

Exam Code: AZ-305
Exam Name: Designing Microsoft Azure Infrastructure Solutions



Topic 1 - Litware Inc

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 Qbutton 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.

QUESTION 1

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:

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 2

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:

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 3

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:

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 4

You need to implement the Azure RBAC role assignments for the Network Contributor role. The solution must meet the authentication and authorization requirements. What is the minimum number of assignments that you must use?

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

Correct Answer: B

Section:

Explanation:

QUESTION 5

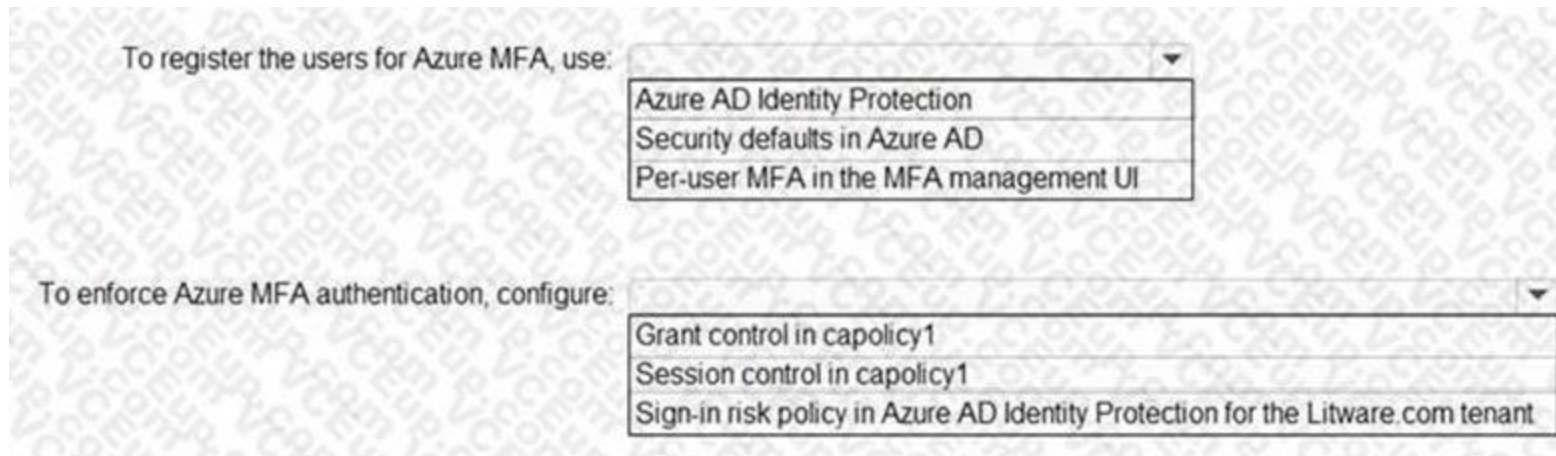
HOTSPOT

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.

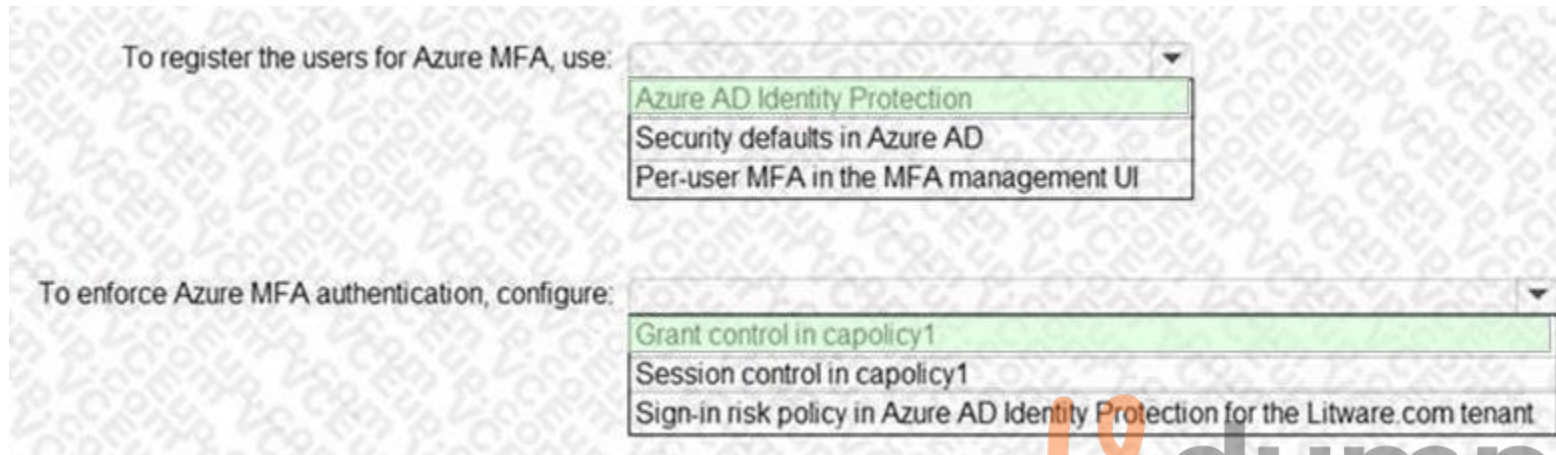
What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area:



Section:

Explanation:

1: Azure AD Identity Protection

2: Grant control in capolicy1

QUESTION 6

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. | |
| 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:

Explanation:

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 7

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:

| |
|---|
| 1 |
| 2 |
| 3 |
| 6 |

Number of virtual machine scale sets:

| |
|---|
| 0 |
| 1 |
| 3 |

Answer Area:

Number of host groups:

| |
|---|
| 1 |
| 2 |
| 3 |
| 6 |

Number of virtual machine scale sets:

| |
|---|
| 0 |
| 1 |
| 3 |



Section:

Explanation:

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

When creating a virtual machine scale set you can specify an existing host group to have all of the VM instances created on dedicated hosts. Which means one scale set for each host group with dedicated hosts.

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

QUESTION 8

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:

- 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

Answer Area:

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:

Explanation:

QUESTION 9

HOTSPOT

You plan to migrate App1 to Azure.

You need to recommend a storage solution for App1 that meets the security and compliance requirements. Which type of storage should you recommend, and how should you recommend configuring the storage?

To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Storage account type:

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

Configuration:

| | |
|------------------------|---|
| | ▼ |
| NFSv3 | |
| Large file shares | |
| Hierarchical namespace | |

Answer Area:

Answer Area

Storage account type:

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

Configuration:

| | |
|------------------------|---|
| | ▼ |
| NFSv3 | |
| Large file shares | |
| Hierarchical namespace | |

Section:

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 10

HOTSPOT

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

Hot Area:

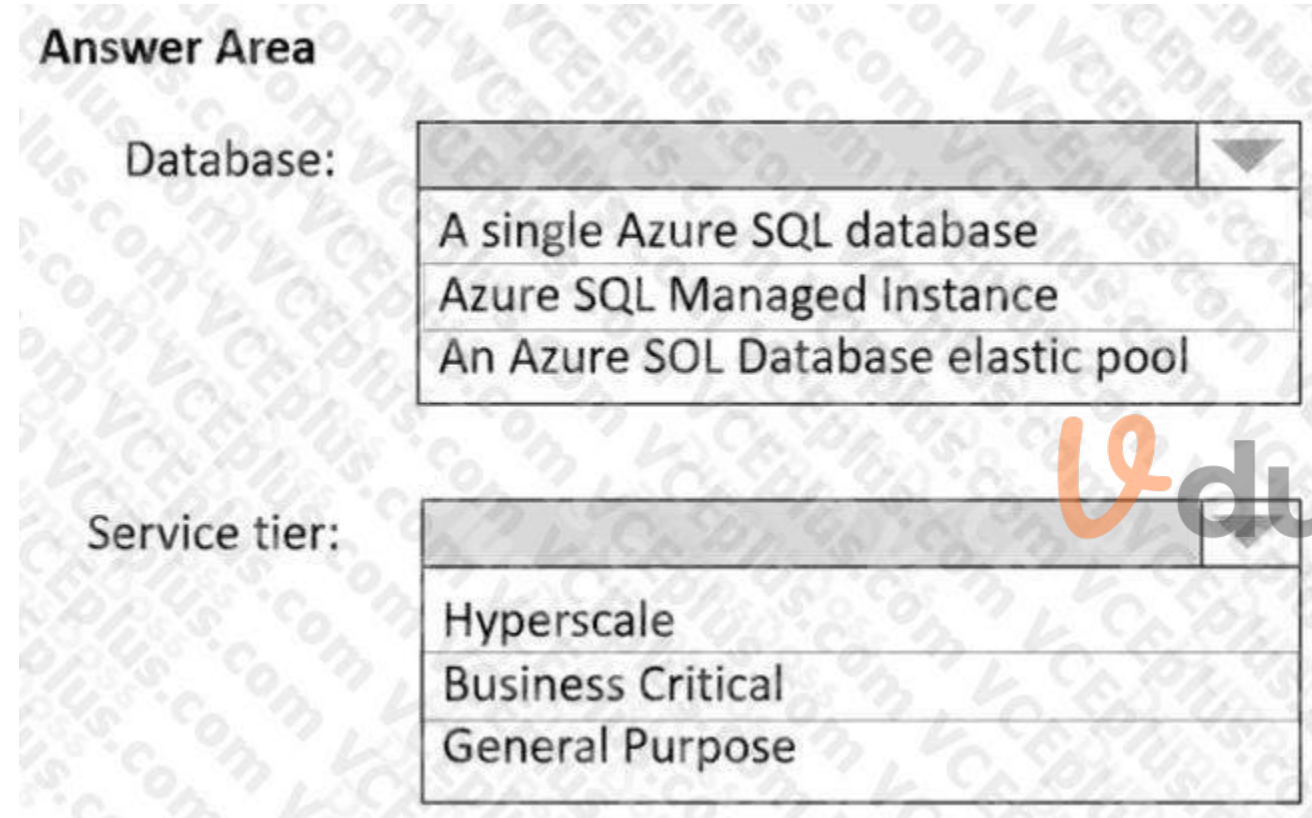
Answer Area

Database:

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

Service tier:

| | |
|-------------------|--|
| | |
| Hyperscale | |
| Business Critical | |
| General Purpose | |



Answer 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

Section:

Explanation:

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>

Exam B

QUESTION 1

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: C

Section:

QUESTION 2

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 AS1 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: D

Section:

QUESTION 3

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:

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 4

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 | |

Answer Area:

Answer Area

Databricks SKU:

| | |
|----------|---|
| | ▼ |
| Premium | |
| Standard | |

Cluster configuration:

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

Section:

Explanation:

Box 1: Standard

Choose Standard to minimize costs.



Answer Area

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

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

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

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

Section:

Explanation:

Box 1: An Azure AD app registration

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

Box 2: A conditional access policy

Conditional Access policies at their simplest are if-then statements, if a user wants to access a resource, then they must complete an action. By using Conditional Access policies, you can apply the right access controls when needed to keep your organization secure and stay out of your user's way when not needed.

Reference:

<https://codingcanvas.com/using-azure-active-directory-authentication-in-your-web-application/> <https://docs.microsoft.com/enus/azure/active-directory/conditional-access/overview>

QUESTION 6

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 | Answer Area |
|------------------|---|
| AzureActivity | Events from Windows event logs: Table |
| AzureDiagnostics | Events from Linux system logging: Table |
| Event | |
| Syslog | |

Correct Answer:

| Tables | Answer Area |
|------------------|--|
| AzureActivity | Events from Windows event logs: Event |
| AzureDiagnostics | Events from Linux system logging: Syslog |
| | |
| | |

Udumps

Section:

Explanation:

Reference:

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

QUESTION 7

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

- 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

Answer Area



Correct Answer:

Services

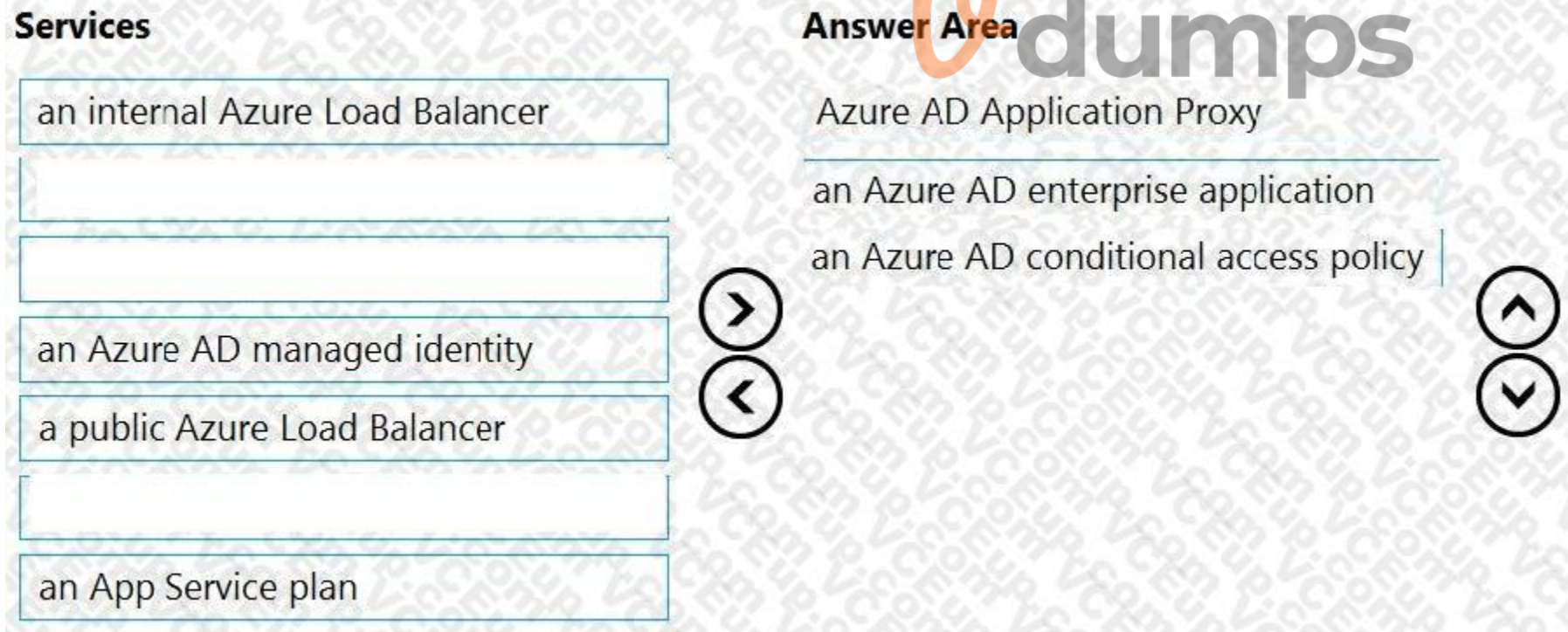
- an internal Azure Load Balancer
-
-
- an Azure AD managed identity
- a public Azure Load Balancer
-
- an App Service plan

Answer Area

Azure AD Application Proxy

an Azure AD enterprise application

an Azure AD conditional access policy



Section:

Explanation:

QUESTION 8

HOTSPOT

You need to design a storage solution for an app that will store large amounts of frequently used data. The solution must meet the following requirements:

Maximize data throughput.

Prevent the modification of data for one year.

Minimize latency for read and write operations.

Which Azure Storage account type and storage service should you recommend? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Storage account type:

| | |
|-------------------------------------|---|
| | ▼ |
| BlobStorage | |
| BlockBlobStorage | |
| FileStorage | |
| StorageV2 with Premium performance | |
| StorageV2 with Standard performance | |

Storage service:

| | |
|-------|---|
| | ▼ |
| Blob | |
| File | |
| Table | |

Vdumps

Answer Area:

Answer Area

Storage account type:

| | |
|-------------------------------------|---|
| | ▼ |
| BlobStorage | |
| BlockBlobStorage | |
| FileStorage | |
| StorageV2 with Premium performance | |
| StorageV2 with Standard performance | |

Storage service:

| | |
|-------|---|
| | ▼ |
| Blob | |
| File | |
| Table | |

Section:

Explanation:

Box 1: BlockBlobStorage

Block Blob is a premium storage account type for block blobs and append blobs. Recommended for scenarios with high transactions rates, or scenarios that use smaller objects or require consistently low storage

latency. Box 2: Blob

The Archive tier is an offline tier for storing blob data that is rarely accessed. The Archive tier offers the lowest storage costs, but higher data retrieval costs and latency compared to the online tiers (Hot and Cool).

Data must remain in the Archive tier for at least 180 days or be subject to an early deletion charge.

Reference: <https://docs.microsoft.com/en-us/azure/storage/blobs/archive-blob>

QUESTION 9

HOTSPOT

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

| Name | Type | Performance |
|----------|-------------|-------------|
| storage1 | StorageV2 | Standard |
| storage2 | StorageV2 | Premium |
| storage3 | BlobStorage | Standard |
| storage4 | FileStorage | Premium |

You plan to implement two new apps that have the requirements shown in the following table.

| Name | Requirement |
|------|--|
| App1 | Use lifecycle management to migrate app data between storage tiers |
| App2 | Store app data in an Azure file share |

Which storage accounts should you recommend using for each app? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

App1:

| |
|--|
| Storage1 and storage2 only |
| Storage1 and storage3 only |
| Storage1, storage2, and storage3 only |
| Storage1, storage2, storage3, and storage4 |

App2:

| |
|--|
| Storage4 only |
| Storage1 and storage4 only |
| Storage1, storage2, and storage4 only |
| Storage1, storage2, storage3, and storage4 |

Answer Area:

Answer Area

App1:

| |
|--|
| Storage1 and storage2 only |
| Storage1 and storage3 only |
| Storage1, storage2, and storage3 only |
| Storage1, storage2, storage3, and storage4 |

App2:

| |
|--|
| Storage4 only |
| Storage1 and storage4 only |
| Storage1, storage2, and storage4 only |
| Storage1, storage2, storage3, and storage4 |

Section:

Explanation:

Box 1: Storage1 and storage3 only

Azure Blob Storage lifecycle management offers a rich, rule-based policy for GPv2 and blob storage accounts. Storage 2 does not support access tiers. Box 2: Storage1 and storage4 only
 FileStorage storage accounts allow you to deploy Azure file shares on premium/solid-state disk-based (SSD-based) hardware.

Reference:

<https://docs.microsoft.com/en-us/azure/storage/blobs/storage-lifecycle-management-concepts> <https://docs.microsoft.com/japp/azure/storage/common/storage-account-overview>

QUESTION 10

HOTSPOT

You have an on-premises database that you plan to migrate to Azure.

You need to design the database architecture to meet the following requirements:

Support scaling up and down.

Support geo-redundant backups.

Support a database of up to 75 TB.

Be optimized for online transaction processing (OLTP).

What should you include in the design? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Service:

| | |
|--------------------------------------|---|
| | ▼ |
| Azure SQL Database | |
| Azure SQL Managed Instance | |
| Azure Synapse Analytics | |
| SQL Server on Azure Virtual Machines | |

Service tier:

| | |
|-------------------|---|
| | ▼ |
| Basic | |
| Business Critical | |
| General Purpose | |
| Hyperscale | |
| Premium | |
| Standard | |

Vdumps

Answer Area:

Answer Area

Service:

| |
|--------------------------------------|
| ▼ |
| Azure SQL Database |
| Azure SQL Managed Instance |
| Azure Synapse Analytics |
| SQL Server on Azure Virtual Machines |

Service tier:

| |
|-------------------|
| ▼ |
| Basic |
| Business Critical |
| General Purpose |
| Hyperscale |
| Premium |
| Standard |

Section:

Explanation:

Box 1: Azure SQL Database Azure SQL Database:

Database size always depends on the underlying service tiers (e.g. Basic, Business Critical, Hyperscale). It supports databases of up to 100 TB with Hyperscale service tier model. Active geo-replication is a feature that lets you to create a continuously synchronized readable secondary database for a primary database. The readable secondary database may be in the same Azure region as the primary, or, more commonly, in a different region. This kind of readable secondary databases are also known as geo-secondaries, or geo-replicas. Azure SQL Database and SQL Managed Instance enable you to dynamically add more resources to your database with minimal downtime. Box 2: Hyperscale Incorrect Answers:

SQL Server on Azure VM: geo-replication not supported.

Azure Synapse Analytics is not optimized for online transaction processing (OLTP).

Azure SQL Managed Instance max database size is up to currently available instance size (depending on the number of vCores). Max instance storage size (reserved) - 2 TB for 4 vCores - 8 TB for 8 vCores - 16 TB for other sizes

Reference: <https://docs.microsoft.com/en-us/azure/azure-sql/database/active-geo-replication-overview> <https://medium.com/awesome-azure/azure-difference-between-azure-sql-database-and-sql-server-on-vm-comparison-azuresql-vs-sql-server-vm-cf02578a1188>

QUESTION 11

HOTSPOT

Your company has two on-premises sites in New York and Los Angeles and Azure virtual networks in the East US Azure region and the West US Azure region. Each on-premises site has Azure ExpressRoute circuits to both regions. You need to recommend a solution that meets the following requirements:

Outbound traffic to the Internet from workloads hosted on the virtual networks must be routed through the closest available on-premises site. If an on-premises site fails, traffic from the workloads on the virtual networks to the Internet must reroute automatically to the other site. 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:

| | |
|---|---|
| Routing from the virtual networks to the on-premises locations must be configured by using: | ▼ |
| | Azure default routes |
| | Border Gateway Protocol (BGP) |
| | User-defined routes |
| The automatic routing configuration following a failover must be handled by using: | ▼ |
| | Border Gateway Protocol (BGP) |
| | Hot Standby Routing Protocol (HSRP) |
| | Virtual Router Redundancy Protocol (VRRP) |

Answer Area:

| | |
|---|---|
| Routing from the virtual networks to the on-premises locations must be configured by using: | ▼ |
| | Azure default routes |
| | Border Gateway Protocol (BGP) |
| | User-defined routes |
| The automatic routing configuration following a failover must be handled by using: | ▼ |
| | Border Gateway Protocol (BGP) |
| | Hot Standby Routing Protocol (HSRP) |
| | Virtual Router Redundancy Protocol (VRRP) |

Section:

Explanation:

An on-premises network gateway can exchange routes with an Azure virtual network gateway using the border gateway protocol (BGP). Using BGP with an Azure virtual network gateway is dependent on the type you selected when you created the gateway. If the type you selected were: ExpressRoute:

You must use BGP to advertise on-premises routes to the Microsoft Edge router. You cannot create user-defined routes to force traffic to the ExpressRoute virtual network gateway if you deploy a virtual network gateway deployed as type:

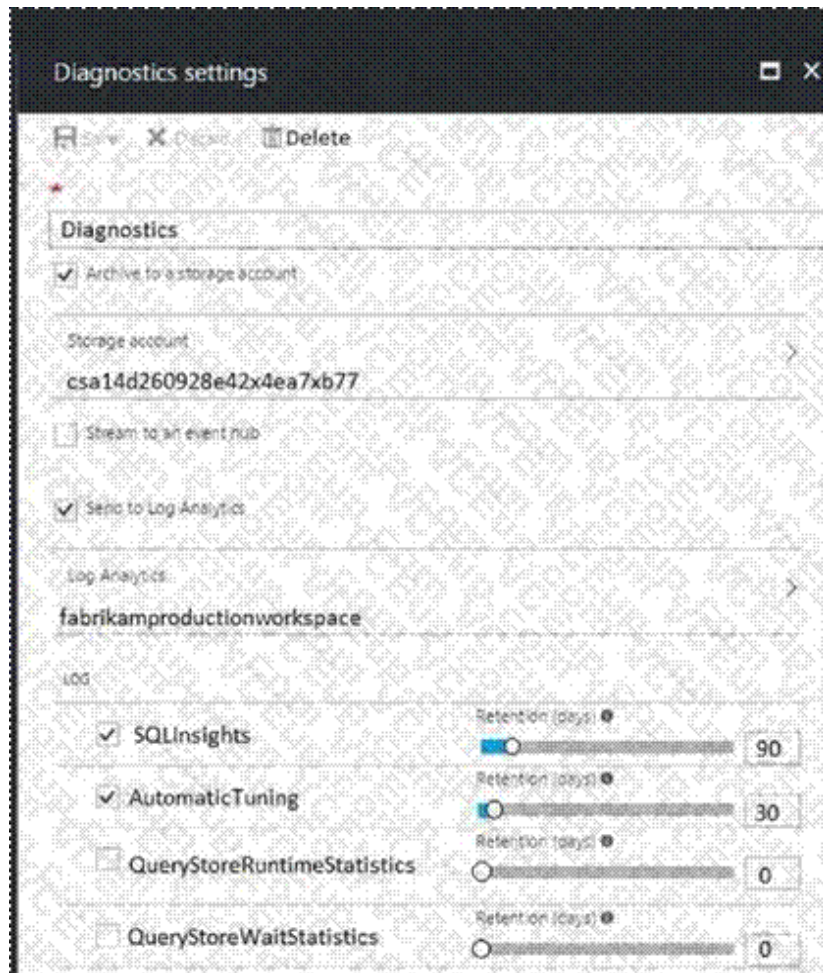
ExpressRoute. You can use user-defined routes for forcing traffic from the Express Route to, for example, a Network Virtual Appliance. [https://docs.microsoft.com/ja-jp/azure/expressroute/designing-for-disaster-recovery-withQuestions&Answers PDF P-91expressroute-privatepeering](https://docs.microsoft.com/ja-jp/azure/expressroute/designing-for-disaster-recovery-withQuestions&Answers%20PDF%20P-91expressroute-privatepeering) <https://docs.microsoft.com/en-us/azure/expressroute/expressroute-optimize-routing#suboptimalrouting-from-customer-to-microsoft>

QUESTION 12

HOTSPOT

You deploy several Azure SQL Database instances.

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



Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic. NOTE: Each correct selection is worth one point.



Hot Area:

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

| | |
|------------|---|
| | ▼ |
| 30 days | |
| 90 days | |
| 730 days | |
| indefinite | |

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

| | |
|------------|---|
| | ▼ |
| 30 days | |
| 90 days | |
| 730 days | |
| indefinite | |

Answer Area:

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

| | |
|------------|---|
| | ▼ |
| 30 days | |
| 90 days | |
| 730 days | |
| indefinite | |

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

| | |
|------------|---|
| | ▼ |
| 30 days | |
| 90 days | |
| 730 days | |
| indefinite | |

Section:

Explanation:

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

QUESTION 13

HOTSPOT

You have an Azure App Service web app that uses a system-assigned managed identity.

You need to recommend a solution to store their settings of the web app as secrets in an Azure key vault. The solution must meet the following requirements:

- Minimize changes to the app code,
- Use the principle of least privilege.

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

Hot Area:

Answer Area

| | |
|---|---|
| Key Vault integration method: | <input type="checkbox"/> Key Vault references in Application settings <input type="checkbox"/> Key Vault references in Appsettings.json <input type="checkbox"/> Key Vault references in Web.config <input type="checkbox"/> Key Vault SDK |
| Key Vault permissions for the managed identity: | <input type="checkbox"/> Keys: Get <input type="checkbox"/> Keys: List and Get <input type="checkbox"/> Secrets: Get <input type="checkbox"/> Secrets: List and Get |

Answer Area:

Answer Area

Key Vault integration method:

- Key Vault references in Application settings
- Key Vault references in Appsettings.json
- Key Vault references in Web.config
- Key Vault SDK

Key Vault permissions for the managed identity:

- Keys: Get
- Keys: List and Get
- Secrets: Get
- Secrets: List and Get

Section:

Explanation:

QUESTION 14

HOTSPOT

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

- For new resources, assign tags and values that match the tags and values of the resource group to which the resources are deployed.
- For existing resources, identify whether the tags and values match the tags and values of the resource group that contains the resources.
- For any non-compliant resources, trigger auto-generated remediation tasks to create missing tags and values. The solution must use the principle of least privilege.

What should you include in the design? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Hot Area:

Azure Policy effect to use:

- Append
- EnforceOPAConstraint
- EnforceRegoPolicy
- Modify

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

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

Answer Area:

Azure Policy effect to use:

- Append
- EnforceOPAConstraint
- EnforceRegoPolicy
- Modify

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

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

Section:

Explanation:

Box 1: Modify

Modify is used to add, update, or remove properties or tags on a resource during creation or update. A common example is updating tags on resources such as costCenter. Existing non-compliant resources can be remediated with a remediation task. A single Modify rule can have any number of operations. Box 2: A managed identity with the Contributor role

Managed identity

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

Contributor role

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

Reference:

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

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

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

<https://docs.microsoft.com/en-us/azure/governance/policy/concepts/effects#modify>

QUESTION 15

HOTSPOT

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

| Name | Type | Kind | Location |
|------------|-------------------------------|-----------------------|----------|
| storage1 | Azure Storage account | Storage | East US |
| storage2 | Azure Storage account | StorageV2 | East US |
| Workspace1 | Azure Log Analytics workspace | <i>Not applicable</i> | East US |
| Workspace2 | Azure Log Analytics workspace | <i>Not applicable</i> | East US |
| Hub1 | Azure event hub | <i>Not applicable</i> | East US |

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

To DB1, you add a diagnostic setting named Settings1. Settings1 archives SQLInsights to storage1 and sends SQLInsights to Workspace1. For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.



Hot Area:

| Statements | Yes | No |
|--|-----------------------|-----------------------|
| You can add a new diagnostic setting that archives SQLInsights logs to storage2. | <input type="radio"/> | <input type="radio"/> |
| You can add a new diagnostic setting that sends SQLInsights logs to Workspace2. | <input type="radio"/> | <input type="radio"/> |
| You can add a new diagnostic setting that sends SQLInsights logs to Hub1. | <input type="radio"/> | <input type="radio"/> |

Answer Area:

| Statements | Yes | No |
|--|----------------------------------|-----------------------|
| You can add a new diagnostic setting that archives SQLInsights logs to storage2. | <input checked="" type="radio"/> | <input type="radio"/> |
| You can add a new diagnostic setting that sends SQLInsights logs to Workspace2. | <input checked="" type="radio"/> | <input type="radio"/> |
| You can add a new diagnostic setting that sends SQLInsights logs to Hub1. | <input checked="" type="radio"/> | <input type="radio"/> |

Section:

Explanation:

Box 1: Yes

Box 2: Yes

Box 3: Yes

For more information on Azure SQL diagnostics , you can visit the below link

<https://docs.microsoft.com/en-us/azure/azure-sql/database/metrics-diagnostic-telemetry-loggingstreaming-export-configure>

QUESTION 16

HOTSPOT

Your company has the divisions shown in the following table.

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



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

A resource group

An Azure web app

Custom role assignments

An Azure Cosmos DB account

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

What is the minimum number of objects required to deploy the application? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Hot Area:

Management groups: ▼

| |
|---|
| 1 |
| 2 |
| 3 |
| 4 |

Blueprint definitions: ▼

| |
|---|
| 1 |
| 2 |
| 3 |
| 4 |

Blueprint assignments: ▼

| |
|---|
| 1 |
| 2 |
| 3 |
| 4 |

Answer Area:

Management groups: ▼

| |
|---|
| 1 |
| 2 |
| 3 |
| 4 |

Blueprint definitions: ▼

| |
|---|
| 1 |
| 2 |
| 3 |
| 4 |

Blueprint assignments: ▼

| |
|---|
| 1 |
| 2 |
| 3 |
| 4 |

Section:

Explanation:

Box 1: 2



One management group for East, and one for West.

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

Box 2: 2

Box 3: 4

One assignment for each subscription.

"Assigning a blueprint definition to a management group means the assignment object exists at the management group. The deployment of artifacts still targets a subscription. To perform a management group assignment, the Create Or Update REST API must be used and the request body must include a value for properties.scope to define the target subscription." <https://docs.microsoft.com/en-us/azure/governance/blueprints/overview#blueprint-assignment>

QUESTION 17

HOTSPOT

You have an Azure subscription that contains 300 Azure virtual machines that run Windows Server 2016. You need to centrally monitor all warning events in the System logs of the virtual machines. What should you include in the solutions? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Hot Area:

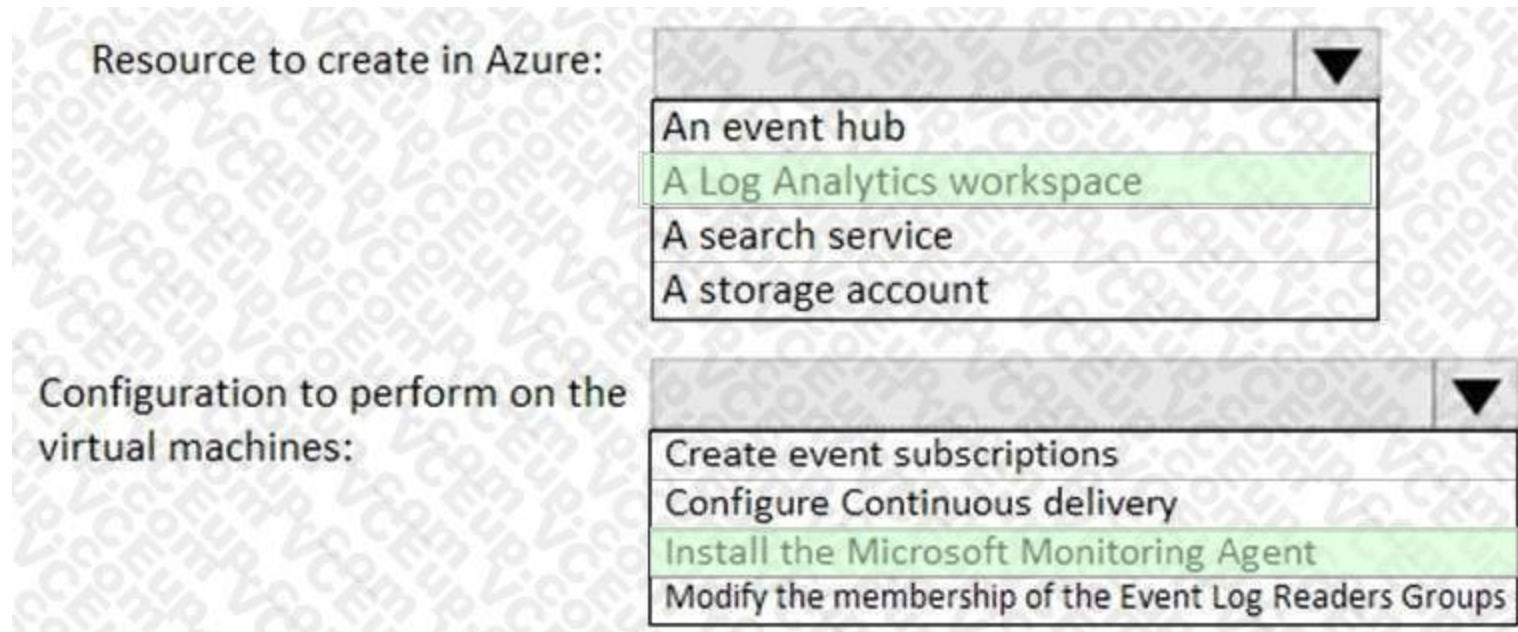
Resource to create in Azure:

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

Configuration to perform on the virtual machines:

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

Answer Area:



Section:

Explanation:

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

<https://docs.microsoft.com/en-us/azure/azure-monitor/platform/agent-windows>

QUESTION 18

HOTSPOT

Your organization has developed and deployed several Azure App Service Web and API applications.

The applications use Azure Key Vault to store several authentication, storage account, and data encryption keys. Several departments have the following requests to support the applications:

| Department | Request |
|-------------------|---|
| Security | <ul style="list-style-type: none"> Review membership of administrative roles and require to provide a justification for continued membership Get alerts about changes in administrator assignments See a history of administrator activation, including which changes administrators made to Azure resources |
| Development | <ul style="list-style-type: none"> Enable the applications to access Azure Key Vault and retrieve keys for use in code |
| Quality Assurance | <ul style="list-style-type: none"> Receive temporary administrator access to create and configure additional Web and API applications in the test environment. |

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

What should you recommend? To answer, configure the appropriate options in the dialog box in the answer area. NOTE: Each correct selection is worth one point.

Hot Area:

| Department | Azure Service |
|-------------------|---|
| Security | <div style="border: 1px solid black; padding: 2px;"> ▼ </div> <div style="border: 1px solid black; padding: 2px;"> Azure AD Privileged Identity Management Azure AD Managed Service Identity Azure AD Connect Azure AD Identity Protection </div> |
| Development | <div style="border: 1px solid black; padding: 2px;"> ▼ </div> <div style="border: 1px solid black; padding: 2px;"> Azure AD Privileged Identity Management Azure AD Managed Service Identity Azure AD Connect Azure AD Identity Protection </div> |
| Quality Assurance | <div style="border: 1px solid black; padding: 2px;"> ▼ </div> <div style="border: 1px solid black; padding: 2px;"> Azure AD Privileged Identity Management Azure AD Managed Service Identity Azure AD Connect Azure AD Identity Protection </div> |

Vdumps

Answer Area:

| Department | Azure Service |
|-------------------|--|
| Security | <div style="border: 1px solid black; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px;">▼</div> <div style="padding: 2px;"> <p>Azure AD Privileged Identity Management</p> <p>Azure AD Managed Service Identity</p> <p>Azure AD Connect</p> <p>Azure AD Identity Protection</p> </div> </div> |
| Development | <div style="border: 1px solid black; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px;">▼</div> <div style="padding: 2px;"> <p>Azure AD Privileged Identity Management</p> <p>Azure AD Managed Service Identity</p> <p>Azure AD Connect</p> <p>Azure AD Identity Protection</p> </div> </div> |
| Quality Assurance | <div style="border: 1px solid black; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px;">▼</div> <div style="padding: 2px;"> <p>Azure AD Privileged Identity Management</p> <p>Azure AD Managed Service Identity</p> <p>Azure AD Connect</p> <p>Azure AD Identity Protection</p> </div> </div> |

Section:

Explanation:

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

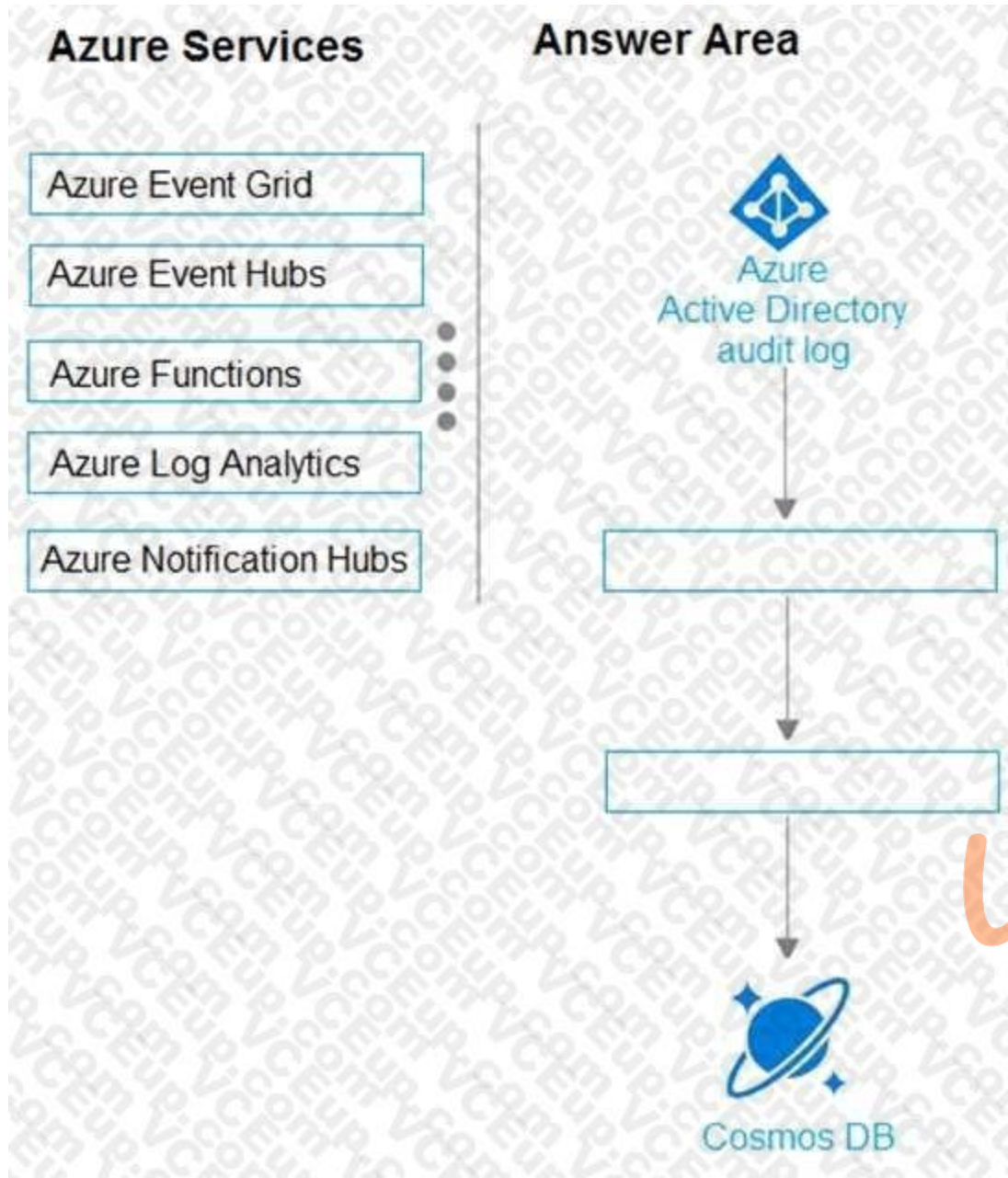
QUESTION 19

DRAG DROP

You need to design an architecture to capture the creation of users and the assignment of roles. The captured data must be stored in Azure Cosmos DB. Which Azure services should you include in the design? To answer, drag the appropriate services to the correct targets. 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.

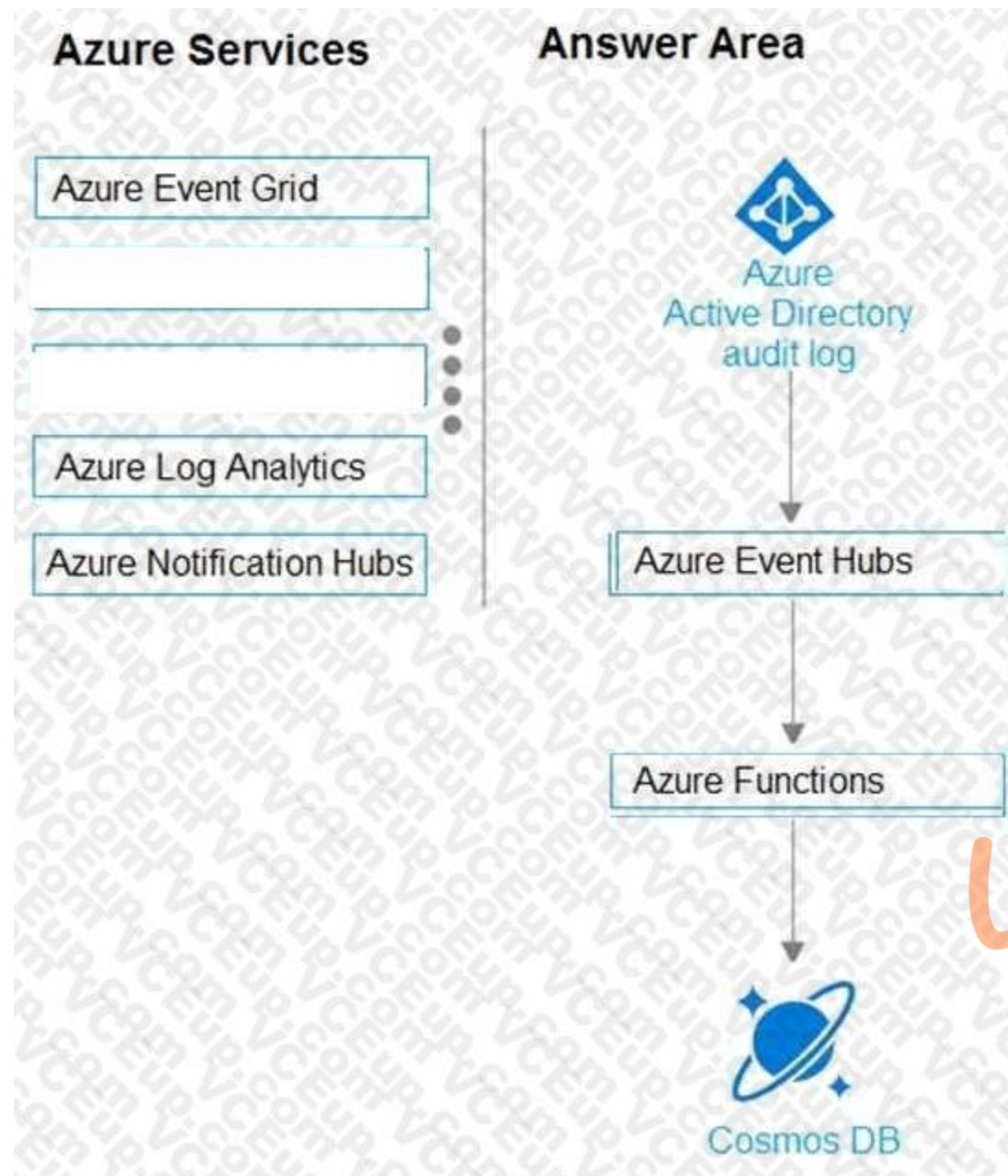
NOTE: Each correct selection is worth one point.

Select and Place:



 **vdumps**

Correct Answer:



vdumps

Section:

Explanation:

1. AAD audit log -> Event Hub (other two choices, LAW, storage, but not available in this question) <https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/tutorial-azuremonitor-stream-logs-to-event-hub> 2. Azure function has the Event hub trigger and Cosmos output binding

a. Event Hub trigger for function

<https://docs.microsoft.com/en-us/azure/azure-functions/functions-bindings-event-hubtrigger?tabs=csharp>

QUESTION 20

HOTSPOT

You are designing an application that will use Azure Linux virtual machines to analyze video files. The files will be uploaded from corporate offices that connect to Azure by using ExpressRoute. You plan to provision an Azure Storage account to host the files.

You need to ensure that the storage account meets the following requirements:

- Supports video files of up to 7 TB
 - Provides the highest availability possible
 - Ensures that storage is optimized for the large video files
 - Ensures that files from the on-premises network are uploaded by using ExpressRoute
- How should you configure the storage account? To answer, select the appropriate options in the answer area. NOTE: Each

correct selection is worth one point.

Hot Area:

Answer Area

| | |
|--|---|
| Storage account type: | <input type="checkbox"/> Premium file shares <input type="checkbox"/> Premium page blobs <input type="checkbox"/> Standard general-purpose v2 |
| Data redundancy: | <input type="checkbox"/> Geo-redundant storage (GRS) <input type="checkbox"/> Locally-redundant storage (LRS) - <input type="checkbox"/> Zone-redundant storage (ZRS) |
| These are the selections for Data redundancy | |
| Networking: | <input type="checkbox"/> Azure Route Server <input type="checkbox"/> A private endpoint <input type="checkbox"/> A service endpoint |

Answer Area:

Answer Area

| | |
|--|--|
| Storage account type: | <input checked="" type="checkbox"/> Premium file shares <input type="checkbox"/> Premium page blobs <input type="checkbox"/> Standard general-purpose v2 |
| Data redundancy: | <input type="checkbox"/> Geo-redundant storage (GRS) <input checked="" type="checkbox"/> Locally-redundant storage (LRS) - <input type="checkbox"/> Zone-redundant storage (ZRS) |
| These are the selections for Data redundancy | |
| Networking: | <input checked="" type="checkbox"/> Azure Route Server <input type="checkbox"/> A private endpoint <input type="checkbox"/> A service endpoint |

Section:

Explanation:

QUESTION 21

HOTSPOT

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

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

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

Each correct selection is worth one point

Hot Area:

Answer Area

Application1:

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

Application2:

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

Answer Area:



Answer Area

Application1:

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

Application2:

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



Section:

Explanation:

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

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

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

Box 2: General purpose v2 with Standard performance..

General-purpose v2 accounts: Basic storage account type for blobs, files, queues, and tables.

Recommended for most scenarios using Azure Storage.

Reference:

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

<https://docs.microsoft.com/en-us/azure/storage/common/storage-redundancy>

QUESTION 22

HOTSPOT

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

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

What storage solution should you recommend for the app? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Storage Account type:

- Standard general-purpose v1
- Standard general-purpose v2
- Premium block blobs

Redundancy:

- Zone-redundant storage (ZRS)
- Locally-redundant storage (LRS)
- Read-access geo-redundant storage (RA-GRS)

Answer Area:

Answer Area

Storage Account type:

- Standard general-purpose v1
- Standard general-purpose v2
- Premium block blobs

Redundancy:

- Zone-redundant storage (ZRS)
- Locally-redundant storage (LRS)
- Read-access geo-redundant storage (RA-GRS)

Section:

Explanation:



QUESTION 23

HOTSPOT

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

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

You add a new data factory.

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

NOTE: Each correct selection is worth one point.

Hot Area:

From Server1:

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

From the data factory:

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

Answer Area:

From Server1:

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

From the data factory:

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

Section:

Explanation:

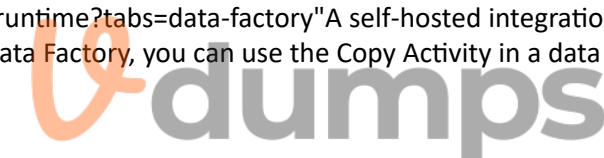
Box 1: Install a self-hosted integration runtime

The Integration Runtime is a customer-managed data integration infrastructure used by Azure Data Factory to provide data integration capabilities across different network environments. Box 2: Create a pipeline With ADF, existing data processing services can be composed into data pipelines that are highly available and managed in the cloud. These data pipelines can be scheduled to ingest, prepare, transform, analyze, and publish data, and ADF manages and orchestrates the complex data and processing dependencies

Reference:

<https://docs.microsoft.com/en-us/azure/machine-learning/team-data-science-process/move-sqlazure-adf> <https://docs.microsoft.com/pl-pl/azure/data-factory/tutorial-hybrid-copy-data-toolsy31svc> 3 months, 4 weeks ago

<https://docs.microsoft.com/en-us/azure/data-factory/create-self-hosted-integrationruntime?tabs=data-factory>"A self-hosted integration runtime can run copy activities between a cloud data store and a datastore in a private network" <https://docs.microsoft.com/en-us/azure/data-factory/introduction>"With Data Factory, you can use the Copy Activity in a data pipeline to move data from both onpremisesand cloud source data stores to a centralization data store in the cloud for further analysis"



QUESTION 24

HOTSPOT

You have the resources shown in the following table.

| Name | Type | Resource group |
|------|-----------------------------|----------------|
| VM1 | Azure virtual machine | RG1 |
| VM2 | On-premises virtual machine | Not applicable |

You create a new resource group in Azure named RG2.

You need to move the virtual machines to RG2.

What should you use to move each virtual machine? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Hot Area:

VM1: Azure Arc
 Azure Lighthouse
 Azure Migrate
 Azure Resource Mover
 The Data Migration Assistant (DMA)

VM2: Azure Arc
 Azure Lighthouse
 Azure Migrate
 Azure Resource Mover
 The Data Migration Assistant (DMA)

Answer Area:

VM1: Azure Arc
 Azure Lighthouse
 Azure Migrate
 Azure Resource Mover
 The Data Migration Assistant (DMA)

VM2: Azure Arc
 Azure Lighthouse
 Azure Migrate
 Azure Resource Mover
 The Data Migration Assistant (DMA)



Section:

Explanation:

VM1: Azure Lighthouse

VM2: Azure Migrate

QUESTION 25

HOTSPOT

You have the Azure resources shown in the following table.

| Name | Type | Description |
|-------------|--------------------|---|
| VNET1 | Virtual network | Connected to an on-premises network by using ExpressRoute |
| VM1 | Virtual machine | Configured as a DNS server |
| SQLDB1 | Azure SQL Database | Single instance |
| PE1 | Private endpoint | Provides connectivity to SQLDB1 |
| contoso.com | Private DNS zone | Linked to VNET1 and contains an A record for PE1 |
| contoso.com | Public DNS zone | Contains a CNAME record for SQLDB1 |

You need to design a solution that provides on-premises network connectivity to SQLDB1 through PE1. How should you configure name resolution? To answer, select the appropriate options in the answer area.

Hot Area:

Azure configuration:

Configure VM1 to forward contoso.com to the public DNS zone.
Configure VM1 to forward contoso.com to the Azure-provided DNS at 168.63.129.16.
In VNet1, configure a custom DNS server set to the Azure-provided DNS at 168.63.129.16.

On-premises DNS configuration:

Forward contoso.com to VM1.
Forward contoso.com to the public DNS zone.
Forward contoso.com to the Azure-provided DNS at 168.63.129.16.

Answer Area:

Azure configuration:

Configure VM1 to forward contoso.com to the public DNS zone.
Configure VM1 to forward contoso.com to the Azure-provided DNS at 168.63.129.16.
In VNet1, configure a custom DNS server set to the Azure-provided DNS at 168.63.129.16.

On-premises DNS configuration:

Forward contoso.com to VM1.
Forward contoso.com to the public DNS zone.
Forward contoso.com to the Azure-provided DNS at 168.63.129.16.

Section:

Explanation:

QUESTION 26

HOTSPOT

You plan to migrate on-premises Microsoft SQL Server databases to Azure.

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

Supports user-initiated backups

Supports multiple automatically replicated instances across Azure regions Minimizes administrative effort to implement and maintain business continuity What should you recommendation? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

| | |
|----------------------|---|
| Deployment solution: | Azure SQL Managed Instance SQL Server on Azure Virtual Machines An Azure SQL Database single database |
| Resiliency solution: | Auto-failover group Active geo-replication Zone-redundant deployment |

Answer Area:

| | |
|----------------------|---|
| Deployment solution: | Azure SQL Managed Instance SQL Server on Azure Virtual Machines An Azure SQL Database single database |
| Resiliency solution: | Auto-failover group Active geo-replication Zone-redundant deployment |

Section:

Explanation:

Box 1: An Azure SQL Database single database.

SQL Server Managed instance versus SQL Server Virtual Machines

Active geo-replication is not supported by Azure SQL Managed Instance.

Box 2: Active geo-replication

Active geo-replication is a feature that lets you to create a continuously synchronized readable secondary database for a primary database. The readable secondary database may be in the same Azure region as the primary, or, more commonly, in a different region. This kind of readable secondary databases are also known as geo-secondaries, or geo-replicas.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-sql/database/active-geo-replication-overview>



QUESTION 27

HOTSPOT

You have an Azure subscription that is linked to an Azure Active Directory Premium Plan 2 tenant. The tenant has multi-factor authentication (MFA) enabled for all users.

| Name | IP address range | Trusted |
|------|------------------|---------|
| NY | 192.168.2.0/27 | Yes |
| DC | 192.168.1.0/27 | No |
| LA | 192.168.3.0/27 | No |

You have the named locations shown in the following table.

| Name | Device operating system | User-risk level | Matching compliance policies |
|-------|-------------------------|-----------------|------------------------------|
| User1 | Windows 10 | High | None |
| User2 | Windows 10 | Medium | None |
| User3 | macOS | Low | None |

You have the users shown in the following table.

| Name | Assignment | Conditions: Locations | Conditions: User risk | Conditions: Sign-in risk | Access Control: Grant |
|------|------------|-----------------------|-----------------------|--------------------------|---|
| CA1 | All users | Trusted locations | High, Medium | None | Block access |
| CA2 | All users | NY | None | High, Medium | Block access |
| CA3 | All users | LA | None | None | Grant access: Require device to marked as compliant |

You plan to deploy the Conditional Access policies shown in the following table.
 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 |
|---|-----------------------|-----------------------|
| To ensure that the conditions in CA1 can be evaluated, you must enforce an Azure Active Directory (Azure AD) Identity Protection user risk policy . | <input type="radio"/> | <input type="radio"/> |
| To ensure that the conditions in CA2 can be evaluated, you must enforce an Azure Active Directory (Azure AD) Identity Protection sign-in risk policy. | <input type="radio"/> | <input type="radio"/> |
| To ensure that the conditions in CA3 can be evaluated, you must deploy Microsoft Endpoint Manager. | <input type="radio"/> | <input type="radio"/> |

Answer Area:

| Statements | Yes | No |
|---|----------------------------------|----------------------------------|
| To ensure that the conditions in CA1 can be evaluated, you must enforce an Azure Active Directory (Azure AD) Identity Protection user risk policy . | <input type="radio"/> | <input checked="" type="radio"/> |
| To ensure that the conditions in CA2 can be evaluated, you must enforce an Azure Active Directory (Azure AD) Identity Protection sign-in risk policy. | <input type="radio"/> | <input checked="" type="radio"/> |
| To ensure that the conditions in CA3 can be evaluated, you must deploy Microsoft Endpoint Manager. | <input checked="" type="radio"/> | <input type="radio"/> |

Section:

Explanation:

QUESTION 28

HOTSPOT

You have an Azure Load Balancer named LB1 that balances requests to five Azure virtual machines.

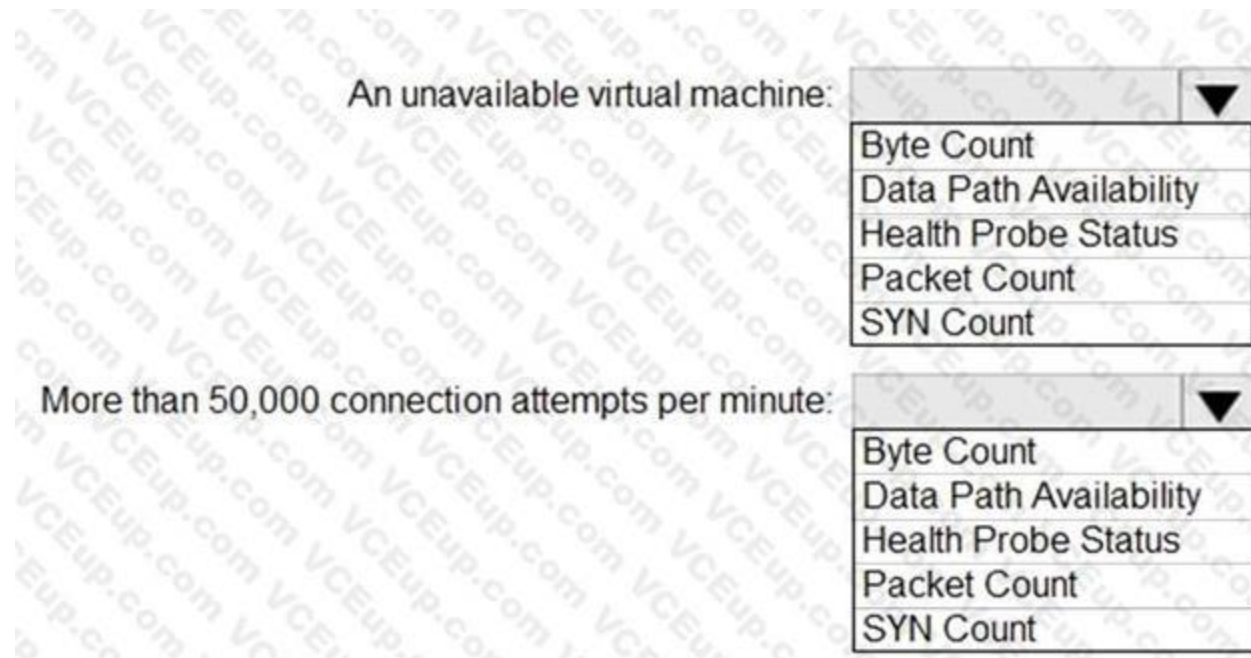
You need to develop a monitoring solution for LB1. The solution must generate an alert when any of the following conditions are met:

A virtual machine is unavailable.

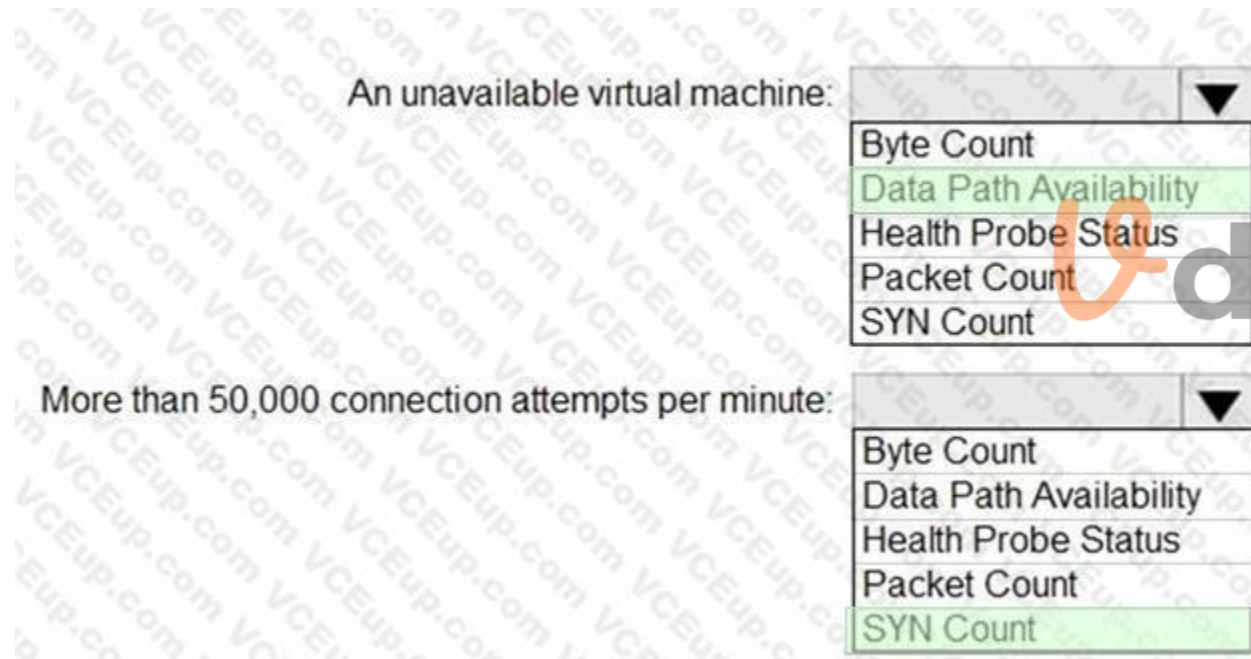
Connection attempts exceed 50,000 per minute.

Which signal should you include in the solution for each condition? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area:



Section:

Explanation:

Box 1: Data path availability

Standard Load Balancer continuously exercises the data path from within a region to the load balancer front end, all the way to the SDN stack that supports your VM. As long as healthy instances remain, the measurement follows the same path as your application's load-balanced traffic. The data path that your customers use is also validated. The measurement is invisible to your application and does not interfere with other operations. Note: Load balancer distributes inbound flows that arrive at the load balancer's front end to backend pool instances. These flows are according to configured load-balancing rules and health probes. The backend pool instances can be Azure Virtual Machines or instances in a virtual machine scale set.

Box 2: SYN count

SYN (synchronize) count: Standard Load Balancer does not terminate Transmission Control Protocol

(TCP) connections or interact with TCP or UDP packet flows. Flows and their handshakes are always between the source and the VM instance. To better troubleshoot your TCP protocol scenarios, you can make use of SYN packets counters to understand how many TCP connection attempts are made.

The metric reports the number of TCP SYN packets that were received.

Reference:

<https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-standard-diagnostics>

QUESTION 29

HOTSPOT

Your company deploys several Linux and Windows virtual machines (VMs) to Azure. The VMs are deployed with the Microsoft Dependency Agent and the Microsoft Monitoring Agent installed by using Azure VM extensions. On-premises connectivity has been enabled by using Azure ExpressRoute.

You need to design a solution to monitor the VMs.

Which Azure monitoring services should you use? To answer, select the appropriate Azure monitoring services in the answer area. NOTE: Each correct selection is worth one point.

Hot Area:

| Scenario | Azure Monitoring Service |
|--|--|
| Analyze Network Security Group (NSG) flow logs for VMs attempting internet access. | <input type="checkbox"/> Azure Network Watcher <input type="checkbox"/> Azure ExpressRoute Monitor <input type="checkbox"/> Azure Service Endpoint Monitor <input type="checkbox"/> Azure DNS Analytics |
| Visualize the VMs with their different processes and dependencies on other computers and external processes. | <input type="checkbox"/> Azure Service Map <input type="checkbox"/> Azure Activity Log <input type="checkbox"/> Azure Service Health <input type="checkbox"/> Azure Advisor |

Answer Area:

| Scenario | Azure Monitoring Service |
|--|---|
| Analyze Network Security Group (NSG) flow logs for VMs attempting internet access. | <input checked="" type="checkbox"/> Azure Network Watcher <input type="checkbox"/> Azure ExpressRoute Monitor <input type="checkbox"/> Azure Service Endpoint Monitor <input type="checkbox"/> Azure DNS Analytics |
| Visualize the VMs with their different processes and dependencies on other computers and external processes. | <input checked="" type="checkbox"/> Azure Service Map <input type="checkbox"/> Azure Activity Log <input type="checkbox"/> Azure Service Health <input type="checkbox"/> Azure Advisor |

Section:

Explanation:

Box 1: Azure Network Watcher

Traffic Analytics is a cloud-based solution that provides visibility into user and application activity in cloud networks. Traffic analytics analyzes Network Watcher network security group (NSG) flow logs to provide insights into traffic flow in your Azure cloud. With traffic analytics, you can:

Identify security threats to, and secure your network, with information such as open-ports, applications attempting internet access, and virtual machines (VM) connecting to rogue networks. Visualize network activity across your Azure subscriptions and identify hot spots.

Understand traffic flow patterns across Azure regions and the internet to optimize your network deployment for performance and capacity. Pinpoint network misconfigurations leading to failed connections in your network.

Box 2: Azure Service Map

Service Map automatically discovers application components on Windows and Linux systems and maps the communication between services. With Service Map, you can view your servers in the way that you think of them: as interconnected systems that deliver critical services. Service Map shows connections between servers, processes, inbound and outbound connection latency, and ports across any TCP-connected

architecture, with no configuration required other than the installation of an agent.

Reference:

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

<https://docs.microsoft.com/en-us/azure/azure-monitor/insights/service-map>

QUESTION 30

HOTSPOT

You manage a database environment for a Microsoft Volume Licensing customer named Contoso, Ltd. Contoso uses License Mobility through Software Assurance. You need to deploy 50 databases. The solution must meet the following requirements:

Support automatic scaling.

Minimize Microsoft SQL Server licensing costs.

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:

Purchase model:

| |
|--|
| DTU |
| vCore |
| Azure reserved virtual machine instances |

Deployment option:

| |
|---|
| An Azure SQL managed instance |
| An Azure SQL Database elastic pool |
| A SQL Server Always On availability group |

Answer Area:

Purchase model:

| |
|--|
| DTU |
| vCore |
| Azure reserved virtual machine instances |

Deployment option:

| |
|---|
| An Azure SQL managed instance |
| An Azure SQL Database elastic pool |
| A SQL Server Always On availability group |

Section:

Explanation:

Box 1: vCore

Virtual core (vCore)-based purchasing model (recommended). This purchasing model provides a choice between a provisioned compute tier and a serverless compute tier. With the provisioned compute tier, you choose the exact amount of compute resources that are always provisioned for your workload. With the serverless compute tier, you specify the autoscaling of the compute resources over a configurable compute

range Box 2: An Azure SQL Database Elastic pool Azure SQL Database provides the following deployment options for a database:

Single database represents a fully managed, isolated database.

Elastic pool is a collection of single databases with a shared set of resources, such as CPU or memory. Single databases can be moved into and out of an elastic pool.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-sql/database/purchasing-models>

QUESTION 31

HOTSPOT

You plan to deploy a custom database solution that will have multiple instances as shown in the following table.

| Host virtual machine | Azure Availability Zone | Azure region |
|----------------------|-------------------------|--------------|
| USDB1 | 1 | US East |
| USDB2 | 2 | US East |
| USDB3 | 3 | US East |
| EUDB1 | 1 | West Europe |
| EUDB2 | 2 | West Europe |
| EUDB3 | 3 | West Europe |

Client applications will access database servers by using db.contoso.com.

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

Access to at least one database server must be maintained in the event of a regional outage.

The virtual machines must not connect to the internet directly.

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:

Global load balancing service:

▼

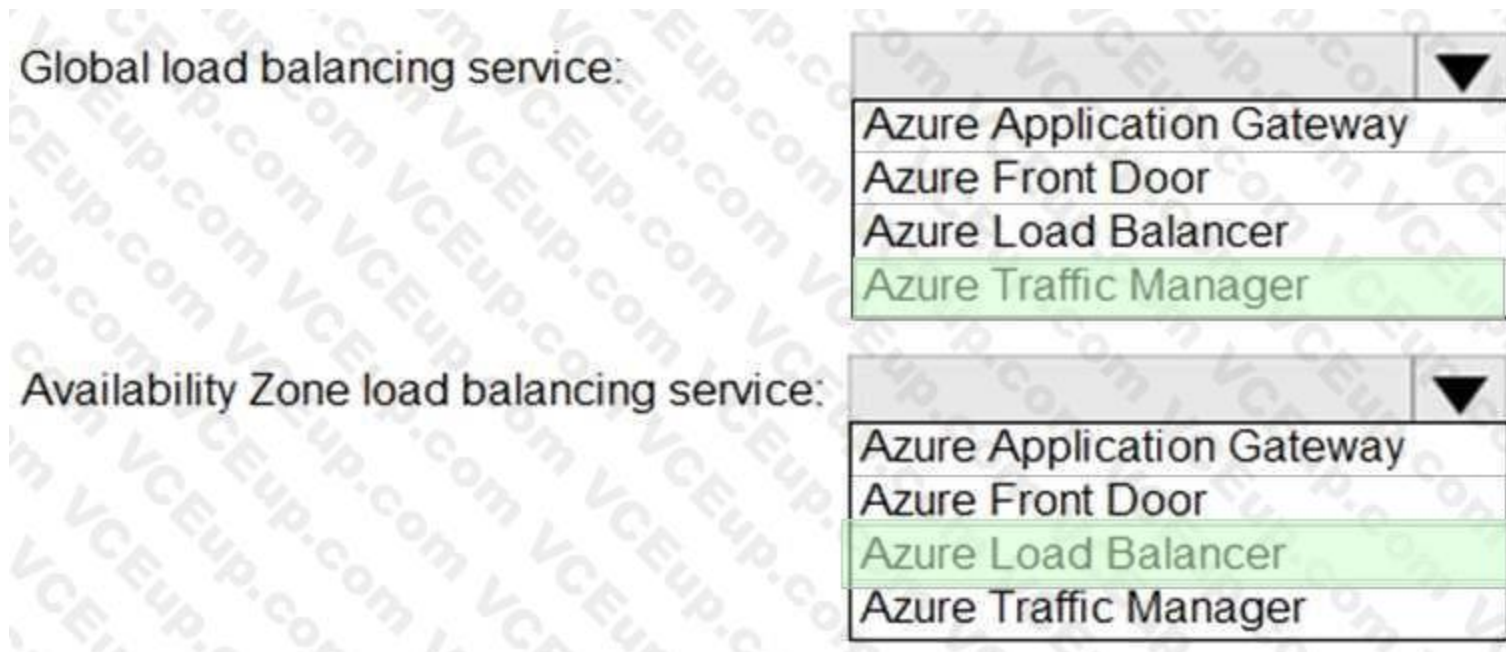
- Azure Application Gateway
- Azure Front Door
- Azure Load Balancer
- Azure Traffic Manager

Availability Zone load balancing service:

▼

- Azure Application Gateway
- Azure Front Door
- Azure Load Balancer
- Azure Traffic Manager

Answer Area:



Section:

Explanation:

Box 1: Azure Traffic Manager

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. Because Traffic Manager is a DNS-based load-balancing service, it load balances only at the domain level. For that reason, it can't fail over as quickly as Front Door, because of common challenges around DNS caching and systems not honoring DNS TTLs.

| Service | Global/regional | Recommended traffic |
|---------------------|-----------------|---------------------|
| Azure Front Door | Global | HTTP(S) |
| Traffic Manager | Global | ncn-HTTP(S) |
| Application Gateway | Regional | HTTP(S) |
| Azure Load Balancer | Regional | ncn-HTTP(S) |



Reference:

<https://docs.microsoft.com/en-us/azure/architecture/guide/technology-choices/load-balancingoverview>

QUESTION 32

HOTSPOT

You have a resource group named RG1 that contains the objects shown in the following table.

| Name | Type | Location |
|---------|------------------|-------------|
| ASP-RG1 | App Service plan | East US |
| KV1 | Azure Key Vault | East US |
| KV2 | Azure Key Vault | West Europe |
| App1 | Azure Logic Apps | West US |

You need to configure permissions so that App1 can copy all the secrets from KV1 to KV2. App1 currently has the Get permission for the secrets in KV1. Which additional permissions should you assign to App1? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Hot Area:

Permission to assign so that App1 can copy the secrets from KV1:

- Add
- Backup
- Create
- List
- Unwrap Key

Permission to assign so that App1 can copy the secrets to KV2:

- Create
- Import
- List
- Wrap Key

Answer Area:

Permission to assign so that App1 can copy the secrets from KV1:

- Add
- Backup
- Create
- List
- Unwrap Key

Permission to assign so that App1 can copy the secrets to KV2:

- Create
- Import
- List
- Wrap Key

Section:

Explanation:

Box 1: List

Get: Gets the specified Azure key vault.

List: The List operation gets information about the vaults associated with the subscription.

Box 2: Create

Create Or Update: Create or update a key vault in the specified subscription.

Reference:

<https://docs.microsoft.com/en-us/rest/api/keyvault/>

Vdumps

QUESTION 33

HOTSPOT

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

You plan to use Azure Monitor to monitor user sign-ins and generate alerts based on specific user sign-in events. You need to recommend a solution to trigger the alerts based on the events.

What should you include in the recommendation? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Hot Area:

Send Azure AD logs to:

| | |
|--------------------------|----------------------------------|
| <input type="checkbox"/> | An Azure event hub |
| <input type="checkbox"/> | An Azure Log Analytics workspace |
| <input type="checkbox"/> | An Azure Storage account |

Signal type to use for triggering the alerts:

| | |
|--------------------------|--------------|
| <input type="checkbox"/> | Activity log |
| <input type="checkbox"/> | Log |
| <input type="checkbox"/> | Metric |

Answer Area:

Send Azure AD logs to:

| | |
|-------------------------------------|----------------------------------|
| <input checked="" type="checkbox"/> | An Azure event hub |
| <input checked="" type="checkbox"/> | An Azure Log Analytics workspace |
| <input type="checkbox"/> | An Azure Storage account |

Signal type to use for triggering the alerts:

| | |
|-------------------------------------|--------------|
| <input type="checkbox"/> | Activity log |
| <input checked="" type="checkbox"/> | Log |
| <input type="checkbox"/> | Metric |

Section:

Explanation:

Box 1: An Azure Log Analytics workspace

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

Note: You can forward your AAD logs and events to either an Azure Storage Account, an Azure Event Hub, Log Analytics, or a combination of all of these. Box 2: Log

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

Reference:

<https://4sysops.com/archives/how-to-create-an-azure-ad-admin-login-alert/>

<https://docs.microsoft.com/en-us/azure/azure-monitor/platform/alerts-log>

QUESTION 34

HOTSPOT

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

Add OAuth2 service
API Management service

Display name *
Unique name used to reference this authorization server on...

Id *
[Empty field with a checkmark]

Description
Authorization server description

Client registration page URL *
https://contoso.com/register [checkmark]

Authorization grant types

- Authorization code
- Implicit
- Resource owner password
- Client credentials

Authorization endpoint URL *
https://login.microsoftonline.com/contosoonmicrosoft.com... [checkmark]

Support state parameter

Authorization request method

- GET
- POST

Token endpoint URL *
Token endpoint is used by clients to obtain access tokens in...

Create



Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic. NOTE: Each correct selection is worth one point.

Hot Area:

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

- Background services
- Headless device authentication
- Web applications

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

- Client credentials
- Resource owner password
- Support state parameter

Answer Area:

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

- Background services
- Headless device authentication
- Web applications

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

- Client credentials
- Resource owner password
- Support state parameter

Section:

Explanation:

Box 1: Web applications

The Authorization Code Grant Type is used by both web apps and native apps to get an access token after a user authorizes an app. Note: The Authorization Code grant type is used by confidential and public clients to exchange an authorization code for an access token. After the user returns to the client via the redirect URL, the application will get the authorization code from the URL and use it to request an access token.

Incorrect Answers:

Not Headless device authentication:

A headless system is a computer that operates without a monitor, graphical user interface (GUI) or peripheral devices, such as keyboard and mouse. Headless computers are usually embedded systems in various devices or servers in multi-server data center environments. Industrial machines, automobiles, medical equipment, cameras, household appliances, airplanes, vending machines and toys are among the myriad possible hosts of embedded systems.

Box 2: Client Credentials

How to include additional client data

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

POST /c2id/clients HTTP/1.1

Host: demo.c2id.com

Content-Type: application/json

Authorization: Bearer ztucZS1ZyFKgh0tUEruUtiSTXhnexmd6

```
{
  "redirect_uris" : [ "https://myapp.example.com/callback" ],
  "data" : { "reg_type" : "3rd-party",
  "approved" : true,
  "author_id" : 792440 }
}
```

The data parameter permits arbitrary content packaged in a JSON object. To set it you will need the master registration token or a one-time access token with a client-reg:data scope. Incorrect Answers:
Authorization protocols provide a state parameter that allows you to restore the previous state of your application. The state parameter preserves some state object set by the client in the Authorization request and makes it available to the client in the response.

Reference:

<https://developer.okta.com/blog/2018/04/10/oauth-authorization-code-grant-type>

<https://connect2id.com/products/server/docs/guides/client-registration>

QUESTION 35

HOTSPOT

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

Prevent new data from being modified for one year.

Minimize read latency.

Maximize data resiliency.

You need to recommend a storage solution for the app.

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

Hot Area:

Azure Storage account kind:

| |
|------------------|
| StorageV2 |
| BlobStorage |
| BlockBlobStorage |

Replication:

| |
|--|
| Zone-redundant storage (ZRS) |
| Locally-redundant storage (LRS) |
| Read-access geo-redundant storage (RA-GRS) |

Answer Area:

Azure Storage account kind:

| |
|------------------|
| StorageV2 |
| BlobStorage |
| BlockBlobStorage |

Replication:

| |
|--|
| Zone-redundant storage (ZRS) |
| Locally-redundant storage (LRS) |
| Read-access geo-redundant storage (RA-GRS) |

Section:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/storage/common/storage-account-overview>
<https://docs.microsoft.com/en-us/azure/storage/common/storageredundancy?toc=/azure/storage/blobs/toc.json>

QUESTION 36

HOTSPOT

You have the Free edition of a hybrid Azure Active Directory (Azure AD) tenant. The tenant uses password hash synchronization. You need to recommend a solution to meet the following requirements:
Prevent Active Directory domain user accounts from being locked out as the result of brute force attacks targeting Azure AD user accounts. Block legacy authentication attempts to Azure AD integrated apps.
Minimize costs.

What should you recommend for each requirement? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Hot Area:

To protect against brute force attacks:

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

To block legacy authentication attempts:

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

Answer Area:

To protect against brute force attacks:

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

To block legacy authentication attempts:

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

Section:

Explanation:

Box 1: Smart lockout

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

Box 2: Conditional access policies
If your environment is ready to block legacy authentication to improve your tenant's protection, you can accomplish this goal with Conditional Access. How can you prevent apps using legacy authentication from accessing your tenant's resources? The recommendation is to just block them with a Conditional Access policy. If necessary, you allow only certain users and specific network locations to use apps that are based on legacy authentication.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-password-smartlockout>

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/block-legacyauthentication>

QUESTION 37

HOTSPOT

You need to implement the Azure RBAC role assignment. The solution must meet the authentication and authorization requirements. How many assignment should you configure for the Network Contributor role for Role1? To answer, select appropriate in the answer area.

Hot Area:

Answer Area



Answer Area:



Section:

Explanation:



QUESTION 38

DRAG DROP

You have an on-premises network that uses on IP address space of 172.16.0.0/16 You plan to deploy 25 virtual machines to a new azure subscription. You identify the following technical requirements.

All Azure virtual machines must be placed on the same subnet subnet1.

All the Azure virtual machines must be able to communicate with all on premises servers.

The servers must be able to communicate between the on-premises network and Azure by using a site to site VPN. You need to recommend a subnet design that meets the technical requirements.

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

NOTE: Each correct selection is worth one point.



Select and Place:

| Network Addresses | Answer Area |
|-------------------|--|
| 172.16.0.0/16 | Subnet1: <input type="text" value="Network address"/> |
| 172.16.1.0/28 | Gateway subnet: <input type="text" value="Network address"/> |
| 192.168.0.0/24 | |
| 192.168.1.0/28 | |

Correct Answer:

| Network Addresses | Answer Area |
|-------------------|--------------------------------|
| 172.16.0.0/16 | Subnet1: 192.168.0.0/24 |
| 172.16.1.0/28 | Gateway subnet: 192.168.1.0/28 |
| | |
| | |

Section:

Explanation:

QUESTION 39

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:

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 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. 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:

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 41

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:

Explanation:

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



QUESTION 42

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:

Explanation:

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

QUESTION 43

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:

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 44

You have an Azure subscription that contains a Basic Azure virtual WAN named VirtualWAN1 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:

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 45

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:

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 46

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 on-premises Active Directory domain. You plan to migrate Server1 to a virtual machine in Subscription1.

A company security policy states that the virtual machines and services deployed to Subscription1 must be prevented from accessing the on-premises network. You need to recommend a solution to ensure that 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:

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 47

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:

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 48

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 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:

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 49

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:

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 50

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:

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 51

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:

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 52

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: B

Section:

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 53

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:

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 54

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:

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-your-azure-migration>

QUESTION 55

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:

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 56

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:

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 57

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:

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 58

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:

Explanation:

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

QUESTION 59

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:

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 60

DRAG DROP

Your company identifies the following business continuity and disaster recovery objectives for virtual machines that host sales, finance, and reporting application in the company's on-premises data center. •The finance application requires that data be retained for seven years. In the event of a disaster, the application must be able to run from Azure. The recovery in objective (RTO) is 10 minutes,

- The reporting application must be able to recover point in-time data at a daily granularity. The RTO is eight hours.
- The sales application must be able to fail over to second on-premises data center.

You need to recommend which Azure services meet the business continuity and disaster recovery objectives. The solution must minimize costs. What should you recommend for each application? To answer, drag the appropriate services to the correct application. Each service may be used once or more than once. You may need to drag the spin bar between panes or scroll to view content.

Select and Place:



| Actions | Answer Area |
|--------------------------------------|--------------------------------|
| Azure Backup only | Sales: Service or Services |
| Azure Site Recovery only | Finance: Service or Services |
| Azure Site Recovery and Azure Backup | Reporting: Service or Services |

Correct Answer:

| Actions | Answer Area |
|---------|---|
| | Sales: Azure Site Recovery only |
| | Finance: Azure Site Recovery and Azure Backup |
| | Reporting: Azure Backup only |

Section:

Explanation:

- 1) Sales: Azure Site Recovery only
- 2) Finance: Azure Site Recovery and Azure Backup
- 3) Reporting: Azure Backup only



QUESTION 61

HOTSPOT

Your company deploys an Azure App Service Web App.

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

You need to improve the performance of the application.

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

NOTE: Each correct selection is worth one point.

Hot Area:

| Scenario | Solution |
|---|---|
| Store content close to end users. | <div style="border: 1px solid black; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px; display: flex; justify-content: space-between; align-items: center;"> ▼ </div> <div style="padding: 2px;"> <ul style="list-style-type: none"> Azure Redis Cache Azure Traffic Manager Azure Content Delivery Network Azure Application Gateway </div> </div> |
| Store content close to the application. | <div style="border: 1px solid black; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px; display: flex; justify-content: space-between; align-items: center;"> ▼ </div> <div style="padding: 2px;"> <ul style="list-style-type: none"> Azure Redis Cache Azure Traffic Manager Azure Content Delivery Network Azure Application Gateway </div> </div> |

Answer Area:

| Scenario | Solution |
|---|--|
| Store content close to end users. | <div style="border: 1px solid black; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px; display: flex; justify-content: space-between; align-items: center;"> ▼ </div> <div style="padding: 2px;"> <ul style="list-style-type: none"> Azure Redis Cache Azure Traffic Manager <li style="background-color: #e0ffe0;">Azure Content Delivery Network Azure Application Gateway </div> </div> |
| Store content close to the application. | <div style="border: 1px solid black; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px; display: flex; justify-content: space-between; align-items: center;"> ▼ </div> <div style="padding: 2px;"> <ul style="list-style-type: none"> <li style="background-color: #e0ffe0;">Azure Redis Cache Azure Traffic Manager Azure Content Delivery Network Azure Application Gateway </div> </div> |

Section:

Explanation:

Box 1: Content Delivery Network

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

Azure Content Delivery Network (CDN) offers developers a global solution for rapidly delivering highbandwidth content to users by caching their content at strategically placed physical nodes across the world.

Azure CDN can also accelerate dynamic content, which cannot be cached, by leveraging various network optimizations using CDN POPs. For example, route optimization to bypass Border Gateway Protocol (BGP).

Box 2: Azure Redis Cache

Azure Cache for Redis is based on the popular software Redis. It is typically used as a cache to improve the performance and scalability of systems that rely heavily on backend data-stores. Performance is improved

by temporarily copying frequently accessed data to fast storage located close to the application. With Azure Cache for Redis, this fast storage is located in-memory with Azure Cache for Redis instead of being loaded from disk by a database.

Reference:

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

QUESTION 62

HOTSPOT

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

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

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

Be available if a single Azure datacenter fails.

Support storage tiers.

Minimize cost.

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

Hot Area:

Account type:

| |
|--------------------------------|
| Blob storage |
| Storage (general purpose v1) |
| StorageV2 (general purpose v2) |

Replication solution:

| |
|--|
| Geo-redundant storage (GRS) |
| Zone-redundant storage (ZRS) |
| Locally-redundant storage (LRS) |
| Read-access geo-redundant storage (RA-GRS) |

Answer Area:

Account type:

- Blob storage
- Storage (general purpose v1)
- StorageV2 (general purpose v2)

Replication solution:

- Geo-redundant storage (GRS)
- Zone-redundant storage (ZRS)
- Locally-redundant storage (LRS)
- Read-access geo-redundant storage (RA-GRS)

Section:

Explanation:

Account Type: StorageV2

Replication solution: Zone-redundant storage (ZRS)

QUESTION 63

DRAG DROP

You are designing a virtual machine that will run Microsoft SQL Server and will contain two data disks. The first data disk will store log files, and the second data disk will store data. Both disks are P40 managed disks. You need to recommend a caching policy for each disk. The policy must provide the best overall performance for the virtual machine. Which caching policy should you recommend for each disk? To answer, drag the appropriate policies to the correct disks. Each policy may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:

| Policies | Answer Area |
|-----------|--------------|
| None | Log: Policy |
| ReadOnly | Data: Policy |
| ReadWrite | |

Correct Answer:

Policies

Answer Area

Log: None

Data: ReadOnly

ReadWrite

Section:

Explanation:

Reference:

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

QUESTION 64

DRAG DROP

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

Two virtual machines that will run Microsoft SQL Server 2016, will be deployed to different data centers in the same Azure region, and will be part of an Always On availability group. SQL Server data that will be backed up by using the Automated Backup feature of the SQL Server IaaS Agent Extension (SQLIaaSExtension) You identify the storage priorities for various data types as shown in the following table.

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

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

NOTE: Each correct selection is worth one point.

Select and Place:

Storage Types

Answer Area

Operating system:

Databases and logs:

Backups:

A geo-redundant storage (GRS) account

A locally-redundant storage (LRS) account

A premium managed disk

A standard managed disk

Correct Answer:

| Storage Types | Answer Area |
|---|--|
| A geo-redundant storage (GRS) account | Operating system: A premium managed disk |
| A locally-redundant storage (LRS) account | Databases and logs: A premium managed disk |
| A premium managed disk | Backups: A locally-redundant storage (LRS) account |
| A standard managed disk | |

Section:

Explanation:

QUESTION 65

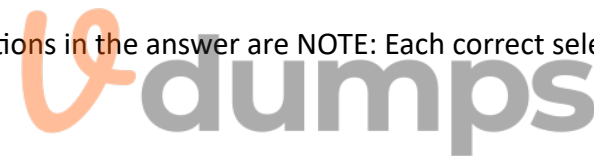
HOTSPOT

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

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

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

What should you include in the solution? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



Hot Area:

Level at which to define the blueprints:

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

Level at which to create the blueprint assignments:

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

Answer Area:

Level at which to define the blueprints:

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

Level at which to create the blueprint assignments:

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

Section:

Explanation:

Reference: <https://docs.microsoft.com/en-us/azure/governance/blueprints/create-blueprint-portal> Assign a blueprint After a blueprint has been published, it can be assigned to a subscription. Assign the blueprint that you created to one of the subscriptions under your management group hierarchy.

If the blueprint is saved to a subscription, it can only be assigned to that subscription

QUESTION 66

HOTSPOT

You are designing a cost-optimized solution that uses Azure Batch to run two types of jobs on Linux nodes. The first job type will consist of short-running tasks for a development environment. The second job type will consist of long-running Message Passing Interface (MPI) applications for a production environment that requires timely job completion. You need to recommend the pool type and node type for each job type. The solution must minimize compute charges and leverage Azure Hybrid Benefit whenever possible. What should you recommend? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

First job: User subscription and low-priority virtual machines
Batch service and dedicated virtual machines
User subscription and dedicated virtual machines
User subscription and low-priority virtual machines

Second job: Batch service and dedicated virtual machines
Batch service and dedicated virtual machines
User subscription and dedicated virtual machines
User subscription and low-priority virtual machines

Answer Area:

Answer Area

First job: User subscription and low-priority virtual machines
Batch service and dedicated virtual machines
User subscription and dedicated virtual machines
User subscription and low-priority virtual machines

Second job: Batch service and dedicated virtual machines
Batch service and dedicated virtual machines
User subscription and dedicated virtual machines
User subscription and low-priority virtual machines

Section:

Explanation:

QUESTION 67

HOTSPOT

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

The company is developing 10 web apps that will use the web APIs. The web apps and the APIs are registered in the company's Azure AD tenant. The web APIs are published by using Azure API Management. You need to recommend a solution to block unauthorized requests originating from the web apps from reaching the web APIs. The solution must meet the following requirements:

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

What should you include in the recommendation? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area:



Section:

Explanation:

QUESTION 68

You have an Azure AD tenant.

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

You need to recommend a solution to provide specific Azure AD user accounts with read access to the Cosmos DB databases. What should you include in the recommendation?

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

Correct Answer: A

Section:

QUESTION 69

HOTSPOT

You have several Azure App Service web apps that use Azure Key Vault to store data encryption keys. Several departments have the following requests to support the web app:

| Department | Request |
|-------------|--|
| Security | <ul style="list-style-type: none">• Review the membership of administrative roles and require users to provide a justification for continued membership.• Get alerts about changes in administrator assignments.• See a history of administrator activation, including which changes administrators made to Azure resources. |
| Development | <ul style="list-style-type: none">• Enable the applications to access Key Vault and retrieve keys for use in code. |

Which service should you recommend for each department's request? To answer, configure the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

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

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

Quality Assurance: Azure AD Privileged Identity Management
Azure AD Privileged Identity Management
Azure Managed Identity
Azure AD Connect
Azure AD Identity Protection

Answer Area:

Answer Area

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

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

Quality Assurance: Azure AD Privileged Identity Management
Azure AD Privileged Identity Management
Azure Managed Identity
Azure AD Connect
Azure AD Identity Protection

Section:

Explanation:

QUESTION 70

You have an Azure Functions microservice app named Appl that is hosted in the Consumption plan.

App1 uses an Azure Queue Storage trigger.

You plan to migrate App1 to an Azure Kubernetes Service (AKS) cluster.

You need to prepare the AKS cluster to support App1. The solution must meet the following requirements:

- Use the same scaling mechanism as the current deployment.
- Support kubernetes and Azure Container Networking Interface (CNI) networking.

Which two actions should you perform? Each correct answer presents part of the solution. NOTE:

Each correct answer is worth one point.

- A. Configure the horizontal pod autoscaler.
- B. Install Virtual Kubelet.
- C. Configure the AKS cluster autoscaler.
- D. Configure the virtual node add-on.
- E. Install Kubernetes-based Event Driven Autoscaling (KEDA).

Correct Answer: A, D

Section:

QUESTION 71

You plan to migrate on-premises MySQL databases to Azure Database for MySQL Flexible Server.

You need to recommend a solution for the Azure Database for MySQL Flexible Server configuration.

The solution must meet the following requirements:

- The databases must be accessible if a datacenter fails.
- Costs must be minimized.

Which compute tier should you recommend?

- A. Burstable
- B. General Purpose
- C. Memory Optimized
- D. Other option

Correct Answer: C

Section:

QUESTION 72

You have an app named App1 that uses an on-premises Microsoft SQL Server database named DB1.

You plan to migrate DB1 to an Azure SQL managed instance.

You need to enable customer-managed Transparent Data Encryption (TDE) for the instance. The solution must maximize encryption strength.

Which type of encryption algorithm and key length should you use for the TDE protector?

- A. AES256
- B. RSA4096
- C. RSA2048
- D. RSA3072

Correct Answer: D

Section:



QUESTION 73

HOTSPOT

You have an Azure subscription named Sub1 that is linked to an Azure AD tenant named contoso.com.

You plan to implement two ASP.NET Core apps named App1 and App2 that will be deployed to 100 virtual machines in Sub1. Users will sign in to App1 and App2 by using their contoso.com credentials. App1 requires read permissions to access the calendar of the signed-in user. App2 requires write permissions to access the calendar of the signed-in user. You need to recommend an authentication and authorization solution for the apps. The solution must meet the following requirements:

- Use the principle of least privilege.
- Minimize administrative effort

What should you include in the recommendation? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Authentication: Application registration in Azure AD

- Application registration in Azure AD
- A system-assigned managed identity
- A user-assigned managed identity

Authorization: Azure role-based access control (Azure RBAC)

- Application permissions
- Azure role-based access control (Azure RBAC)
- Delegated permissions

Answer Area:

Answer Area

Authentication: Application registration in Azure AD

- Application registration in Azure AD
- A system-assigned managed identity
- A user-assigned managed identity

Authorization: Azure role-based access control (Azure RBAC)

- Application permissions
- Azure role-based access control (Azure RBAC)
- Delegated permissions

Section:

Explanation:

QUESTION 74

You are designing an app that will use Azure Cosmos DB to collate sales data from multiple countries. You need to recommend an API for the app. The solution must meet the following requirements:

- Support SQL queries.
- Support geo-replication.
- Store and access data relationally.

Which API should you recommend?

- A. PostgreSQL
- B. NoSQL
- C. Apache Cassandra

D. MongoDB

Correct Answer: A
Section:

QUESTION 75

HOTSPOT

You have an Azure AD tenant that contains a management group named MG1. You have the Azure subscriptions shown in the following table.

| Name | Management group |
|------|-------------------|
| Sub1 | MG1 |
| Sub2 | MG1 |
| Sub3 | Tenant Root Group |

The subscriptions contain the resource groups shown in the following table.

| Name | Subscription |
|------|--------------|
| RG1 | Sub1 |
| RG2 | Sub2 |
| RG3 | Sub3 |

The subscription contains the Azure AD security groups shown in the following table.

| Name | Member of |
|--------|-----------|
| Group1 | Group3 |
| Group2 | Group3 |
| Group3 | None |

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

| Name | Member of |
|-------|----------------|
| User1 | Group1 |
| User2 | Group2 |
| User3 | Group1, Group2 |

You perform the following actions:

- Assign User3 the Contributor role for Sub1.
- Assign Group1 the Virtual Machine Contributor role for MG1.
- Assign Group3 the Contributor role for the Tenant Root Group.

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

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

| Statements | Yes | No |
|--|-----------------------|-----------------------|
| User1 can create a new virtual machine in RG1. | <input type="radio"/> | <input type="radio"/> |
| User2 can grant permissions to Group2. | <input type="radio"/> | <input type="radio"/> |
| User3 can create a storage account in RG2. | <input type="radio"/> | <input type="radio"/> |

Answer Area:

Answer Area

| Statements | Yes | No |
|--|----------------------------------|----------------------------------|
| User1 can create a new virtual machine in RG1. | <input type="radio"/> | <input checked="" type="radio"/> |
| User2 can grant permissions to Group2. | <input checked="" type="radio"/> | <input type="radio"/> |
| User3 can create a storage account in RG2. | <input checked="" type="radio"/> | <input type="radio"/> |



Section:

Explanation:

QUESTION 76

HOTSPOT

You are designing an app that will be hosted on Azure virtual machines that run Ubuntu. The app will use a third-party email service to send email messages to users. The third-party email service requires that the app authenticate by using an API key.

You need to recommend an Azure Key Vault solution for storing and accessing the API key. The solution must minimize administrative effort. What should you recommend using to store and access the key? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Storage:

Access:

Answer Area:

Answer Area

The image shows a configuration interface with two dropdown menus. The first dropdown is labeled 'Storage:' and has options 'Secret', 'Certificate', and 'Key'. The 'Secret' option is selected and highlighted in green. The second dropdown is labeled 'Access:' and has options 'A managed service identity (MSI)', 'An API token', 'A managed service identity (MSI)', and 'A service principal'. The second 'A managed service identity (MSI)' option is selected and highlighted in green.

Section:

Explanation:

QUESTION 77

Your company deploys several virtual machines on-premises and to Azure. ExpressRoute is 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 from the Azure virtual machines to the on-premises virtual machines. Solution: Use Azure Advisor.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: B

Section:

QUESTION 78

DRAG DROP

You have two app registrations named App1 and App2 in Azure AD. App1 supports role-based access control (RBAC) and includes a role named Writer.

You need to ensure that when App2 authenticates to access App1, the tokens issued by Azure AD include the Writer role claim.

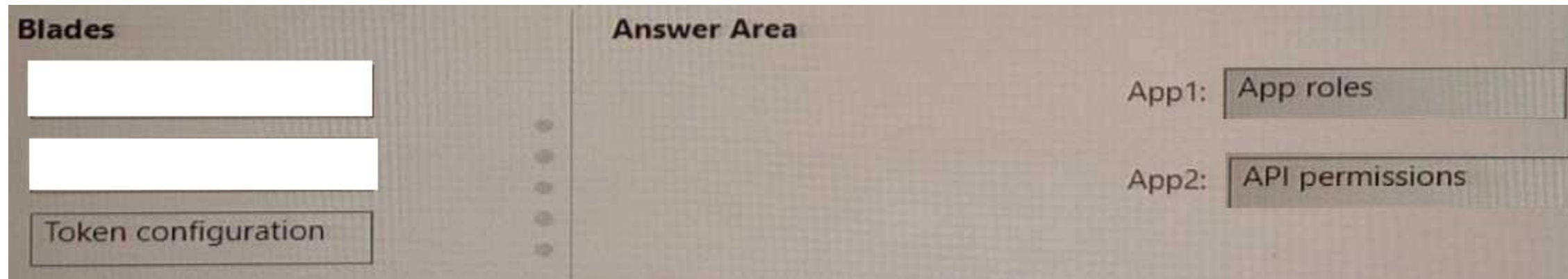
Which blade should you use to modify each app registration? To answer, drag the appropriate blades to the correct app registrations. Each blade may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:

The image shows a drag-and-drop interface. On the left, under the heading 'Blades', there are three boxes: 'API permissions', 'App roles', and 'Token configuration'. On the right, under the heading 'Answer Area', there are two input fields: 'App1:' and 'App2:'. The 'App1:' field is currently empty.

Correct Answer:



Section:

Explanation:

QUESTION 79

You have an Azure subscription that contains 10 web apps. The apps are integrated with Azure AD and are accessed by users on different project teams.

The users frequently move between projects.

You need to recommend an access management solution for the web apps. The solution must meet the following requirements:

- The users must only have access to the app of the project to which they are assigned currently.
- Project managers must verify which users have access to their project's app and remove users that are no longer assigned to their project.
- Once every 30 days, the project managers must be prompted automatically to verify which users are assigned to the projects.

What should you include in the recommendation?

- A. Microsoft Defender for Identity
- B. Azure AD Identity Governance
- C. Microsoft Entra Permissions Management
- D. Azure AD Identity Protection

Correct Answer: B

Section:

