

Microsoft.VCEup.com.AZ-305.2022-July-07.84q

Number: AZ-305
Passing Score: 800
Time Limit: 120 min



Exam Code: AZ-305

Exam Name: Designing Microsoft Azure Infrastructure Solutions

Certification Provider: Microsoft

Corresponding Certification: Microsoft Certified: Azure Solutions Architect Expert

Website: <https://VCEup.com/>

Free Exam: <https://vceup.com/exam-az-305/>



Topic 1: Litware, Inc**QUESTION 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. General Overview

Litware, Inc. is a medium-sized finance company.

Overview. Physical Locations

Litware has a main office in Boston.

Existing Environment. Identity Environment

The network contains an Active Directory forest named Litware.com that is linked to an Azure Active Directory (Azure AD) tenant named Litware.com. All users have Azure Active Directory Premium P2 licenses.

Litware has a second Azure AD tenant named dev.Litware.com that is used as a development environment.

The Litware.com tenant has a conditional access policy named capolicy1. Capolicy1 requires that when users manage the Azure subscription for a production environment by using the Azure portal, they must connect from a hybrid Azure AD-joined device.

Existing Environment. Azure Environment

Litware has 10 Azure subscriptions that are linked to the Litware.com tenant and five Azure subscriptions that are linked to the dev.Litware.com tenant. All the subscriptions are in an Enterprise Agreement (EA).

The Litware.com tenant contains a custom Azure role-based access control (Azure RBAC) role named Role1 that grants the DataActions read permission to the blobs and files in Azure Storage.

Existing Environment. On-premises Environment

The on-premises network of Litware contains the resources shown in the following table.

Name	Type	Configuration
SERVER1 SERVER2 SERVER3	Ubuntu 18.04 virtual machines hosted on Hyper-V	The virtual machines host a third-party app named App1. App1 uses an external storage solution that provides Apache Hadoop-compatible data storage. The data storage supports POSIX access control list (ACL) file-level permissions.
SERVER10	Server that runs Windows Server 2016	The server contains a Microsoft SQL Server instance that hosts two databases named DB1 and DB2.

Existing Environment. Network Environment

Litware has ExpressRoute connectivity to Azure.

Planned Changes and Requirements. Planned Changes

Litware plans to implement the following changes:

Migrate DB1 and DB2 to Azure.

Migrate App1 to Azure virtual machines.

Deploy the Azure virtual machines that will host App1 to Azure dedicated hosts.

Planned Changes and Requirements. Authentication and Authorization Requirements Litware identifies the following authentication and authorization requirements:

Users that manage the production environment by using the Azure portal must connect from a hybrid Azure AD-joined device and authenticate by using Azure Multi-Factor Authentication (MFA).

The Network Contributor built-in RBAC role must be used to grant permission to all the virtual networks in all the Azure subscriptions.

To access the resources in Azure, App1 must use the managed identity of the virtual machines that will host the app.

Role1 must be used to assign permissions to the storage accounts of all the Azure subscriptions.

RBAC roles must be applied at the highest level possible.

Planned Changes and Requirements. Resiliency Requirements

Litware identifies the following resiliency requirements:

Once migrated to Azure, DB1 and DB2 must meet the following requirements:

- Maintain availability if two availability zones in the local Azure region fail.
- Fail over automatically.
- Minimize I/O latency.

App1 must meet the following requirements:

- Be hosted in an Azure region that supports availability zones.
- Be hosted on Azure virtual machines that support automatic scaling.
- Maintain availability if two availability zones in the local Azure region fail.

Planned Changes and Requirements. Security and Compliance Requirements Litware identifies the following security and compliance requirements:

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

On-premises users and services must be able to access the Azure Storage account that will host the data in App1.

Access to the public endpoint of the Azure Storage account that will host the App1 data must be prevented.
All Azure SQL databases in the production environment must have Transparent Data Encryption (TDE) enabled.
App1 must not share physical hardware with other workloads.
Planned Changes and Requirements. Business Requirements
Litware identifies the following business requirements:
Minimize administrative effort.
Minimize costs.

A.

Correct Answer:

Section: (none)

Explanation

Explanation/Reference:

QUESTION 2

You plan to migrate App1 to Azure.

You need to recommend a network connectivity solution for the Azure Storage account that will host the App1 data. The solution must meet the security and compliance requirements.
What should you include in the recommendation?

- A. a private endpoint
- B. a service endpoint that has a service endpoint policy
- C. Azure public peering for an ExpressRoute circuit
- D. Microsoft peering for an ExpressRoute circuit

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

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

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

<https://docs.microsoft.com/en-us/azure/expressroute/expressroute-faqs#microsoft-peering>

QUESTION 3

You plan to migrate App1 to Azure. The solution must meet the authentication and authorization requirements.

Which type of endpoint should App1 use to obtain an access token?

- A. Azure Instance Metadata Service (IMDS)
- B. Azure AD
- C. Azure Service Management
- D. Microsoft identity platform

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Scenario: To access the resources in Azure, App1 must use the managed identity of the virtual machines that will host the app.

Managed identities provide an identity for applications to use when connecting to resources that support Azure Active Directory (Azure AD) authentication. Applications may use the managed identity to obtain Azure AD tokens.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azureresources/overview>

QUESTION 4

You migrate App1 to Azure. You need to ensure that the data storage for App1 meets the security and compliance requirement What should you do?

- A. Create an access policy for the blob
- B. Modify the access level of the blob service.
- C. Implement Azure resource locks.
- D. Create Azure RBAC assignments.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

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

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

Reference:

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

QUESTION 5

You need to implement the Azure RBAC role assignments for the Network Contributor role. The solution must meet the authentication and authorization requirements.

What is the minimum number of assignments that you must use?

- A. 1
- B. 2
- C. 5
- D. 10
- E. 15

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Scenario: The Network Contributor built-in RBAC role must be used to grant permissions to the network administrators for all the virtual networks in all the Azure subscriptions.

RBAC roles must be applied at the highest level possible.

QUESTION 6

HOTSPOT

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

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

NOTE: Each correct selection is worth one point.

Hot Area:

To register the users for Azure MFA, use:

- Azure AD Identity Protection
- Security defaults in Azure AD
- Per-user MFA in the MFA management UI

To enforce Azure MFA authentication, configure:

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

Correct Answer:

To register the users for Azure MFA, use:

Azure AD Identity Protection
Security defaults in Azure AD
Per-user MFA in the MFA management UI

To enforce Azure MFA authentication, configure:

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

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Box 1: Azure AD Identity Protection

Azure AD Identity Protection helps you manage the roll-out of Azure AD Multi-Factor Authentication (MFA) registration by configuring a Conditional Access policy to require MFA registration no matter what modern authentication app you are signing in to.

Scenario: Users that manage the production environment by using the Azure portal must connect from a hybrid Azure AD-joined device and authenticate by using Azure Multi-Factor Authentication (MFA).

Box 2: Sign-in risk policy...

Scenario: The Litware.com tenant has a conditional access policy named capolicy1. Capolicy1 requires that when users manage the Azure subscription for a production environment by using the Azure portal, they must connect from a hybrid Azure AD-joined device.

Identity Protection policies we have two risk policies that we can enable in our directory.

Sign-in risk policy

User risk policy

Reference:

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

<https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identityprotection-configure-risk-policies>

QUESTION 7

DRAG DROP

You need to configure an Azure policy to ensure that the Azure SQL databases have TDE enabled. The solution must meet the security and compliance requirements.

Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place:

Actions	Answer Area
Create an Azure policy definition that uses the deployIfNotExists effect.	<div> <div>⬅️</div> <div>➡️</div> <div>⬅️</div> <div>➡️</div> </div>
Create a user-assigned managed identity.	
Invoke a remediation task.	
Create an Azure policy assignment.	
Create an Azure policy definition that uses the Modify effect.	

Correct Answer:

Actions	Answer Area
	Create an Azure policy definition that uses the deployIfNotExists effect.
Create a user-assigned managed identity.	Create an Azure policy assignment.
	Invoke a remediation task.
Create an Azure policy definition that uses the Modify effect.	

Section: (none)

Explanation

Explanation/Reference:

Scenario: All Azure SQL databases in the production environment must have Transparent Data Encryption (TDE) enabled.

Step 1: Create an Azure policy definition that uses the deployIfNotExists identity.

The first step is to define the roles that deployIfNotExists and modify needs in the policy definition to successfully deploy the content of your included template.

Step 2: Create an Azure policy assignment

When creating an assignment using the portal, Azure Policy both generates the managed identity and grants it the roles defined in roleDefinitionIds.

Step 3: Invoke a remediation task

Resources that are non-compliant to a deployIfNotExists or modify policy can be put into a compliant state through Remediation. Remediation is accomplished by instructing Azure Policy to run the deployIfNotExists effect or the modify operations of the assigned policy on your existing resources and subscriptions, whether that assignment is to a management group, a subscription, a resource group, or an individual resource.

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

Reference:

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

QUESTION 8

HOTSPOT

You plan to migrate App1 to Azure.

You need to recommend a high-availability solution for App1. The solution must meet the resiliency requirements.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Number of host groups:	<div><div></div><div>1</div><div>2</div><div>3</div><div>6</div></div>
Number of virtual machine scale sets:	<div><div></div><div>0</div><div>1</div><div>3</div></div>

Correct Answer:

Number of host groups:

Number of virtual machine scale sets:

Section: (none)

Explanation

Explanation/Reference:

Box 1: 3

Scenario: App1 must meet the following requirements:

Be hosted in an Azure region that supports availability zones.

Maintain availability if two availability zones in the local Azure region fail.

A host group is a resource that represents a collection of dedicated hosts. You create a host group in a region and an availability zone, and add hosts to it.

Use Availability Zones for fault isolation

Availability zones are unique physical locations within an Azure region. Each zone is made up of one or more datacenters equipped with independent power, cooling, and networking. A host group is created in a single availability zone. Once created, all hosts will be placed within that zone. To achieve high availability across zones, you need to create multiple host groups (one per zone) and spread your hosts accordingly.

Box 2: 1

Scenario: App1 must meet the following requirements:

Be hosted on Azure virtual machines that support automatic scaling.

An Azure virtual machine scale set can automatically increase or decrease the number of VM instances that run your application. This automated and elastic behavior reduces the management overhead to monitor and optimize the performance of your application.

Reference:

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

<https://docs.microsoft.com/en-us/azure/virtual-machine-scale-sets/virtual-machine-scale-setsautoscale-overview>

QUESTION 9

HOTSPOT

You plan to migrate App1 to Azure.

You need to estimate the compute costs for App1 in Azure. The solution must meet the security and compliance requirements.

What should you use to estimate the costs, and what should you implement to minimize the costs?

To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

To estimate the costs, use:

Implement:

Correct Answer:

To estimate the costs, use:

- Azure Advisor
- The Azure Cost Management Power BI app
- The Azure Total Cost of Ownership (TCO) calculator

Implement:

- Azure Reservations
- Azure Hybrid Benefit
- Azure Spot Virtual Machine pricing

Section: (none)

Explanation

Explanation/Reference:

Box 1: The Azure Total Cost of Ownership (TCO) Calculator

The Total Cost of Ownership (TCO) Calculator estimates the cost savings you can realize by migrating your workloads to Azure.

Note: The TCO Calculator recommends a set of equivalent services in Azure that will support your applications. Our analysis will show each cost area with an estimate of your on-premises spend versus your spend in Azure. There are several cost categories that either decrease or go away completely when you move workloads to the cloud.

Box 2: Azure Hybrid Benefit

Azure Hybrid Benefit is a licensing benefit that helps you to significantly reduce the costs of running your workloads in the cloud. It works by letting you use your on-premises Software Assurance-enabled Windows Server and SQL Server licenses on Azure. And now, this benefit applies to RedHat and SUSE Linux subscriptions, too.

Scenario:

Litware identifies the following security and compliance requirements:

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

On-premises users and services must be able to access the Azure Storage account that will host the data in App1.

Access to the public endpoint of the Azure Storage account that will host the App1 data must be prevented.

All Azure SQL databases in the production environment must have Transparent Data Encryption (TDE) enabled.

App1 must not share physical hardware with other workloads.

Reference:

<https://azure.microsoft.com/en-us/pricing/tco/>

<https://azure.microsoft.com/en-us/pricing/hybrid-benefit/>

QUESTION 10

HOTSPOT

You plan to migrate App1 to Azure.

You need to recommend a storage solution for App1 that meets the security and compliance requirements.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Hot Area:

Answer Area

Storage account type:

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

Configuration:

	▼
NFSv3	
Large file shares	
Hierarchical namespace	

Correct Answer:**Answer Area**

Storage account type:

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

Configuration:

	▼
NFSv3	
Large file shares	
Hierarchical namespace	

Section: (none)**Explanation****Explanation/Reference:**

Explanation:

Box 1: Standard general-purpose v2

Standard general-purpose v2 supports Blob Storage.

Azure Storage provides data protection for Blob Storage and Azure Data Lake Storage Gen2.

Scenario:

Litware identifies the following security and compliance requirements:

Once App1 is migrated to Azure, you must ensure that new data can be written to the app, and the modification of new and existing data is prevented for a period of three years. On-premises users and services must be able to access the Azure Storage account that will host the data in App1.

Access to the public endpoint of the Azure Storage account that will host the App1 data must be prevented.

All Azure SQL databases in the production environment must have Transparent Data Encryption (TDE) enabled. App1 must NOT share physical hardware with other workloads.

Box 2: NFSv3

Scenario: Plan: Migrate App1 to Azure virtual machines.

Blob storage now supports the Network File System (NFS) 3.0 protocol. This support provides Linux file system compatibility at object storage scale and prices and enables Linux clients to mount a container in Blob storage from an Azure Virtual Machine (VM) or a computer on-premises.

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

QUESTION 11**HOTSPOT**

How should the migrated databases DB1 and DB2 be implemented in Azure?

Hot Area:

Answer Area

Database:

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

Service tier:

Hyperscale
Business Critical
General Purpose

Correct Answer:

Answer Area

Database:

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

Service tier:

Hyperscale
Business Critical
General Purpose

Section: (none)

Explanation

Explanation/Reference:

Box 1: SQL Managed Instance

Scenario: Once migrated to Azure, DB1 and DB2 must meet the following requirements:

Maintain availability if two availability zones in the local Azure region fail. Fail over automatically. Minimize I/O latency.

The auto-failover groups feature allows you to manage the replication and failover of a group of databases on a server or all databases in a managed instance to another region. It is a declarative abstraction on top of the existing active georeplication feature, designed to simplify deployment and management of geo-replicated databases at scale. You can initiate a geo-failover manually or you can delegate it to the Azure service based on a user-defined policy. The latter option allows you to automatically recover multiple related databases in a secondary region after a catastrophic failure or other unplanned event that results in full or partial loss of the SQL Database or SQL Managed Instance availability in

the primary region.

Box 2: Business critical

SQL Managed Instance is available in two service tiers:

General purpose: Designed for applications with typical performance and I/O latency requirements.

Business critical: Designed for applications with low I/O latency requirements and minimal impact of underlying maintenance operations on the workload.

Reference: <https://docs.microsoft.com/en-us/azure/azure-sql/database/auto-failover-group-overview>

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

QUESTION 12

HOTSPOT

You plan to migrate DB1 and DB2 to Azure.

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

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Database:

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

Service tier:

Hyperscale
Business Critical
General Purpose

Correct Answer:

Answer Area

Database:

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

Service tier:

Hyperscale
Business Critical
General Purpose

Section: (none)

Explanation

Explanation/Reference:

Topic 2: Fabrikam, inc Case Study A**QUESTION 1**

Overview:

Existing Environment

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.

Active Directory Environment:

The network contains two Active Directory forests named corp.fabnkam.com and rd.fabrikam.com.

There are no trust relationships between the forests. Corp.fabrikam.com is a production forest that contains identities used for internal user and computer authentication. Rd.fabrikam.com is used by the research and development (R&D) department only. The R&D department is restricted to using on-premises resources only.

Network Infrastructure:

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

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

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

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

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

Problem Statement:

The use of Web App1 is unpredictable. At peak times, users often report delays. At other times, many resources for WebApp1 are underutilized.

Requirements:

Planned Changes:

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

As one of its first projects, the company plans to establish a hybrid identity model, facilitating an upcoming Microsoft Office 365 deployment All R&D operations will remain on-premises.

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

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 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 platform as a service (PaaS).
- 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.fabhkam.com must not be affected by a link failure between Azure and the on premises network.

Database Requirements:

Fabrikam identifies the following database requirements:

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

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.

A.

Correct Answer:

Section: (none)

Explanation

Explanation/Reference:

QUESTION 2

You need to recommend a data storage strategy for WebApp1.

What should you include in in the recommendation?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3

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. Use SQL Server transactional replication.
- C. Copy the BACPAC file that contains the Azure SQL database file to Azure Blob storage.
- D. Copy the VHD that contains the Azure SQL database files to Azure Blob storage

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

Explanation:
Before you upload a Windows virtual machine (VM) from on-premises to Azure, you must prepare the virtual hard disk (VHD or VHDX).
Scenario: WebApp1 has a web tier that uses Microsoft Internet Information Services (IIS) and a database tier that runs Microsoft SQL Server 2016. The web tier and the database tier are deployed to virtual machines that run on Hyper-V.
Reference:
<https://docs.microsoft.com/en-us/azure/virtual-machines/windows/prepare-for-upload-vhd-image>

QUESTION 4

You need to recommend a strategy for the web tier of WebApp1. The solution must minimize What should you recommend?

- A. Create a runbook that resizes virtual machines automatically to a smaller size outside of business hours.
- B. Configure the Scale Up settings for a web app.
- C. Deploy a virtual machine scale set that scales out on a 75 percent CPU threshold.
- D. Configure the Scale Out settings for a web app.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5

You need to recommend a solution to meet the database retention requirement. What should you recommend?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

Explanation:
<https://docs.microsoft.com/en-us/azure/azure-sql/database/long-term-retention-overview>In Azure SQL Database, you can configure a database with a long-term backup retention policy (LTR)to automatically retain the database backups in separate Azure Blob storage containers for up to 10years

QUESTION 6

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

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

QUESTION 7

You need to recommend a notification solution for the IT Support distribution group.

What should you include in the recommendation?

- A. Azure Network Watcher
- B. an action group
- C. a SendGrid account with advanced reporting
- D. Azure AD Connect Health

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Reference:

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

QUESTION 8

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:

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

Correct Answer:

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

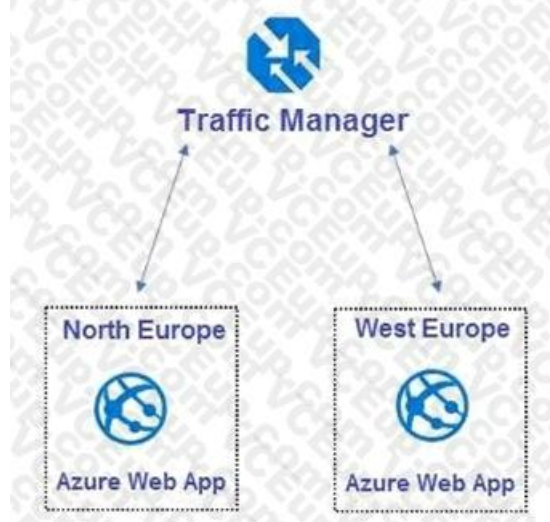
Section: (none)
Explanation

Explanation/Reference:
1
1
0

QUESTION 9

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.

Hot Area:

Statements	Yes	No
The design supports the technical requirements for redundancy.	<input type="radio"/>	<input type="radio"/>
The design supports autoscaling.	<input type="radio"/>	<input type="radio"/>
The design requires a manual configuration if an Azure region fails.	<input type="radio"/>	<input type="radio"/>

Correct Answer:

Statements	Yes	No
The design supports the technical requirements for redundancy.	<input checked="" type="radio"/>	<input type="radio"/>
The design supports autoscaling.	<input checked="" type="radio"/>	<input type="radio"/>
The design requires a manual configuration if an Azure region fails.	<input type="radio"/>	<input checked="" type="radio"/>

Section: (none)**Explanation****Explanation/Reference:**

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/>

QUESTION 10**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:

Statements	Yes	No
You must provision an Azure Storage account for the SQL Server database migration.	<input type="checkbox"/>	<input type="checkbox"/>
You must provision an Azure Storage account for the Web site content storage.	<input type="checkbox"/>	<input type="checkbox"/>
You must provision an Azure Storage account for the Database metric monitoring.	<input type="checkbox"/>	<input type="checkbox"/>

Correct Answer:

Statements	Yes	No
You must provision an Azure Storage account for the SQL Server database migration.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
You must provision an Azure Storage account for the Web site content storage.	<input type="checkbox"/>	<input checked="" type="checkbox"/>
You must provision an Azure Storage account for the Database metric monitoring.	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Section: (none)
Explanation

Explanation/Reference:

Topic 3: Contoso**QUESTION 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.

Existing Environment: Technical Environment

The on-premises network contains a single Active Directory domain named contoso.com.

Contoso has a single Azure subscription.

Existing Environment: Business Partnerships

Contoso has a business partnership with Fabrikam, Inc. Fabrikam users access some Contoso applications over the internet by using Azure Active Directory (Azure AD) guest accounts.

Requirements: Planned Changes

Contoso plans to deploy two applications named App1 and App2 to Azure.

Requirements: App1

App1 will be a Python web app hosted in Azure App Service that requires a Linux runtime. Users from

Contoso and Fabrikam will access App1.

App1 will access several services that require third-party credentials and access strings. The credentials and access strings are stored in Azure Key Vault.

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

App1 has the following data requirements:

Each instance will write data to a data store in the same availability zone as the instance.

Data written by any App1 instance must be visible to all App1 instances.

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

Connections to App1 must pass through a web application firewall (WAF).

Connections to App1 must be active-active load balanced between instances.

All connections to App1 from North America must be directed to the East US region. All other connections must be directed to the West Europe region.

Every hour, you will run a maintenance task by invoking a PowerShell script that copies files from all the App1 instances. The PowerShell script will run from a central location.

Requirements: App2

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

Save files to an Azure Storage account.

Replicate files to an on-premises location.

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

You need to monitor App2 to analyze how long it takes to perform different transactions within the application. The solution must not require changes to the application code.

Application Development Requirements

Application developers will constantly develop new versions of App1 and App2. The development process must meet the following requirements:

A staging instance of a new application version must be deployed to the application host before the new version is used in production.

After testing the new version, the staging version of the application will replace the production version.

The switch to the new application version from staging to production must occur without any downtime of the application.

Identity Requirements

Contoso identifies the following requirements for managing Fabrikam access to resources:

Every month, an account manager at Fabrikam must review which Fabrikam users have access permissions to App1. Accounts that no longer need permissions must be removed as guests.

The solution must minimize development effort.

Security Requirement

All secrets used by Azure services must be stored in Azure Key Vault.

Services that require credentials must have the credentials tied to the service instance. The credentials must NOT be shared between services.

A.

Correct Answer:

Section: (none)

Explanation

Explanation/Reference:

QUESTION 2

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

- A. one App Service Environment (ASE) per availability zone
- B. one App Service plan per availability zone
- C. one App Service plan per region
- D. one App Service Environment (ASE) per region

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 3

You need to recommend a solution that meets the data requirements for App1.

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

- A. an Azure Cosmos DB that uses multi-region writes
- B. an Azure Storage account that uses geo-zone-redundant storage (GZRS)
- C. an Azure Data Lake store that uses geo-zone-redundant storage (GZRS)
- D. an Azure SQL database that uses active geo-replication

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 4

HOTSPOT

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Service:

<input type="checkbox"/>	Azure AD Identity Governance
<input type="checkbox"/>	Azure AD Identity Protection
<input type="checkbox"/>	Azure AD Privilege Access Management (PIM)
<input type="checkbox"/>	Azure Automation

Feature:

<input type="checkbox"/>	Access packages
<input type="checkbox"/>	Access reviews
<input type="checkbox"/>	Approvals
<input type="checkbox"/>	Runbooks

Correct Answer:

Answer Area

Service:

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

Feature:

Access packages
Access reviews
Approvals
Runbooks

Section: (none)

Explanation

Explanation/Reference:

Requirements: Identity Requirements

Contoso identifies the following requirements for managing Fabrikam access to resources:

Every month, an account manager at Fabrikam must review which Fabrikam users have access permissions to App1.

Accounts that no longer need permissions must be removed as guests. The solution must minimize development effort.

Box 1: The Azure AD Privileged Identity Management (PIM) When should you use access reviews?

Too many users in privileged roles: It's a good idea to check how many users have administrative access, how many of them are Global Administrators, and if there are any invited guests or partners that have not been removed after being assigned to do an administrative task. You can recertify the role assignment users in Azure AD roles such as Global Administrators, or Azure resources roles such as User Access Administrator in the Azure AD Privileged Identity Management (PIM) experience.

Box 2: Access reviews

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

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

QUESTION 5

DRAG DROP

You need to recommend a solution that meets the file storage requirements for App2.

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

NOTE: Each correct selection is worth one point.

Select and Place:

Select and Place:

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

Correct Answer:

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

Section: (none)
Explanation

Explanation/Reference:

Box 1: Azure Files

Scenario: App2 has the following file storage requirements:

Save files to an Azure Storage account.

Replicate files to an on-premises location.

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

Box 2: Azure File Sync

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

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

QUESTION 6

You need to recommend a solution that meets the data requirements for App1.

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

A. an Azure Cosmos DB that uses multi-region writes

- B. an Azure Data Lake store that uses geo-zone-redundant storage (GZRS)
- C. an Azure SQL database that uses active geo-replication
- D. an Azure Storage account that uses geo-zone-redundant storage (GZRS)

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Scenario: App1 has the following data requirements:

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

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

Incorrect Answers:

B, D: GZRS protects against failures. Geo-redundant storage (with GRS or GZRS) replicates your data to another physical location in the secondary region to protect against regional outages. However, that data is available to be read only if the customer or Microsoft initiates a failover from the primary to secondary region.

C: Active geo-replication is designed as a business continuity solution that lets you perform quick disaster recovery of individual databases in case of a regional disaster or a large scale outage. Once georeplication is set up, you can initiate a geo-failover to a geo-secondary in a different Azure region. The geo-failover is initiated programmatically by the application or manually by the user.

Reference:

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

QUESTION 7

HOTSPOT

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

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Authenticate App1 by using:

<input type="checkbox"/> A certificate
<input type="checkbox"/> A service principal
<input type="checkbox"/> A system-assigned managed identity
<input type="checkbox"/> A user-assigned managed identity

Authorize App1 to retrieve Key Vault secrets by using:

<input type="checkbox"/> An access policy
<input type="checkbox"/> A connected service
<input type="checkbox"/> A private link
<input type="checkbox"/> A role assignment

Correct Answer:

Answer Area

Authenticate App1 by using:

<input type="radio"/>	A certificate
<input checked="" type="radio"/>	A service principal
<input type="radio"/>	A system-assigned managed identity
<input type="radio"/>	A user-assigned managed identity

Authorize App1 to retrieve Key Vault secrets by using:

<input type="radio"/>	An access policy
<input type="radio"/>	A connected service
<input type="radio"/>	A private link
<input checked="" type="radio"/>	A role assignment

Section: (none)

Explanation

Explanation/Reference:

Scenario: Security Requirement

All secrets used by Azure services must be stored in Azure Key Vault.

Services that require credentials must have the credentials tied to the service instance. The credentials must NOT be shared between services.

Box 1: A service principal

A service principal is a type of security principal that identifies an application or service, which is to say, a piece of code rather than a user or group. A service principal's object ID is known as its client ID and acts like its username. The service principal's client secret acts like its password.

Note: Authentication with Key Vault works in conjunction with Azure Active Directory (Azure AD), which is responsible for authenticating the identity of any given security principal.

A security principal is an object that represents a user, group, service, or application that's requesting access to Azure resources. Azure assigns a unique object ID to every security principal.

Box 2: A role assignment

You can provide access to Key Vault keys, certificates, and secrets with an Azure role-based access control.

Reference:

<https://docs.microsoft.com/en-us/azure/key-vault/general/authentication>

QUESTION 8

HOTSPOT

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

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Azure Traffic Manager:

<input type="radio"/>	1
<input type="radio"/>	2
<input type="radio"/>	3
<input checked="" type="radio"/>	6

Azure Application Gateway:

<input type="radio"/>	1
<input type="radio"/>	2
<input type="radio"/>	3
<input checked="" type="radio"/>	6

Correct Answer:



Section: (none)
Explanation

Explanation/Reference:

Topic 4: Mix Questions**QUESTION 1**

You have an Azure subscription that contains a custom application named Application1. The application was developed by an external company named Fabric, 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 Fabric 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 access permission, automatically revoke that permission.

* Minimize development effort.

What should you recommend?

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

<https://docs.microsoft.com/en-us/azure/active-directory/governance/manage-user-access-with-access-reviews> Azure Active Directory (Azure AD) access reviews enable organizations to efficiently manage group memberships, access to enterprise applications, and role assignments. User's access can be reviewed on a regular basis to make sure only the right people have continued access. Have reviews recur periodically: You can set up recurring access reviews of users at set frequencies such as weekly, monthly, quarterly or annually, and the reviewers will be notified at the start of each review.

Reviewers can approve or deny access with a friendly interface and with the help of smart recommendations.

Why are access reviews important?

"Azure AD enables you to collaborate with users from inside your organization and with external users. Users can join groups, invite guests, connect to cloud apps, and work remotely from their work or personal devices. The convenience of using self-service has led to a need for better access management capabilities."

QUESTION 2

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Reference:

<https://docs.microsoft.com/en-us/azure/storage/common/storage-sas-overview> This allows for limited-time fine grained access control to resources. So you can generate URL, specify duration (for month of April) and disseminate URL to 10 team members. On May 1, the SAS token is automatically invalidated, denying team members continued access.

QUESTION 3

You have an Azure Active Directory (Azure AD) tenant that syncs with an on-premises Active Directory domain.

You have an internal web app named WebApp1 that is hosted on-premises. WebApp1 uses Integrated Windows authentication.

Some users work remotely and do NOT have VPN access to the on-premises network.

You need to provide the remote users with single sign-on (SSO) access to WebApp1.

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 AD Application Proxy
- B. Azure AD Privileged Identity Management (PIM)
- C. Conditional Access policies

- D. Azure Arc
- E. Azure AD enterprise applications
- F. Azure Application Gateway

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

Explanation:

A: 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.

You can configure single sign-on to an Application Proxy application.

C: Microsoft recommends using Application Proxy with pre-authentication and Conditional Access policies for remote access from the internet. An approach to provide Conditional Access for intranet use is to modernize applications so they can directly authenticate with AAD.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy-config-ssohow-to>

<https://docs.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy-deploymentplan>

QUESTION 4

You have an Azure Active Directory (Azure AD) tenant named contoso.com that has a security group named Group1. Group1 is configured with 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. Implement Azure Multi-Factor Authentication.
- B. Change the Membership type of Group1 to Dynamic User.
- C. Implement Azure AD Privileged Identity Management.
- D. Create an access review.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

<https://docs.microsoft.com/en-us/azure/active-directory/governance/access-reviews-overview#learn-about-access-reviews> Have reviews recur periodically: You can set up recurring access reviews of users at set frequencies such as weekly, monthly, quarterly or annually, and the reviewers will be notified at the start of each review. Reviewers can approve or deny access with a friendly interface and with the help of smart recommendations.

An administrator creates an access review of Group C with 50 member users and 25 guest users.

Makes it a self-review. 50 licenses for each user as self-reviewers.* <https://docs.microsoft.com/en-us/azure/active-directory/governance/access-reviews-overview#example-license-scenarios> There are 4 requirements and every single one is only met by access reviews.

<https://docs.microsoft.com/en-us/azure/active-directory/governance/access-reviews-overview#when-should-you-use-access-reviews> Dynamic User is needed if a user must be automatically granted access on the basis of its attributes

(department, job title, location, etc.) <https://techcommunity.microsoft.com/t5/itops-talkblog/dynamic-groups-in-azure-ad-and-microsoft-365/ba-p/2267494> Implementing Azure AD PIM is no solution and absolutely not necessary for access reviews.

<https://docs.microsoft.com/en-us/azure/active-directory/governance/access-reviews-overview#where-do-you-create-reviews>

QUESTION 5

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

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

Your company deploys several virtual machines on-premises and to Azure. ExpressRoute is being deployed and configured for on-premises to Azure connectivity.

Several virtual machines exhibit network connectivity issues.

You need to analyze the network traffic to identify whether packets are being allowed or denied to the virtual machines.

Solution: Use Azure Traffic Analytics in Azure Network Watcher to analyze the network traffic.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Instead use Azure Network Watcher IP Flow Verify, which allows you to detect traffic filtering issues at a VM level.

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.

Reference:

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

<https://docs.microsoft.com/en-us/azure/network-watcher/traffic-analytics>

QUESTION 6

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

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

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

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 7

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

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

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 8

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

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

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

NOTE: Each correct selection is worth one point.

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

Correct Answer: ABD

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Azure Policy evaluates resources in Azure by comparing the properties of those resources to business rules.

Once your business rules have been formed, the policy definition or initiative is assigned to any scope of resources that Azure supports, such as management groups, subscriptions, resource groups, or individual resources.

Reference:

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

QUESTION 9

You need to recommend a solution to generate a monthly report of all the new Azure Resource Manager resource deployment in your subscription. What should you include in the recommendation?

- A. Azure Activity Log
- B. Azure Monitor action groups
- C. Azure Advisor
- D. Azure Monitor metrics

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

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

Through activity logs, you can determine: what operations were taken on the resources in your subscription who started the operation when the operation occurred the status of the operation the values of other properties that might help you research the operation

Reference:

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

<https://docs.microsoft.com/en-us/azure/automation/change-tracking>

QUESTION 10

You have 100 servers that run Windows Server 2012 R2 and host Microsoft SQL Server 2012 R2 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 single databases
- B. Azure SQL Database Managed Instance
- C. Azure SQL Database elastic pools
- D. SQL Server 2016 on Azure virtual machines

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Reference:
<https://docs.microsoft.com/en-us/azure/sql-database/sql-database-managed-instance> SQL Managed Instance allows existing SQL Server customers to lift and shift their on-premises applications to the cloud with minimal application and database changes. At the same time, SQL Managed Instance preserves all PaaS capabilities (automatic patching and version updates, automated backups, high availability) that drastically reduce management overhead and TCO.
<https://docs.microsoft.com/en-us/azure/azure-sql/managed-instance/transact-sql-tsql-differences#sql-server#clr>
<https://docs.microsoft.com/en-gb/azure/azure-sql/database/transact-sql-tsql-differences-sqlserver#transact-sql-syntax-not-supported-in-azure-sql-database>

QUESTION 11

You have an Azure subscription that contains an Azure Blob storage account named store1.
You have an on-premises file server named Setver1 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 Azure Batch account
- B. an integration account
- C. an On-premises data gateway
- D. an Azure Import/Export job
- E. Azure Data factory

Correct Answer: DE

Section: (none)

Explanation

Explanation/Reference:

Explanation:
<https://docs.microsoft.com/en-us/azure/storage/common/storage-import-export-data-from-blobs>
<https://docs.microsoft.com/en-us/answers/questions/311113/fastest-method-to-copy-500gb-tablefrom-on-premise.html>

QUESTION 12

You have an Azure subscription that contains two applications named App1 and App2. App1 is a sales processing application. When a transaction in App1 requires shipping, a message is added to an Azure Storage account queue, and then App2 listens to the queue for relevant transactions.
In the future, additional applications will be added that will process some of the shipping requests based on the specific details of the transactions.
You need to recommend a replacement for the storage account queue to ensure that each additional application will be able to read the relevant transactions.
What should you recommend?

- A. one Azure Service Bus queue
- B. one Azure Service Bus topic
- C. one Azure Data Factory pipeline
- D. multiple storage account queues

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

A queue allows processing of a message by a single consumer. In contrast to queues, topics and subscriptions provide a one-to-many form of communication in a publish and subscribe pattern. It's useful for scaling to large numbers of recipients. Each published message is made available to each subscription registered with the topic. Publisher sends a message to a topic and one or more subscribers receive a copy of the message, depending on filter rules set on these subscriptions.

Reference:

<https://docs.microsoft.com/en-us/azure/service-bus-messaging/service-bus-queues-topicssubscriptions>

QUESTION 13

The application will host video files that range from 50 MB to 12 GB. The application will use certificate-based authentication and will be available to users on the internet.

You need to recommend a storage option for the video files. The solution must provide the fastest read performance and must minimize storage costs.

What should you recommend?

- A. Azure Files
- B. Azure Data Lake Storage Gen2
- C. Azure Blob Storage
- D. Azure SQL Database

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Blob Storage: Stores large amounts of unstructured data, such as text or binary data, that can be accessed from anywhere in the world via HTTP or HTTPS. You can use Blob storage to expose data publicly to the world, or to store application data privately.

Max file in Blob Storage. 4.77 TB.

Reference:

<https://docs.microsoft.com/en-us/azure/architecture/solution-ideas/articles/digital-media-video>

QUESTION 14

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

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

Guaranteed 99.995 percent uptime for SQL Database

Reference:

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

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

<https://www.azure.cn/en-us/support/sla/virtual-machines/>

<https://techcommunity.microsoft.com/t5/azure-sql/optimize-price-performance-with-computeauto-scaling-in-azure/ba-p/966149>

QUESTION 15

You are planning an Azure IoT Hub solution that will include 50,000 IoT devices.

Each device will stream data, including temperature, device ID, and time data. Approximately 50,000 records will be written every second. The data will be visualized in near real time.

You need to recommend a service to store and query the data.
Which two services can you recommend? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

- A. Azure Table Storage
- B. Azure Event Grid
- C. Azure Cosmos DB SQL API
- D. Azure Time Series Insights

Correct Answer: CD

Section: (none)

Explanation

Explanation/Reference:

Explanation:

D: Time Series Insights is a fully managed service for time series data. In this architecture, Time Series Insights performs the roles of stream processing, data store, and analytics and reporting. It accepts streaming data from either IoT Hub or Event Hubs and stores, processes, analyzes, and displays the data in near real time.

C: The processed data is stored in an analytical data store, such as Azure Data Explorer, HBase, Azure Cosmos DB, Azure Data Lake, or Blob Storage.

Reference:

<https://docs.microsoft.com/en-us/azure/architecture/data-guide/scenarios/time-series>

QUESTION 16

You are designing an application that will aggregate content for users.

You need to recommend a database solution for the application. The solution must meet the following requirements:

Support SQL commands.

Support multi-master writes.

Guarantee low latency read operations.

What should you include in the recommendation?

- A. Azure Cosmos DB SQL API
- B. Azure SQL Database that uses active geo-replication
- C. Azure SQL Database Hyperscale
- D. Azure Database for PostgreSQL

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

With Cosmos DB's novel multi-region (multi-master) writes replication protocol, every region supports both writes and reads. The multi-region writes capability also enables:

Unlimited elastic write and read scalability.

99.999% read and write availability all around the world.

Guaranteed reads and writes served in less than 10 milliseconds at the 99th percentile.

Reference:

<https://docs.microsoft.com/en-us/azure/cosmos-db/distribute-data-globally>

QUESTION 17

You have SQL Server on an Azure virtual machine. The databases are written to nightly as part of a batch process.

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

Provide the ability to recover in the event of a regional outage.

Support a recovery time objective (RTO) of 15 minutes.

Support a recovery point objective (RPO) of 24 hours.

Support automated recovery.

Minimize costs.

What should you include in the recommendation?

- A. Azure virtual machine availability sets
- B. Azure Disk Backup
- C. an Always On availability group

D. Azure Site Recovery

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Replication with Azure Site Recover:

RTO is typically less than 15 minutes.

RPO: One hour for application consistency and five minutes for crash consistency.

Reference:

<https://docs.microsoft.com/en-us/azure/site-recovery/site-recovery-sql>

QUESTION 18

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Azure Traffic Manager is a DNS-based traffic load balancer that enables you to distribute traffic optimally to services across global Azure regions, while providing high availability and responsiveness.

<https://docs.microsoft.com/en-us/azure/traffic-manager/traffic-manager-overview>

QUESTION 19

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 an Azure virtual machine to two Azure regions, and you deploy an Azure Application Gateway.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

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

QUESTION 20

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 Azure virtual machine scale set that uses autoscaling.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

Explanation:

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

QUESTION 21

You plan to move a web application named App1 from an on-premises data center to Azure.

App1 depends on a custom COM component that is installed on the host server.

You need to recommend a solution to host App1 in Azure. The solution must meet the following requirements:

App1 must be available to users if an Azure data center becomes unavailable.

Costs must be minimized.

What should you include in the recommendation?

- A. In two Azure regions, deploy a load balancer and a virtual machine scale set.
- B. In two Azure regions, deploy a Traffic Manager profile and a web app.
- C. In two Azure regions, deploy a load balancer and a web app.
- D. Deploy a load balancer and a virtual machine scale set across two availability zones.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

Explanation:

(<https://docs.microsoft.com/en-us/dotnet/azure/migration/app-service#com-and-com-components>) Azure App Service does not allow the registration of COM components on the platform. If your app makes use of any COM components, these need to be rewritten in managed code and deployed with the site or application. <https://docs.microsoft.com/en-us/dotnet/azure/migration/app-service> "Azure App Service with Windows Containers If your app cannot be migrated directly to App Service, consider App Service using Windows Containers, which enables usage of the GAC, COM components, MSIs, full access to .NET FX APIs, DirectX, and more."

QUESTION 22

You have an Azure subscription that contains a Basic Azure virtual WAN named Virtual/WAN1 and the virtual hubs shown in the following table.

Name	Azure region
Hub1	US East
Hub2	US West

You have an ExpressRoute circuit in the US East region.

You need to create an ExpressRoute association to VirtualWAN1.

What should you do first?

- A. Upgrade VirtualWAN1 to Standard.
- B. Create a gateway on Hub1.
- C. Create a hub virtual network in US East.
- D. Enable the ExpressRoute premium add-on.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

Explanation:

US East and US West are in the same geopolitical region so there is no need for enabling ExpressRoute premium add-on <https://docs.microsoft.com/en-us/azure/virtual-wan/virtual-wan-about#basicstandard> The current config of virtual WAN is only Basic as given, so it can connect to only site to site VPN, to connect to express route it needs to be upgraded from basic to standard.

<https://docs.microsoft.com/en-us/azure/virtual-wan/virtual-wan-about>

<https://docs.microsoft.com/en-us/azure/virtual-wan/virtual-wan-about>

QUESTION 23

You have an Azure subscription that contains a storage account.

An application sometimes writes duplicate files to the storage account.

You have a PowerShell script that identifies and deletes duplicate files in the storage account.

Currently, the script is run manually after approval from the operations manager.

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

Runs the script once an hour to identify whether duplicate files exist
Sends an email notification to the operations manager requesting approval to delete the duplicate files
Processes an email response from the operations manager specifying whether the deletion was approved
Runs the script if the deletion was approved
What should you include in the recommendation?

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

You can schedule a powershell script with Azure Logic Apps.

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

Reference:

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

QUESTION 24

Your company has the infrastructure shown in the following table.

Location	Resource
Azure	<ul style="list-style-type: none">• Azure subscription named Subscription1• 20 Azure web apps
On-premises datacenter	<ul style="list-style-type: none">• 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 Appl that uses LDAP queries to verify user identities in the onpremises 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 Appl continues to function after the migration. The solution must meet the security policy.

What should you include in the recommendation?

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

<https://docs.microsoft.com/en-us/azure/active-directory-domain-services/overview> Azure Active Directory Domain Services (Azure AD DS) provides managed domain services such as domain join, group policy, lightweight directory access protocol (LDAP), and Kerberos/NTLM authentication. Azure AD Domain Services (Azure AD DS) - This one could work since AAD DS will bring in the existing accounts from Azure AD which in turn are synchronised from on-premise AD over AD connect.

However, you would probably need to reconfigure the app and update the LDAP connection. Azure Active Directory (Azure AD) supports LDAP Authentication via Azure AD Domain Services (AD DS). <https://docs.microsoft.com/en-us/azure/>

active-directory/fundamentals/auth-ldap
<https://docs.microsoft.com/en-us/azure/active-directory-domain-services/synchronization>

QUESTION 25

You need to design a solution that will execute custom C# code in response to an event routed to Azure Event Grid. The solution must meet the following requirements:
The executed code must be able to access the private IP address of a Microsoft SQL Server instance that runs on an Azure virtual machine.
Costs must be minimized.
What should you include in the solution?

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

When you create a function app in Azure, you must choose a hosting plan for your app. There are three basic hosting plans available for Azure Functions: Consumption plan, Premium plan, and Dedicated (App Service) plan.

For the Consumption plan, you don't have to pay for idle VMs or reserve capacity in advance.

Connect to private endpoints with Azure Functions

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

Reference:

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

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

Reference:

<https://docs.microsoft.com/en-us/azure/azure-functions/functions-scale#hosting-plans-comparison>

QUESTION 26

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 shares files as quickly as possible if the Toronto branch office is inaccessible.
What should you include in the recommendation?

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Use Azure File Sync to centralize your organization's file shares in Azure Files, while keeping the flexibility, performance, and compatibility of an on-premises file server. Azure File Sync transforms Windows Server into a quick cache of your Azure file share.

You need an Azure file share in the same region that you want to deploy Azure File Sync.

Reference:

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

QUESTION 27

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

One option is to deploy APIM (API Management) inside the cluster VNet.

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

Reference:

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

QUESTION 28

You have .Net web service named service1 that has the following requirements.

Must read and write to the local file system.

Must write to the Windows 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 Azure App Service web app
- B. an Azure virtual machine scale set
- C. an App Service Environment (ASE)
- D. an Azure Functions app

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

<https://social.msdn.microsoft.com/Forums/vstudio/en-US/294b9e3e-e89c-4095-b8d0-ee1646e77268/writing-to-local-file-system-from-web-app-inazure?forum=windowsazurewebsitespreview>

QUESTION 29

You have the Azure resources shown in the following table.

Name	Type	Location
US-Central-Firewall-policy	Azure Firewall policy	Central US
US-East-Firewall-policy	Azure Firewall policy	East US
EU-Firewall-policy	Azure Firewall policy	West Europe
USEastfirewall	Azure Firewall	Central US
USWestfirewall	Azure Firewall	East US
EUFirewall	Azure Firewall	West Europe

You need to deploy a new Azure Firewall policy that will contain mandatory rules for all Azure Firewall deployments. The new policy will be configured as a parent policy for the existing policies.

What is the minimum number of additional Azure Firewall policies you should create?

- A. 0
- B. 1

- C. 2
- D. 3

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Firewall policies work across regions and subscriptions.

Place all your global configurations in the parent policy.

Note: Policies can be created in a hierarchy. You can create a parent/global policy that will contain configurations and rules that will apply to all/a number of firewall instances. Then you create a child policy that inherits from the parent; note that rules changes in the parent instantly appear in the child. The child is associated with a firewall and applies configurations/rules from the parent policy and the child policy instantly to the firewall.

Reference:

<https://aidanfinn.com/?p=22006>

QUESTION 30

Your company has an app named App1 that uses data from the on-premises Microsoft SQL Server databases shown in the following table.

Name	Size
DB1	450 GB
DB2	250 GB
DB3	300 GB
DB4	50 GB

App1 and the data are used on the first day of the month only. The data is not expected to grow more than 3% each year.

The company is rewriting App1 as an Azure web app and plans to migrate all the data to Azure.

You need to migrate the data to Azure SQL Database. The solution must minimize costs.

Which service tier should you use?

- A. vCore-based Business Critical
- B. vCore-based General Purpose
- C. DTU-based Standard
- D. DTU-based Basic

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

DTU-based Standard supports databases up to 1 TB in size.

Reference:

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

QUESTION 31

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

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

What should you include in the recommendation?

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

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

Reference:

<https://docs.microsoft.com/en-us/azure/service-bus-messaging/service-bus-transactions>" Service Bus offers a reliable and secure platform for asynchronous transfer of data and state." ...

"Service Bus supports standard AMQP 1.0 and HTTP/REST protocols." <https://docs.microsoft.com/enus/azure/service-bus-messaging/service-bus-messaging-overview>

QUESTION 32

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 Cost Management
- B. Azure Pricing calculator
- C. Azure Migrate
- D. Azure Advisor

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

<https://docs.microsoft.com/en-us/azure/migrate/migrate-appliance#collected-data---vmware>"Metadata discovered by the Azure Migrate appliance helps you to figure out whether servers are ready for migration to Azure, right-size servers, plans costs, and analyze application dependencies".

<https://docs.microsoft.com/en-us/learn/modules/design-your-migration-to-azure/2-plan-yourazure-migration>

QUESTION 33

You plan provision a High Performance Computing (HPC) cluster in Azure that will use a third-party scheduler.

You need to recommend a solution to provision and manage the HPC cluster node.

What should you include in the recommendation?

- A. Azure Lighthouse
- B. Azure CycleCloud
- C. Azure Purview
- D. Azure Automation

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

You can dynamically provision Azure HPC clusters with Azure CycleCloud.

Azure CycleCloud is the simplest way to manage HPC workloads.

Note: Azure CycleCloud is an enterprise-friendly tool for orchestrating and managing High Performance Computing (HPC) environments on Azure. With CycleCloud, users can provision infrastructure for HPC systems, deploy familiar HPC schedulers, and automatically scale the infrastructure to run jobs efficiently at any scale. Through CycleCloud, users can create different types of file systems and mount them to the compute cluster nodes to support HPC workloads.

Reference:

<https://docs.microsoft.com/en-us/azure/cyclecloud/overview>

QUESTION 34

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 Traffic Analytics solution in Azure Log Analytics to analyze the network traffic.
Does the solution meet the goal?

- A. Yes
- B. No

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

Explanation:
Instead use Azure Network Watcher to run IP flow verify to analyze the network traffic.
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 35

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: Install and configure the Microsoft Monitoring Agent and the Dependency Agent on all VMs. Use the Wire Data solution in Azure Monitor to analyze the network traffic.
Does the solution meet the goal?

- A. Yes
- B. No

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

Explanation:
Instead use Azure Network Watcher to run IP flow verify to analyze the network traffic.
Note: Wire Data looks at network data at the application level, not down at the TCP transport layer.
The solution doesn't look at individual ACKs and SYNs.
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 36

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

Explanation:

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

QUESTION 37

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 initiative to enforce the location.

Does this meet the goal?

A. Yes

B. No

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

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 38

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

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

Your company plans to deploy various Azure App Service instances that will use Azure SQL databases.

The App Service instances will be deployed at the same time as the Azure SQL databases.

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

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

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

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The Regulatory compliance dashboard in Azure Security Center is not used for regional compliance.

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

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

Reference:

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

<https://azure.microsoft.com/en-us/blog/regulatory-compliance-dashboard-in-azure-security-centernow-available/>

QUESTION 39

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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 40

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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 41

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. IncL 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.
I 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 AD Application Proxy
- C. Azure Front Door
- D. Azure API Management

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

Explanation:

API Management helps organizations publish APIs to external, partner, and internal developers to unlock the potential of their data and services.

You can secure API Management using the OAuth 2.0 client credentials flow.

Reference:

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

<https://docs.microsoft.com/en-us/azure/api-management/api-management-features>

<https://docs.microsoft.com/en-us/azure/api-management/api-management-howto-protect-backend-with-aad#enable-oauth-20-user-authorization-in-the-developer-console>

QUESTION 42

You have an Azure subscription.

You need to recommend an Azure Kubernetes service (AKS) solution that will use Linux nodes. The solution must meet the following requirements:

- Minimize the time it takes to provision compute resources during scale-out operations.
- Support autoscaling of Linux containers.
- Minimize administrative effort.

Which scaling option should you recommend?

- A. Virtual Kubetet
- B. cluster autoscaler
- C. virtual nodes
- D. horizontal pod autoscaler

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

<https://docs.microsoft.com/en-us/azure/aks/virtual-nodes>

QUESTION 43

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. horizontal pod autoscaler
- B. Kubernetes version 1.20.2 or newer
- C. cluster autoscaler
- D. Virtual nodes
- E. with Virtual Kubelet ACI

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

<https://docs.microsoft.com/en-us/azure/aks/cluster-autoscaler#about-the-cluster-autoscaler>

QUESTION 44

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?
D18912E1457D5D1DDCBD40AB3BF70D5D
Which type of resource should you recommend for the integration component?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

Explanation:
A data factory can have one or more pipelines. A pipeline is a logical grouping of activities that together perform a task.
The activities in a pipeline define actions to perform on your data.
Data Factory has three groupings of activities: data movement activities, data transformation activities, and control activities.
Azure Functions is now integrated with Azure Data Factory, allowing you to run an Azure function as a step in your data factory pipelines.
Reference:
<https://docs.microsoft.com/en-us/azure/data-factory/concepts-pipelines-activities>

QUESTION 45

You plan to deploy 10 applications to Azure. The applications will be deployed to two Azure Kubernetes Service (AKS) clusters. Each cluster will be deployed to a separate Azure region.
The application deployment must meet the following requirements:

- Ensure that the applications remain available if a single AKS cluster fails.
- Ensure that the connection traffic over the internet is encrypted by using SSL without having to configure SSL on each container.

Which service should you include in the recommendation?

- A. AKS ingress controller
- B. Azure Traffic Manager
- C. Azure Front Door
- D. Azure Load Balancer

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

Explanation:
"Azure Front Door, which focuses on global load-balancing and site acceleration, and Azure CDN Standard, which offers static content caching and acceleration. The new Azure Front Door brings together security with CDN technology for a cloud-based CDN with threat protection and additional capabilities. "

QUESTION 46

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. Conditional Access policies
- B. role-based access control (RBAC)
- C. Azure Resource Manager (ARM) templates
- D. Azure Policy

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

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

<https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/manage/azure-servermanagement/common-policies#restrict-vm-size>

QUESTION 47

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.

Which type of identity should you include in the recommendation?

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Managed identities for Azure resources is a feature of Azure Active Directory.

User-assigned managed identity can be shared. The same user-assigned managed identity can be associated with more than one Azure resource.

Incorrect Answers:

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

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azureresources/overview>

QUESTION 48

You have an application that is used by 6,000 users to validate their vacation requests. The application manages its own credential. Users must enter a username and password to access the application. The application does NOT support identity providers.

You plan to upgrade the application to use single sign-on (SSO) authentication by using an Azure Active Directory (Azure AD) application registration.

Which SSO method should you use?

- A. password-based
- B. OpenID Connect
- C. header-based
- D. SAML

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 49

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 service should you use?

- A. Azure Data Box Gateway

- B. Azure Databricks
- C. Azure Data Factory
- D. Azure Storage Sync

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

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

Reference:

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

QUESTION 50

You plan to deploy an app that will use an Azure Storage account.

You need to deploy the storage account. The solution must meet the following requirements:

- Store the data of multiple users.
- Encrypt each user's data by using a separate key.
- Encrypt all the data in the storage account by using Microsoft keys or customer-managed keys.

What should you deploy?

- A. files in a general purpose v2 storage account.
- B. blobs in an Azure Data Lake Storage Gen2 account.
- C. files in a premium file share storage account.
- D. blobs in a general purpose v2 storage account

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 51

You plan to deploy an Azure SQL database that will store Personally Identifiable Information (PII). You need to ensure that only privileged users can view the PII.

What should you include in the solution?

- A. Transparent Data Encryption (TDE)
- B. Data Discovery & Classification
- C. dynamic data masking
- D. role-based access control (RBAC)

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 52

You have the resources shown in the following table.

Name	Type
AS1	Azure Synapse Analytics instance
CDB1	Azure Cosmos DB SQL API account

CDB1 hosts a container that stores continuously updated operational data.

You are designing a solution that will use AS! to analyze the operational data daily.

You need to recommend a solution to analyze the data without affecting the performance of the operational data store.
What should you include in the recommendation?

- A. Azure Cosmos DB change feed
- B. Azure Data Factory with Azure Cosmos DB and Azure Synapse Analytics connectors
- C. Azure Synapse Analytics with PolyBase data loading
- D. Azure Synapse Link for Azure Cosmos DB

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 53

You store web access logs data in Azure Blob storage.
You plan to generate monthly reports from the access logs.
You need to recommend an automated process to upload the data to Azure SQL Database every month.
What should you include in the recommendation?

- A. Azure Data Factory
- B. Data Migration Assistant
- C. Microsoft SQL Server Migration Assistant (SSMA)
- D. AzCopy

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Azure Data Factory is the platform that solves such data scenarios. It is the cloud-based ETL and data integration service that allows you to create data-driven workflows for orchestrating data movement and transforming data at scale. Using Azure Data Factory, you can create and schedule data-driven workflows (called pipelines) that can ingest data from disparate data stores. You can build complex ETL processes that transform data visually with data flows or by using compute services such as Azure HDInsight Hadoop, Azure Databricks, and Azure SQL Database.

Reference:

<https://docs.microsoft.com/en-gb/azure/data-factory/introduction>

QUESTION 54

HOTSPOT

You plan to deploy Azure Databricks to support a machine learning application. Data engineers will mount an Azure Data Lake Storage account to the Databricks file system. Permissions to folders are granted directly to the data engineers.

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

Ensure that the data engineers can only access folders to which they have permissions. Minimize development effort.

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 Area

Databricks SKU:

	▼
Premium	
Standard	

Cluster configuration:

	▼
Credential passthrough	
Managed identities	
MLflow	
A runtime that contains Photon	
Secret scope	

Correct Answer:

Answer Area

Databricks SKU:

	▼
Premium	
Standard	

Cluster configuration:

	▼
Credential passthrough	
Managed identities	
MLflow	
A runtime that contains Photon	
Secret scope	

Section: (none)

Explanation

Explanation/Reference:

Box 1: Standard

Choose Standard to minimize costs.

Box 2: Credential passthrough

Athenticate automatically to Azure Data Lake Storage Gen1 (ADLS Gen1) and Azure Data Lake Storage Gen2 (ADLS Gen2) from Azure Databricks clusters using the same Azure Active Directory (Azure AD) identity that you use to log into Azure Databricks. When you enable Azure Data Lake Storage credential passthrough for your cluster, commands that you run on that cluster can read and write data in Azure Data Lake Storage without requiring you to configure service principal credentials for access to storage.

Reference: <https://docs.microsoft.com/en-us/azure/databricks/security/credential-passthrough/adls-passthrough>

QUESTION 55

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.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

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

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

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

A Conditional Access policy
An Azure AD administrative unit
Azure Application Gateway
Azure Blueprints
Azure Policy

Correct Answer:

Answer Area

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

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

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

A Conditional Access policy
An Azure AD administrative unit
Azure Application Gateway
Azure Blueprints
Azure Policy

Section: (none)
Explanation

Explanation/Reference:

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/enus/azure/active-directory/conditional-access/overview>

QUESTION 56
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 table 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

Correct Answer:

Tables

AzureActivity

AzureDiagnostics

Answer Area

Events from Windows event logs:

Event

Events from Linux system logging:

Syslog

Section: (none)
Explanation

Explanation/Reference:

Reference:
<https://docs.microsoft.com/en-us/azure/azure-monitor/platform/data-sources-windows-events>
<https://docs.microsoft.com/enus/azure/azure-monitor/agents/data-sources-syslog>

QUESTION 57
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 features should you recommend be deployed and configured in sequence? To answer, move the appropriate features from the list of features to the answer area and arrange them in the correct order.

Select and Place:

Services	Answer Area
an internal Azure Load Balancer	
an Azure AD conditional access policy	
Azure AD Application Proxy	
an Azure AD managed identity	
a public Azure Load Balancer	
an Azure AD enterprise application	
an App Service plan	

Correct Answer:

Services	Answer Area
an internal Azure Load Balancer	Azure AD Application Proxy
	an Azure AD enterprise application
	an Azure AD conditional access policy
an Azure AD managed identity	
a public Azure Load Balancer	
an App Service plan	

Section: (none)
Explanation

Explanation/Reference: