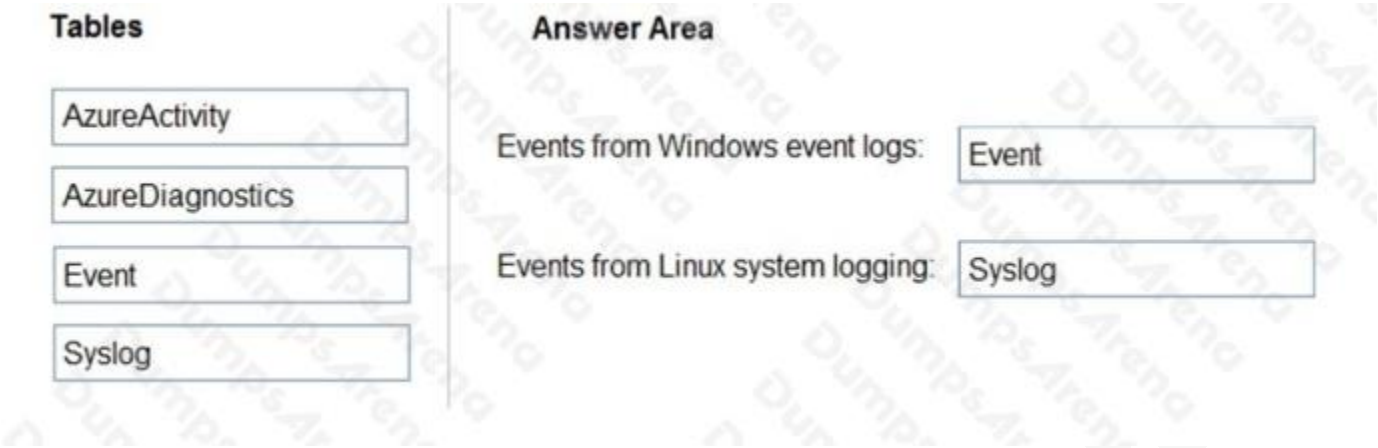
Tables

- AzureActivity
- AzureDiagnostics
- Event
- Syslog

Answer Area

Events from Windows event logs:	Table
Events from Linux system logging:	Table

ANSWER:



Explanation:

QUESTION NO: 159 - (DRAG DROP) - (Topic 5)

DRAG DROP

You are designing a network connectivity strategy for a new Azure subscription. You identify the following requirements:

- The Azure virtual machines on a subnet named Subnet1 must be accessible only from the computers in your London office.

- Engineers require access to the Azure virtual machines on a subnet named Subsnet2 over the Internet on a specific TCP/IP management port.

- The Azure virtual machines in the West Europe Azure region must be able to communicate on all ports to the Azure virtual machines in the North Europe Azure region. - Azure virtual machines on Subnet1 and Subnet2 have public IP addresses.

You need to recommend which components must be used to meet the requirements. The solution must minimize costs and administrative effort whenever possible.

What should you include in the recommendation? To answer, drag the appropriate components to the correct requirements. Each component 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:

Components	Answer Area	
An Azure ExpressRoute connection	The Azure virtual machines on Subnet1 must be accessible only from the computers in the London office:	Component
A network security group (NSG)	Engineers require access to the Azure virtual machines on Subnet2 over the Internet on a specific TCP/IP management port:	Component
A new virtual network	The Azure virtual machines in the West Europe region must be able to communicate on all ports to the Azure virtual machines in the North Europe region:	Component
A site-to-site VPN		
Virtual network peering		

ANSWER:

Components	Answer Area	
An Azure ExpressRoute connection	The Azure virtual machines on Subnet1 must be accessible only from the computers in the London office:	A site-to-site VPN
A network security group (NSG)	Engineers require access to the Azure virtual machines on Subnet2 over the Internet on a specific TCP/IP management port:	A network security group (NSG)
A new virtual network	The Azure virtual machines in the West Europe region must be able to communicate on all ports to the Azure virtual machines in the North Europe region:	Virtual network peering
A site-to-site VPN		
Virtual network peering		

Explanation:

QUESTION NO: 160 - (Topic 5)

You are designing a container solution in Azure that will include two containers. One container will host a web API that will be available to the public. The other container will perform health monitoring of the web API and will remain private. The two containers will be deployed together as a group.

You need to recommend a compute service for the containers. The solution must minimize costs and maintenance overhead.

What should you include in the recommendation?

A. Azure Service Fabric

B. Azure Kubernetes Service (AKS)

C. Azure Container Instances

D. Azure Container registries

ANSWER: C

Explanation:

Azure Container Instances supports the deployment of multiple containers onto a single host using a container group. A container group is useful when building an application sidecar for logging, monitoring, or any other configuration where a service needs a second attached process.

Reference:

https://docs.microsoft.com/en-us/azure/container-instances/container-instances-multi-container-group

QUESTION NO: 161 - (Topic 5)

You plan to run an image rendering workload in Azure. The workload uses parallel compute processes.

What is the best service to use to run the workload? More than one answer choice may achieve the goal. Select the BEST answer.

A. an Azure virtual machine scale set

B. Azure Function App

C. Azure Kubernetes Service (AKS)

D. Azure Batch

ANSWER: D

Explanation:

Azure Batch works well with intrinsically parallel (also known as "embarrassingly parallel") workloads. Intrinsically parallel workloads are those where the applications can run independently, and each instance completes part of the work. When the applications are executing, they might access some common data, but they do not communicate with other instances of the application. Intrinsically parallel workloads can therefore run at a large scale, determined by the amount of compute resources available to run applications simultaneously.

Reference:

https://docs.microsoft.com/en-us/azure/batch/batch-technical-overview

QUESTION NO: 162 - (Topic 5)

You are designing a microservices architecture that will use Azure Kubernetes Service (AKS) to host pods that run containers. Each pod deployment will host a separate API. Each API will be implemented as a separate service.

You need to recommend a solution to make the APIs available to external users from Azure API Management. The solution must meet the following requirements:

▪ Control access to the APIs by using mutual TLS authentication between API Management and the AKS-based APIs. ▪ Provide access to the APIs by using a single IP address.

What should you recommend to provide access to the APIs?

A. the LoadBalancer service in AKS

B. custom network security groups (NSGs)

C. the Ingress Controller in AKS

ANSWER: C

Explanation:

An ingress controller is a piece of software that provides reverse proxy, configurable traffic routing, and TLS termination for Kubernetes services. Kubernetes ingress resources are used to configure the ingress rules and routes for individual Kubernetes services. Using an ingress controller and ingress rules, a single IP address can be used to route traffic to multiple services in a Kubernetes cluster.

Reference:

https://docs.microsoft.com/en-us/azure/aks/ingress-basic

QUESTION NO: 163 - (HOTSPOT) - (Topic 5)

HOTSPOT

You are designing a cost-optimized solution that uses Azure Batch to run two types of jobs on Linux nodes. The first job type will consist of short-running tasks for a development environment.

The second jot type will consist of long-running Message Passing Interface (MPI) applications for a production environment that requires timely job completion.

You need to recommend the pool type and node type for each job type. The solution must minimize compute charges and leverage Azure Hybrid Benefit whenever possible.

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

First job:

- Batch service and dedicated virtual machines
- User subscription and dedicated virtual machines
- User subscription and low-priority virtual machines

Second job:

- Batch service and dedicated virtual machines
- User subscription and dedicated virtual machines
- User subscription and low-priority virtual machines

ANSWER:

Answer Area

First job:

- Batch service and dedicated virtual machines
- User subscription and dedicated virtual machines
- User subscription and low-priority virtual machines

Second job:

- Batch service and dedicated virtual machines
- User subscription and dedicated virtual machines
- User subscription and low-priority virtual machines

Explanation:

Box 1: User subscription and low-priority virtual machines

Azure Batch offers low-priority virtual machines (VMs) to reduce the cost of Batch workloads. Low-priority VMs make new types of Batch workloads possible by enabling a large amount of compute power to be used for a very low cost.

Some examples of batch processing use cases well suited to use low-priority VMs are:

▪ Development and testing: In particular, if large-scale solutions are being developed, significant savings can be realized. All types of testing can benefit, but large-scale load testing and regression testing are great uses.

▪ Supplementing on-demand capacity. ▪ Flexible job execution time.

Box 2: Batch service and dedicate virtual machines

Reference:

https://docs.microsoft.com/en-us/azure/batch/batch-low-pri-vms

QUESTION NO: 164 - (Topic 5)

Your company has an on-premises Windows HPC cluster. The cluster runs a parallel, compute-intensive workload that performs financial risk modeling.

You plan to migrate the workload to Azure Batch.

You need to design a solution that will support the workload. The solution must meet the following requirements:

▪ Support the large-scale parallel execution of Azure Batch jobs. ▪ Minimize cost.

What should you include in the solution?

A. burstable virtual machines

B. low-priority virtual machines

C. Azure virtual machine sizes that support the Message Passing Interface (MPI) API

D. Basic A-series virtual machines

ANSWER: B

Explanation:

Reference: https://docs.microsoft.com/en-us/azure/batch/batch-technical-overview

QUESTION NO: 165 - (Topic 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.

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 an Azure policy to enforce the resource group location.

Does this meet the goal?

A. Yes

B. No

ANSWER: A

Explanation:

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

Reference:

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

QUESTION NO: 166 - (Topic 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.

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 creating resource groups based on locations and implementing resource locks on the resource groups.

Does this meet the goal?

A. Yes

B. No

ANSWER: B

Explanation:

Resource locks are not used for compliance purposes. Resource locks prevent changes from being made to resources.

Reference:

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

QUESTION NO: 167 - (Topic 5)

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)

ANSWER: B

QUESTION NO: 168 - (Topic 5)

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

ANSWER: A

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 NO: 169 - (Topic 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 a virtual machine scale set that uses autoscaling.

Does this meet the goal?

A. Yes

B. No

ANSWER: B

Explanation:

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

QUESTION NO: 170 - (Topic 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 you deploy an Azure Application Gateway.

Does this meet the goal?

A. Yes

B. No

ANSWER: B

Explanation:

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

QUESTION NO: 171 - (Topic 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 plan to deploy multiple instances of an Azure web app across several Azure regions.

You need to design an access solution for the app. The solution must meet the following replication requirements:

- Support rate limiting.
- Balance requests between all instances.
- Ensure that users can access the app in the event of a regional outage.

Solution: You use Azure Front Door to provide access to the app.

Does this meet the goal?

A. Yes

B. No

ANSWER: A

Explanation:

Reference:

https://docs.microsoft.com/en-us/azure/frontdoor/front-door-overview https://docs.microsoft.com/en-us/azure/frontdoor/front-door-waf https://www.cloudmatter.io/post/azure-front-door-and-web-application-firewall-cheatsheet

QUESTION NO: 172 - (Topic 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 plan to deploy multiple instances of an Azure web app across several Azure regions.

You need to design an access solution for the app. The solution must meet the following replication requirements:

- Support rate limiting.
- Balance requests between all instances.
- Ensure that users can access the app in the event of a regional outage.

Solution: You use Azure Load Balancer to provide access to the app.

Does this meet the goal?

A. Yes

B. No

ANSWER: B

Explanation:

Load Balancer distributes inbound flows that arrive at the load balancer's front end to backend pool instances but it does not provide high availability at the regional level.

Reference:

https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-overview

QUESTION NO: 173 - (Topic 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 plan to deploy multiple instances of an Azure web app across several Azure regions.

You need to design an access solution for the app. The solution must meet the following replication requirements:

- Support rate limiting.
- Balance requests between all instances.
- Ensure that users can access the app in the event of a regional outage.

Solution: You use Azure Traffic Manager to provide access to the app.

Does this meet the goal?

A. Yes

B. No

ANSWER: B

Explanation:

Azure Traffic Manager is a DNS-based traffic load balancer. This service allows you to distribute traffic to your public facing applications across the global Azure regions. Traffic Manager also provides your public endpoints with high availability and quick responsiveness. It does not provide rate limiting.

Reference: https://docs.microsoft.com/en-us/azure/app-service/web-sites-traffic-manager https://docs.microsoft.com/en-us/azure/traffic-manager/traffic-manager-overview

QUESTION NO: 174 - (Topic 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 you create a Traffic Manager profile.

Does this meet the goal?

A. Yes

B. No

ANSWER: A

QUESTION NO: 175 - (HOTSPOT) - (Topic 5)

HOTSPOT

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

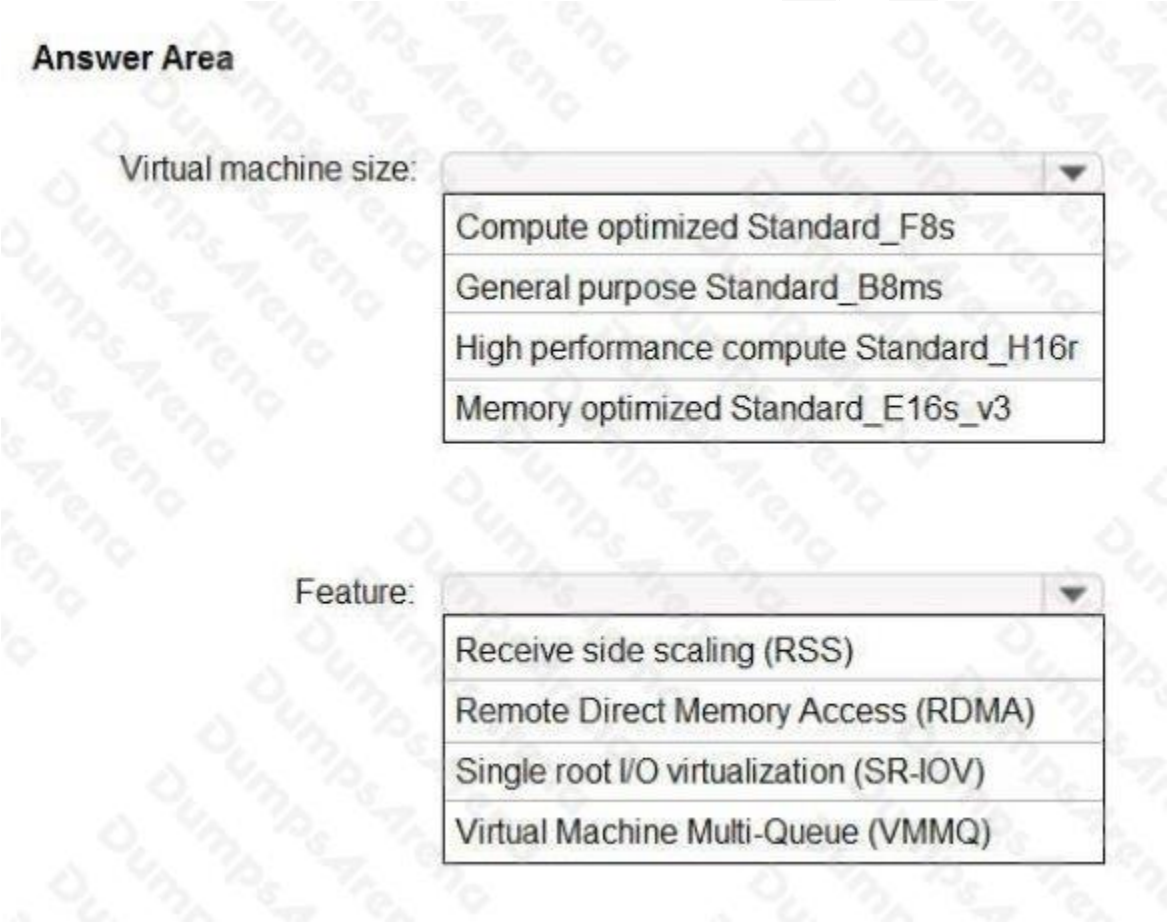
You need to recommend a solution that meets the following requirements:

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

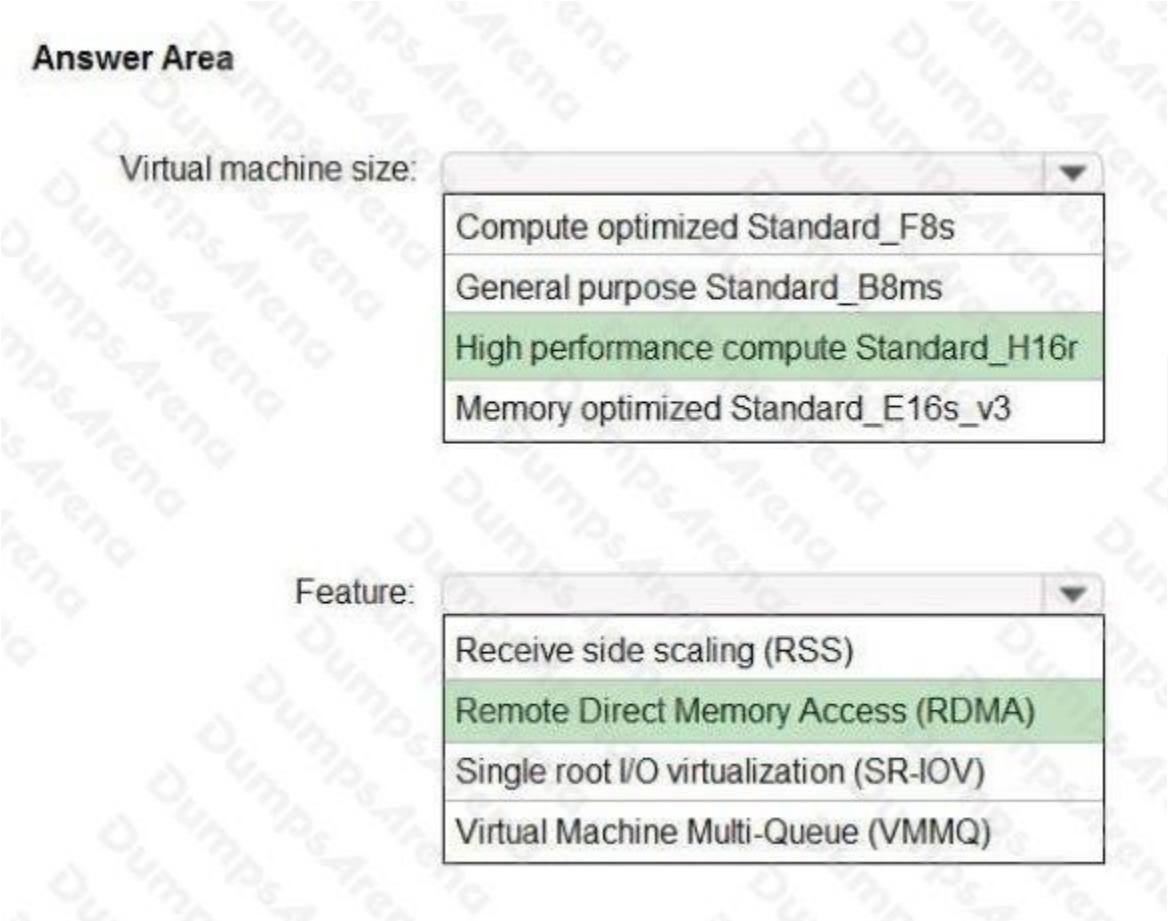
Which virtual machine size and feature should you use? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



ANSWER:



Explanation:

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

QUESTION NO: 176 - (Topic 5)

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

ANSWER: C

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 NO: 177 - (Topic 5)

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.

ANSWER: A C

QUESTION NO: 178 - (Topic 5)

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 Fabric

B. Azure Blob storage

C. Azure Queue storage

D. Azure Traffic Manager

ANSWER: A

Explanation:

Asynchronous messaging can be implemented in a variety of different ways: with queues, topics, and subscriptions. Azure Service Bus supports asynchronism via a store and forward mechanism.

Reference: https://docs.microsoft.com/en-us/azure/service-bus-messaging/service-bus-async-messaging https://docs.microsoft.com/en-us/azure/architecture/guide/technology-choices/messaging https://docs.microsoft.com/en-us/azure/service-fabric/service-fabric-reliable-services-quick-start

QUESTION NO: 179 - (Topic 5)

You are designing a solution that will include containerized applications running in an Azure Kubernetes Service (AKS) cluster.

You need to recommend a load balancing solution for HTTPS traffic. The solution must meet the following requirements:

- Automatically configure load balancing rules as the applications are deployed to the cluster.
- Support Azure Web Application Firewall (WAF).
- Support cookie-based affinity. • Support URL routing.

What should you include the recommendation?

A. an NGINX ingress controller

B. Application Gateway Ingress Controller (AGIC)

C. an HTTP application routing ingress controller

D. the Kubernetes load balancer service

ANSWER: B

Explanation:

Much like the most popular Kubernetes Ingress Controllers, the Application Gateway Ingress Controller provides several features, leveraging Azure's native Application Gateway L7 load balancer. To name a few:

- URL routing
- Cookie-based affinity
- Secure Sockets Layer (SSL) termination
- End-to-end SSL
- Support for public, private, and hybrid web sites
- Integrated support of Azure web application firewall

Application Gateway redirection support isn't limited to HTTP to HTTPS redirection alone. This is a generic redirection mechanism, so you can redirect from and to any port you define using rules. It also supports redirection to an external site as well.

Reference:

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

QUESTION NO: 180 - (Topic 5)

You plan to deploy an Azure App Service web app that will have multiple instances across multiple Azure regions.

You need to recommend a load balancing service for the planned deployment. The solution must meet the following requirements:

- Maintain access to the app in the event of a regional outage.
- Support Azure Web Application Firewall (WAF).
- Support cookie-based affinity. ▪ Support URL routing.

What should you include in the recommendation?

A. Azure Front Door

B. Azure Load Balancer

C. Azure Traffic Manager

D. Azure Application Gateway

ANSWER: B

Explanation:

Azure Traffic Manager performs the global load balancing of web traffic across Azure regions, which have a regional load balancer based on Azure Application Gateway. This combination gets you the benefits of Traffic Manager many routing rules and Application Gateway's capabilities such as WAF, TLS termination, path-based routing, cookie-based session affinity among others.

Reference:

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

QUESTION NO: 181 - (Topic 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 a web app in an Isolated App Service plan.

Does this meet the goal?

A. Yes

B. No

ANSWER: B

Explanation:

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

QUESTION NO: 182 - (Topic 5)

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

What should you include in the recommendation?

A. a new product

B. a modification to the URL scheme

C. a new policy

ANSWER: C

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 NO: 183 - (Topic 5)

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

ANSWER: A

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 NO: 184 - (DRAG DROP) - (Topic 5)

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:

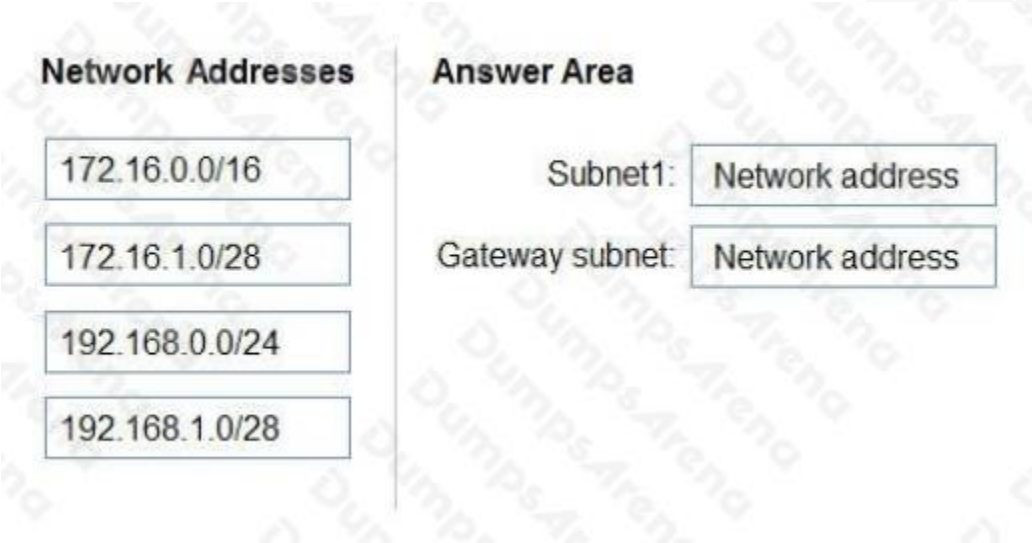
- All Azure virtual machines must be placed on the same subnet named Subnet1.
- All the Azure virtual machines must be able to communicate with all on-premises servers.
- The servers must be able to communicate between the on-premises network and Azure by using a site-to-site VPN.

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

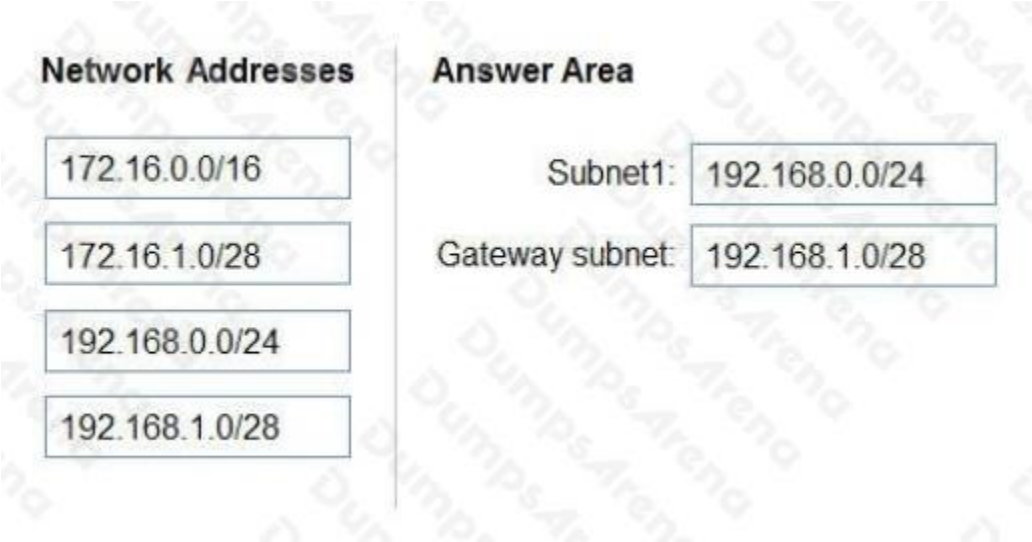
What should you include in the recommendation? To answer, drag the appropriate network addresses to the correct subnets. Each network address may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:



ANSWER:



Explanation:

QUESTION NO: 185 - (Topic 5)

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

ANSWER: D

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 NO: 186 - (Topic 5)

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 logic 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

ANSWER: C

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 NO: 187 - (Topic 5)

You have an Azure subscription that contains a Windows Virtual Desktop tenant.

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

▪ Start and stop Windows Virtual Desktop session hosts based on business hours. ▪ Scale out Windows Virtual Desktop session hosts when required. ▪ Minimize compute costs.

What should you include in the recommendation?

A. Microsoft Intune

B. a Windows Virtual Desktop automation task

C. Azure Automation

D. Azure Service Health

ANSWER: C

Explanation:

Reference: https://www.ciraltos.com/automatically-start-and-stop-wvd-vms-with-azure-automation/ https://wvdlogix.net/windows-virtual-desktop-host-pool-automation-2 https://getnerdio.com/academy/how-to-optimize-windows-virtual-desktop-wvd-azure-costs-with-event-based-autoscaling-and-azure-vm-scale-sets/

QUESTION NO: 188 - (Topic 5)

You have an Azure subscription.

You need to deploy an Azure Kubernetes Service (AKS) solution that will use Windows Server 2019 nodes. The solution must meet the following requirements:

▪ Minimize the time it takes to provision compute resources during scale-out operations. ▪ Support autoscaling of Windows Server containers.

Which scaling option should you recommend?

A. cluster autoscaler

B. horizontal pod autoscaler

C. Kubernetes version 1.20.2 or newer

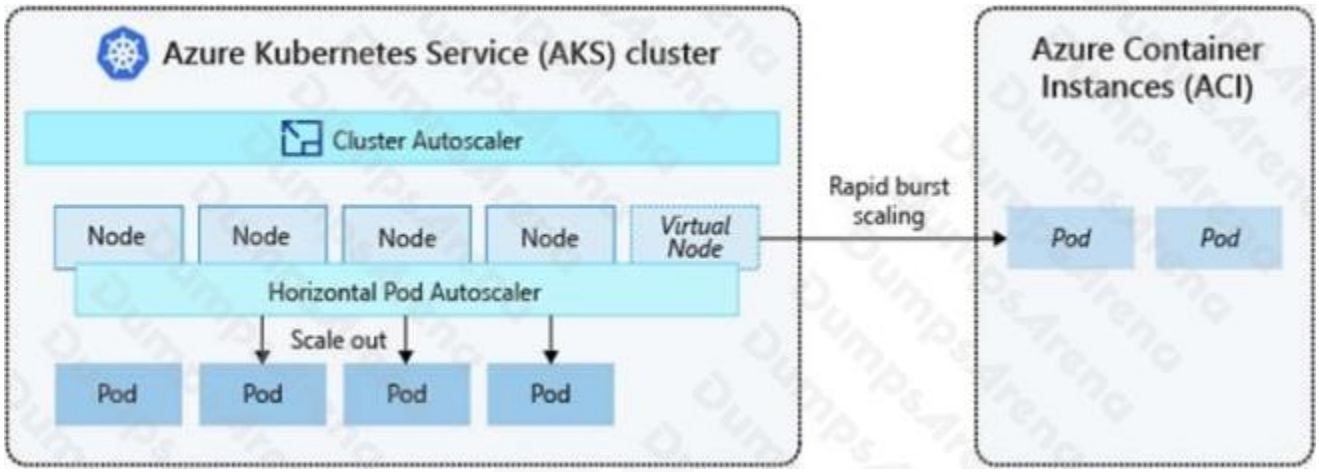
D. Virtual nodes with Virtual Kubelet ACI

ANSWER: A

Explanation:

Azure Container Instances (ACI) lets you quickly deploy container instances without additional infrastructure overhead. When you connect with AKS, ACI becomes a secured, logical extension of your AKS cluster. The virtual nodes component, which is based on Virtual Kubelet, is installed in your AKS cluster that presents ACI as a virtual Kubernetes node. Kubernetes can then schedule pods that run as ACI instances through virtual nodes, not as pods on VM nodes directly in your AKS cluster.

Your application requires no modification to use virtual nodes. Deployments can scale across AKS and ACI and with no delay as cluster autoscaler deploys new nodes in your AKS cluster.



Note: AKS clusters can scale in one of two ways:

- The cluster autoscaler watches for pods that can't be scheduled on nodes because of resource constraints. The cluster then automatically increases the number of nodes.

- The horizontal pod autoscaler uses the Metrics Server in a Kubernetes cluster to monitor the resource demand of pods. If an application needs more resources, the number of pods is automatically increased to meet the demand.

Incorrect Answers:

B: To rapidly scale your AKS cluster, you can integrate with Azure Container Instances (ACI). Kubernetes has built-in components to scale the replica and node count. However, if your application needs to rapidly scale, the horizontal pod autoscaler may schedule more pods than can be provided by the existing compute resources in the node pool. If configured, this scenario would then trigger the cluster autoscaler to deploy additional nodes in the node pool, but it may take a few minutes for those nodes to successfully provision and allow the Kubernetes scheduler to run pods on them.

Reference:

https://docs.microsoft.com/en-us/azure/aks/concepts-scale5

QUESTION NO: 189 - (Topic 5)

You plan to deploy an application that will run in a Linux-based Docker container.

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

- Support a custom domain name and an associated SSL certificate.
- Scale-out automatically based on demand. ▪ Minimize administrative effort and costs.

What should you include in the recommendation?

A. Azure App Service

B. Azure Container Instances

C. an Azure virtual machine

D. Azure Kubernetes Service (AKS)

ANSWER: A

Explanation:

App Service not only adds the power of Microsoft Azure to your application, such as security, load balancing, autoscaling, and automated management. You can also take advantage of its DevOps capabilities, such as continuous deployment from Azure DevOps, GitHub, Docker Hub, and other sources, package management, staging environments, custom domain, and TLS/SSL certificates.

Key features of App Service include:

- Containerization and Docker - Dockerize your app and host a custom Windows or Linux container in App Service.
- Scale up or out manually or automatically. Host your apps anywhere in Microsoft's global datacenter infrastructure, and the App Service SLA promises high availability.

App Service can also host web apps natively on Linux for supported application stacks. It can also run custom Linux containers (also known as Web App for Containers).

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

QUESTION NO: 190 - (HOTSPOT) - (Topic 5)

HOTSPOT

You are designing an Azure web app.

You plan to deploy the web app to the North Europe Azure region and the West Europe Azure region.

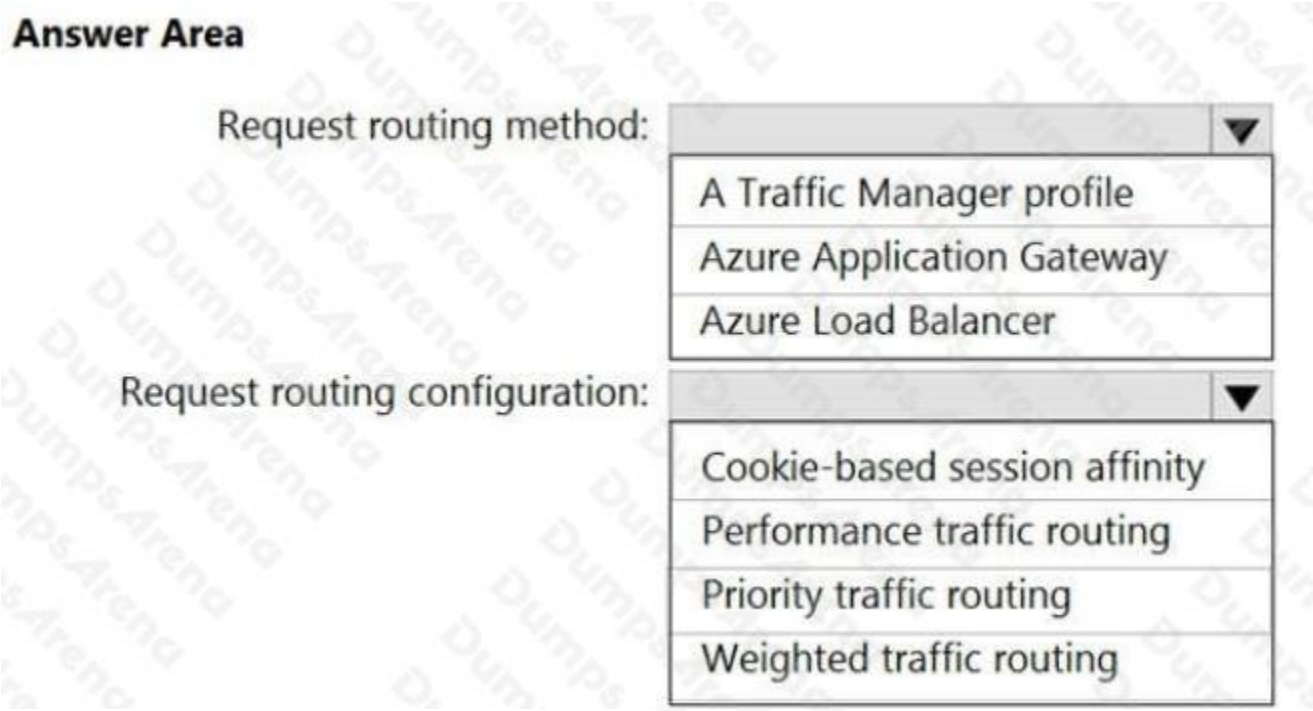
You need to recommend a solution for the web app. The solution must meet the following requirements:

- Users must always access the web app from the North Europe region, unless the region fails.
- The web app must be available to users if an Azure region is unavailable. ▪ Deployment costs must be minimized.

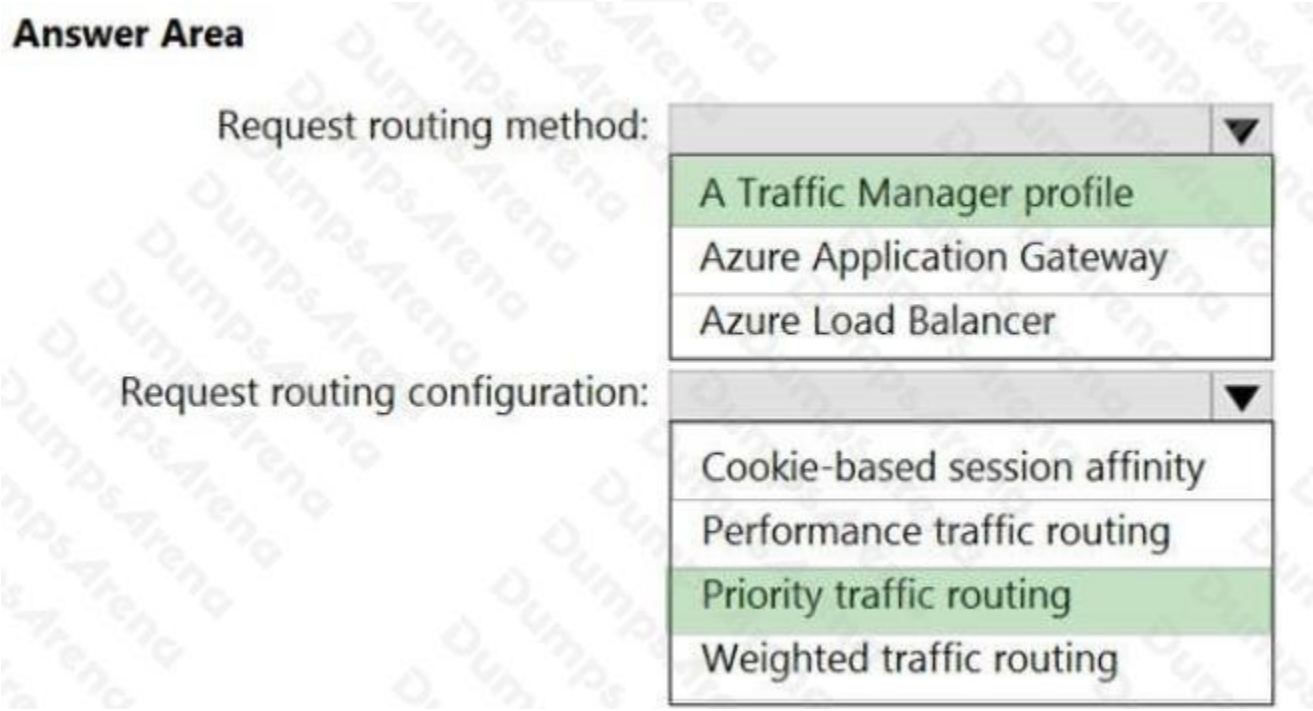
What should you include in the recommendation? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



ANSWER:



Explanation:

QUESTION NO: 191 - (HOTSPOT) - (Topic 5)

HOTSPOT

You have the application architecture 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 change the front end to an active/active architecture in which both regions process incoming connections, you must **[answer choice]**.

- add a load balancer to each region
- add an Azure Application Gateway to each region
- add an Azure content delivery network (CDN)
- modify the Azure Traffic Manager routing method

To control the threshold for failing over the front end to the standby region, you must configure the **[answer choice]**.

- Application Insights availability test
- Azure SQL Database failover groups
- Connection Monitor in Azure Network Watcher
- Endpoint monitor settings in Azure Traffic Manager

ANSWER:

Answer Area

To change the front end to an active/active architecture in which both regions process incoming connections, you must **[answer choice]**.

- add a load balancer to each region
- add an Azure Application Gateway to each region
- add an Azure content delivery network (CDN)
- modify the Azure Traffic Manager routing method

To control the threshold for failing over the front end to the standby region, you must configure the **[answer choice]**.

- Application Insights availability test
- Azure SQL Database failover groups
- Connection Monitor in Azure Network Watcher
- Endpoint monitor settings in Azure Traffic Manager

Explanation:

Box 1: Modify the Azure Traffic Manager routing

Azure Traffic Manager supports six traffic-routing methods to determine how to route network traffic to the various service endpoints.

Box 2: Endpoint monitor settings in the Azure Traffic Manager

Azure Traffic Manager includes built-in endpoint monitoring and automatic endpoint failover. This feature helps you deliver high-availability applications that are resilient to endpoint failure, including Azure region failures.

To configure endpoint monitoring, you must specify the following settings on your Traffic Manager profile: Protocol, Port, Path, custom header settings, etc.

Reference:

https://docs.microsoft.com/en-us/azure/traffic-manager/traffic-manager-routing-methods https://docs.microsoft.com/en-us/azure/traffic-manager/traffic-manager-monitoring

QUESTION NO: 192 - (HOTSPOT) - (Topic 5)

HOTSPOT

You have an Azure subscription named Subscription1 that is linked to a hybrid Azure Active Directory (Azure AD) tenant.

You have an on-premises datacenter that does NOT have a VPN connection to Subscription1. The datacenter contains a computer named Server1 that has Microsoft SQL Server 2016 installed. Server1 is prevented from accessing the internet.

An Azure logic app named LogicApp1 requires write access to a database on Server1.

You need to recommend a solution to provide LogicApp1 with the ability to access Server1.

What should you recommend deploying on-premises and in Azure? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

On-premises:

- A Web Application Proxy for Windows Server
- An Azure AD Application Proxy connector
- An On-premises data gateway
- Hybrid Connection Manager

Azure:

- A connection gateway resource
- An Azure Application Gateway
- An Azure Event Grid domain
- An enterprise application

ANSWER:

Answer Area

On-premises:

- A Web Application Proxy for Windows Server
- An Azure AD Application Proxy connector
- An On-premises data gateway
- Hybrid Connection Manager

Azure:

- A connection gateway resource
- An Azure Application Gateway
- An Azure Event Grid domain
- An enterprise application

Explanation:

Box 1: An on-premises data gateway

For logic apps in global, multi-tenant Azure that connect to on-premises SQL Server, you need to have the on-premises data gateway installed on a local computer and a data gateway resource that's already created in Azure.

Box 2: A connection gateway resource

Reference:

https://docs.microsoft.com/en-us/azure/connectors/connectors-create-api-sqlazure

QUESTION NO: 193 - (Topic 5)

You manage an application instance. The application consumes data from multiple databases. Application code references database tables using a combination of the server, database, and table name.

You need to migrate the application data to Azure.

To which two Azure services could you migrate the application to achieve the goal? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. SQL Managed Instance

B. Azure SQL Database

C. SQL Server in an Azure virtual machine

D. SQL Server Stretch Database

ANSWER: A D

Explanation:

A: The managed instance deployment model is designed for customers looking to migrate a large number of apps from on-premises or IaaS, self-built, or ISV provided environment to fully managed PaaS cloud environment, with as low migration effort as possible. Using the fully automated Data Migration Service (DMS) in Azure, customers can lift and shift their on-premises SQL Server to a managed instance that offers compatibility with SQL Server on-premises and complete isolation of customer instances with native VNet support.

D: Access your SQL Server data seamlessly regardless of whether it's on-premises or stretched to the cloud. You set the policy that determines where data is stored, and SQL Server handles the data movement in the background. The entire table is always online and queryable. And, Stretch Database doesn't require any changes to existing queries or applications - the location of the data is completely transparent to the application.

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

QUESTION NO: 194 - (Topic 5)

You manage an on-premises network and Azure virtual networks.

You need to create a secure connection over a private network between the on-premises network and the Azure virtual networks. The connection must offer a redundant pair of cross connections to provide high availability.

What should you recommend?

A. Azure Load Balancer

B. VPN Gateway

C. ExpressRoute

D. virtual network peering

ANSWER: B

Explanation:

Every Azure VPN gateway consists of two instances in an active-standby configuration. For any planned maintenance or unplanned disruption that happens to the active instance, the standby instance would take over (failover) automatically.

Reference:

https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-highlyavailable

QUESTION NO: 195 - (Topic 5)

You have an Azure subscription that contains an Azure Blob storage account named store1.

You have an on-premises file server named Server1 that runs Windows Server 2016. Server1 stores 500 GB of company files.

You need to store a copy of the company files from Server 1 in store1.

Which two possible Azure services achieve this goal? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. an integration account

B. an On-premises data gateway

C. an Azure Batch account

D. an Azure Import/Export job

E. Azure Data Factory

ANSWER: D E

QUESTION NO: 196 - (Topic 5)

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

ANSWER: A

DUMPSARENA