ATMIC NETWORKS
YOUR GUIDE TO GLOBAL CERTIFIATION

"Please note that these files may not be up to date. However, the questions will help you understand the exam format and typical question patterns."

www.atmicnetworks .com

Warning: Keep connected with our support team for latest updates

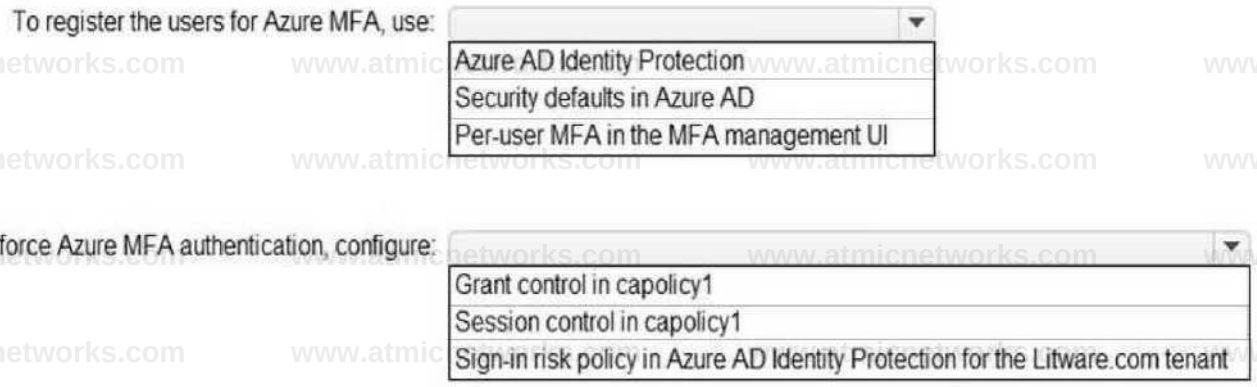
Question: 1

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.

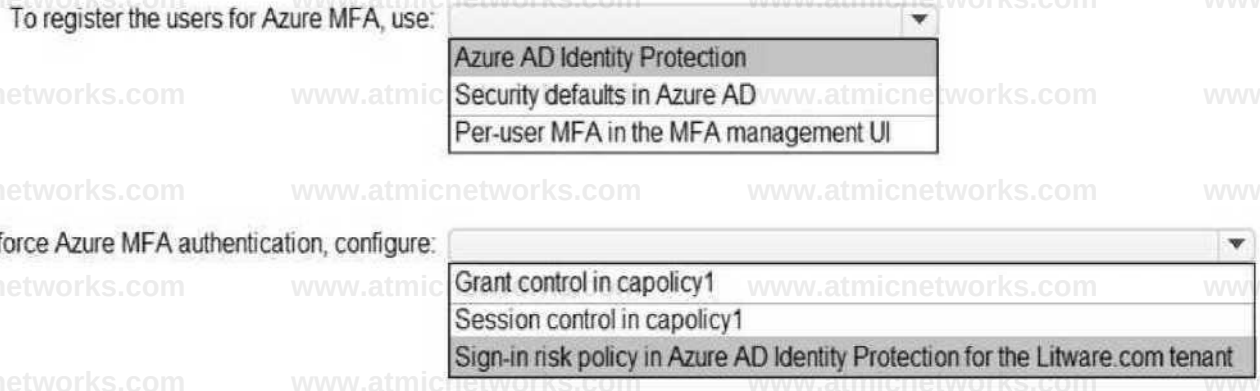
What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer:

Explanation:



Box 1: Azure AD Identity Protection

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

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

Box 2: Sign-in risk policy...

Scenario: The Litware.com tenant has a conditional access policy named capolicy1. Capolicy1

requires that when users manage the Azure subscription for a production environment by using the Azure portal, they must connect from a hybrid Azure AD-joined device.

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

Sign-in risk policy
User risk policy

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

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

Question: 2

You plan to migrate App1 to Azure.

You need to recommend a network connectivity solution for the Azure Storage account that will host the App1 dat

a. 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

Answer: A

Explanation:

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

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

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

Question: 3

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

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

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

Answer: D

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-azure- resources/overview

Question: 4

DRAG DROP

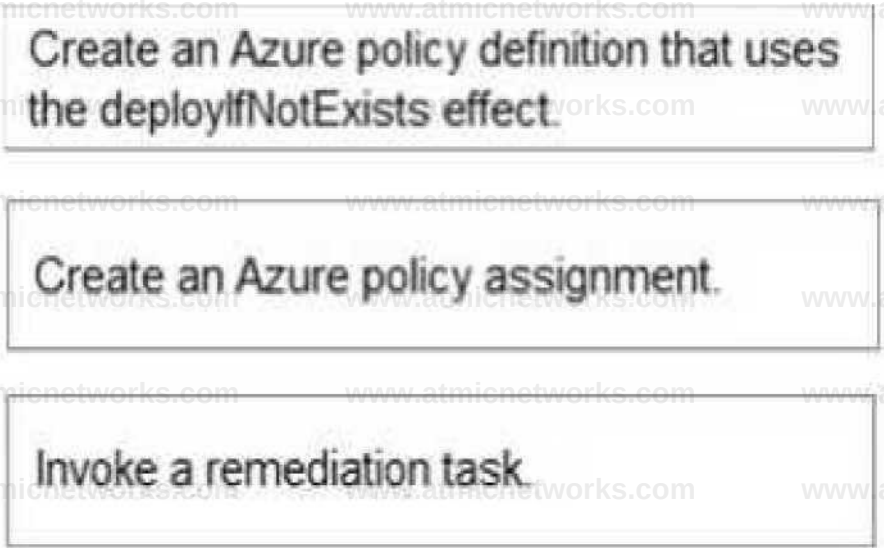
You need to configure an Azure policy to ensure that the Azure SQL databases have TDE enabled. The solution must meet the security and compliance requirements.

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.

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	

Answer:

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.

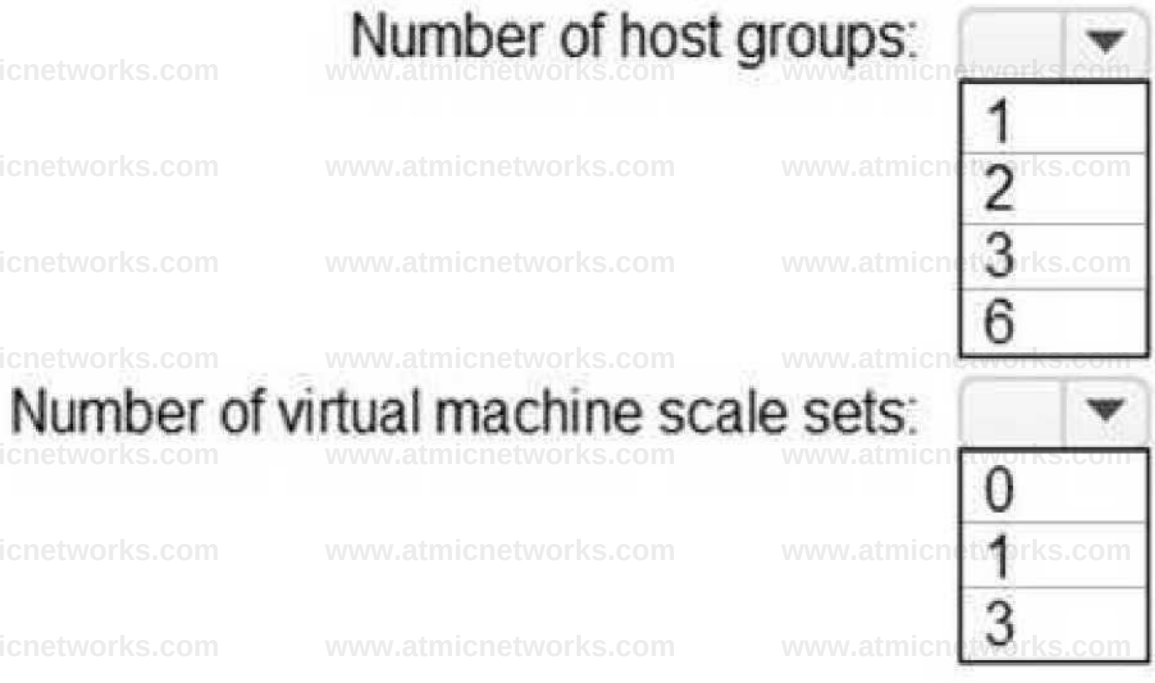
Reference:
https://docs.microsoft.com/en-us/azure/governance/policy/how-to/remediate-resources

Question: 5
HOTSPOT

You plan to migrate App1 to Azure.

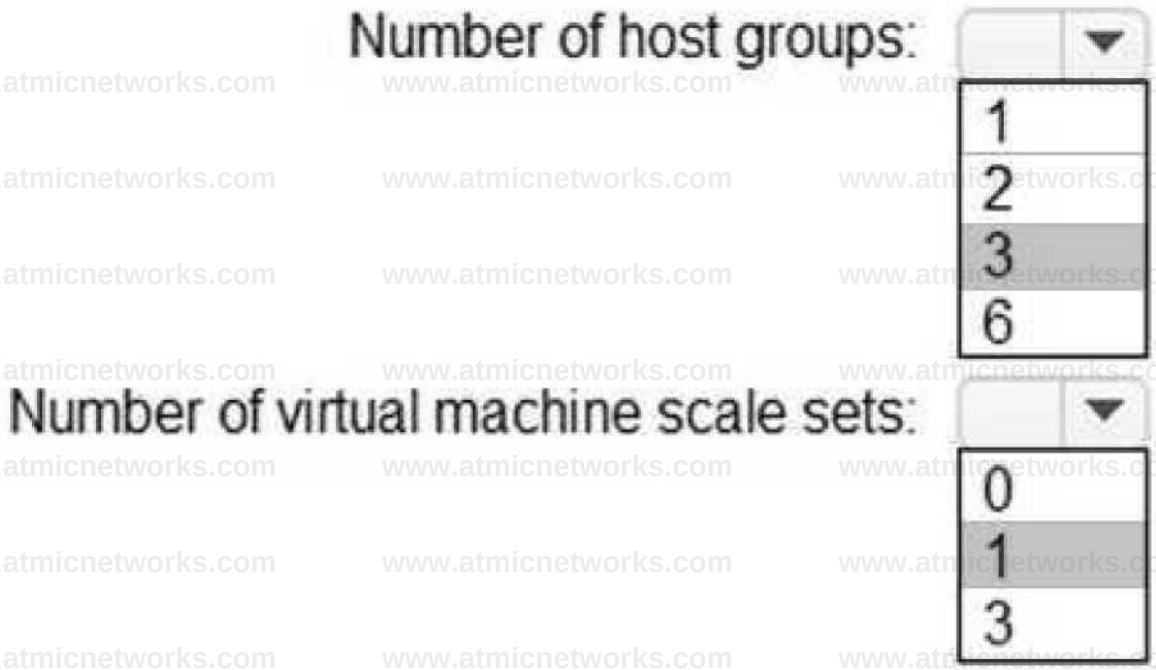
You need to recommend a high-availability solution for App1. The solution must meet the resiliency requirements.

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.



Answer:

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
Scenario: App1 must meet the following requirements:
Be hosted on Azure virtual machines that support automatic scaling.

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

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

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

Question: 6
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.

To estimate the costs, use

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

Implement:

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

Answer:

Explanation:

To estimate the costs, use:

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

Implement:

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

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

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

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

Box 2: Azure Hybrid Benefit

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

Scenario:
Litware identifies the following security and compliance requirements:

Once App1 is migrated to Azure, you must ensure that new data can be written to the app, and the modification of new and existing data is prevented for a period of three years.
On-premises users and services must be able to access the Azure Storage account that will host the data in App1.
Access to the public endpoint of the Azure Storage account that will host the App1 data must be prevented.
All Azure SQL databases in the production environment must have Transparent Data Encryption (TDE) enabled.
App1 must not share physical hardware with other workloads.

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

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

Question: 7
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.

Storage account type:

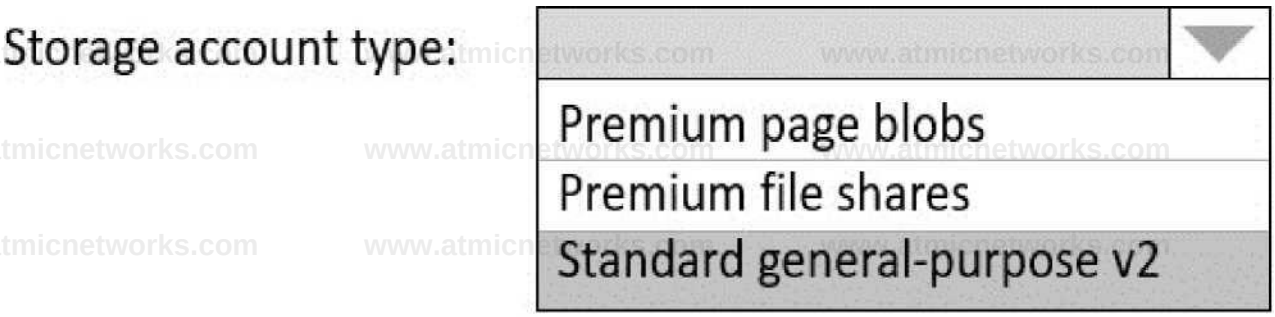
Premium page blobs
Premium file shares
Standard general-purpose v2

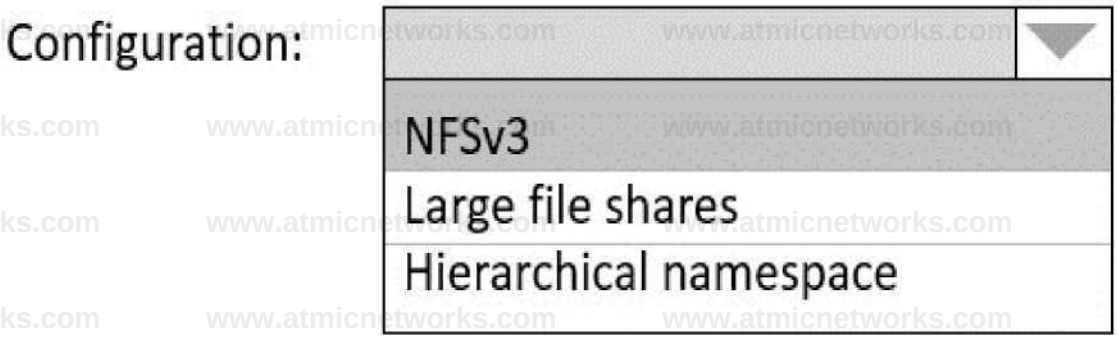
Configuration:

NFSv3
Large file shares
Hierarchical namespace

Answer:

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: 8

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.

Answer: B

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: 9

HOTSPOT

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

Database:

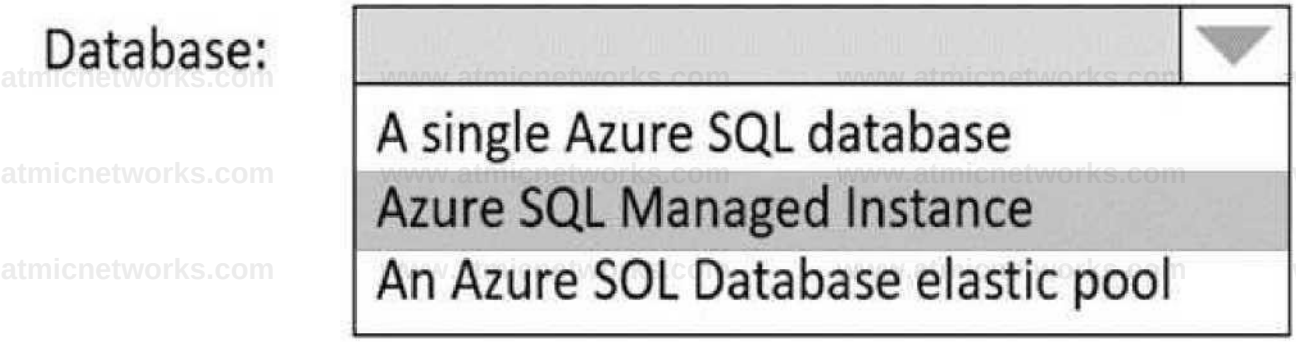
- A single Azure SQL database
- Azure SQL Managed Instance
- An Azure SOL Database elastic pool

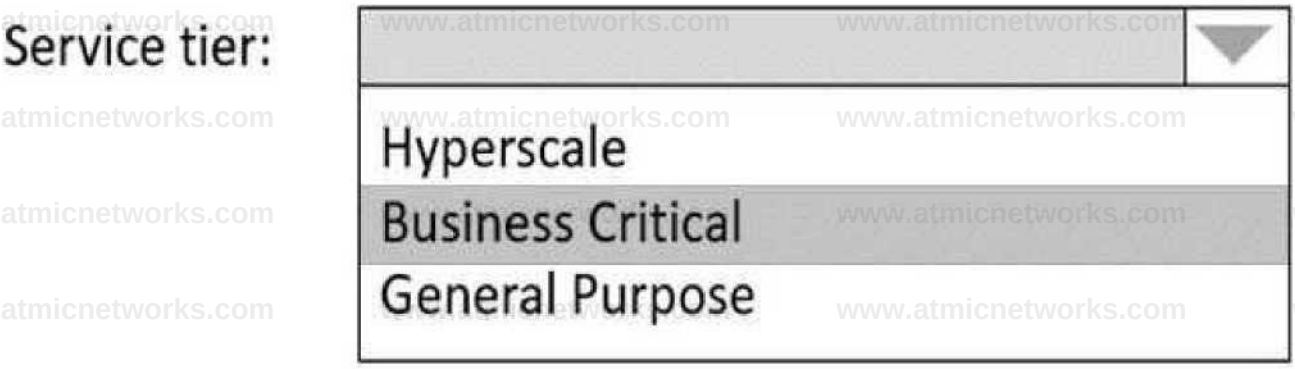
Service tier:

- Hyperscale
- Business Critical
- General Purpose

Answer:

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 geo-replication feature, designed to simplify deployment and management of geo-replicated databases at scale. You can initiate a geo-failover manually or you can delegate it to the Azure service based on a user-defined policy. The latter option allows you to automatically recover multiple related databases in a secondary region after a catastrophic failure or other unplanned event that results in full or partial loss of the SQL Database or SQL Managed Instance availability in the primary region.

Box 2: Business critical

SQL Managed Instance is available in two service tiers:

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

Reference:

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

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

Question: 10

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

Answer: B

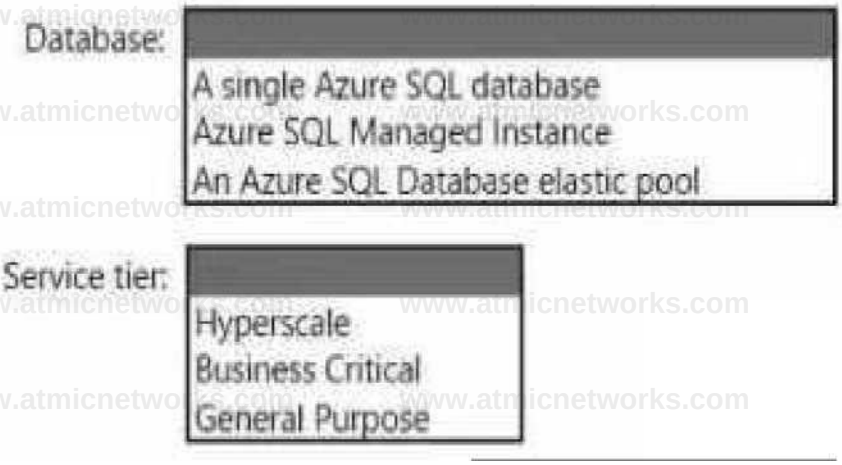
Explanation:

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

Question: 11

HOTSPOT
You plan to migrate DB1 and DB2 to Azure.
You need to ensure that the Azure database and the service tier meet the resiliency and business requirements.
What should you configure? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area



Answer:

Explanation:

Answer Area

Database: Azure SQL Managed instance

Service Her General Purpose

Question: 12

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

What should you do?

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

Answer: B

Explanation:

Topic 2, Fabrikam inc Case Study A

Overview:

Existing Environment

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

Active Directory Environment:

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

Network Infrastructure:

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

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

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

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

Problem Statement:

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

Requirements:

Planned Changes:

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

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

All R&D operations will remain on-premises.

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

Technical Requirements:

Fabrikam identifies the following technical requirements:

- Web site content must be easily updated from a single point.
- User input must be minimized when provisioning new app instances.
- Whenever possible, existing on premises licenses must be used to reduce cost.
- Users must always authenticate by using their corp.fabrikam.com UPN identity.
- Any new deployments to Azure must be redundant in case an Azure region fails.
- Whenever possible, solutions must be deployed to Azure by using platform as a service (PaaS).
- An email distribution group named IT Support must be notified of any issues relating to the directory synchronization services.
- Directory synchronization between Azure Active Directory (Azure AD) and corp.fabhkam.com must not be affected by a link failure between Azure and the on premises network.

Database Requirements:

Fabrikam identifies the following database requirements:

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

Security Requirements:

Fabrikam identifies the following security requirements:

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

Question: 13

HOTSPOT

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

NOTE: Each correct selection is worth one point.

Minimum number of Azure AD tenants:

Minimum number of custom domains to add:

Minimum number of conditional access policies to create:

Answer:

Explanation:

1
1
0

Question: 14

You need to recommend a data storage strategy for WebApp1.
What should you include in in the recommendation?

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

Answer: B

Explanation:

Question: 15

You need to recommend a strategy for migrating the database content of WebApp1 to Azure. What should you include in the recommendation?

A. Use Azure Site Recovery to replicate the SQL servers to Azure.
B. Use SQL Server transactional replication.
C. Copy the BACPAC file that contains the Azure SQL database file to Azure Blob storage.
D. Copy the VHD that contains the Azure SQL database files to Azure Blob storage

Answer: D

Explanation:

Before you upload a Windows virtual machine (VM) from on-premises to Azure, you must prepare the virtual hard disk (VHD or VHDX).

Scenario: WebApp1 has a web tier that uses Microsoft Internet Information Services (IIS) and a database tier that runs Microsoft SQL Server 2016. The web tier and the database tier are deployed to virtual machines that run on Hyper-V.

Reference:
https://docs.microsoft.com/en-us/azure/virtual-machines/windows/prepare-for-upload-vhd-image

Question: 16

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

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

Answer: A

Explanation:

Question: 17

HOTSPOT

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

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

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

Answer:

Explanation:

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

Box 1: Yes
Any new deployments to Azure must be redundant in case an Azure region fails.

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

Box 2: Yes
Recent changes in Azure brought some significant changes in autoscaling options for Azure Web Apps (i.e. Azure App Service to be precise as scaling happens on App Service plan level and has effect on all Web Apps running in that App Service plan).

Box 3: No
Traffic Manager provides a range of traffic-routing methods and endpoint monitoring options to suit different application needs and automatic failover models. Traffic Manager is resilient to failure, including the failure of an entire Azure region.

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

https://blogs.msdn.microsoft.com/hsirtl/2017/07/03/autoscaling-azure-web-apps/

Question: 18

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

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

Answer: A

Explanation:

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

In Azure SQL Database, you can configure a database with a long-term backup retention policy (LTR) to automatically retain the database backups in separate Azure Blob storage containers for up to 10 years

Question: 19

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

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

Answer: B

Explanation:

Directory synchronization between Azure Active Directory (Azure AD) and corp.fabrikam.com must not be affected by a link failure between Azure and the on-premises network. (This requires domain controllers in Azure)

Users on the on-premises network must be able to authenticate to corp.fabrikam.com if an Internet link fails. (This requires domain controllers on-premises)

Question: 20

HOTSPOT

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

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

NOTE: Each correct selection is worth one point.

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

Answer:

Explanation:

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

Question: 21

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

What should you include in the recommendation?

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

Answer: D

Explanation:

Reference:

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

Topic 3, Contoso

Case Study

Overview

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

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

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

To start the case study

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

Existing Environment: Technical Environment

The on-premises network contains a single Active Directory domain named contoso.com. Contoso has a single Azure subscription.

Existing Environment: Business Partnerships

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

Requirements: Planned Changes

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

Requirements: App1

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

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

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

App1 has the following data requirements:

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

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

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

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

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

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

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

Requirements: App2

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

Save files to an Azure Storage account.

Replicate files to an on-premises location.

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

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

Application Development Requirements

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

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

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

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

Identity Requirements

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

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

Security Requirement

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

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

Question: 22

HOTSPOT

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

NOTE: Each correct selection is worth one point.

Answer:

Requirements: Identity Requirements

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

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

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

Box 1: The Azure AD Privileged Identity Management (PIM)

When should you use access reviews?

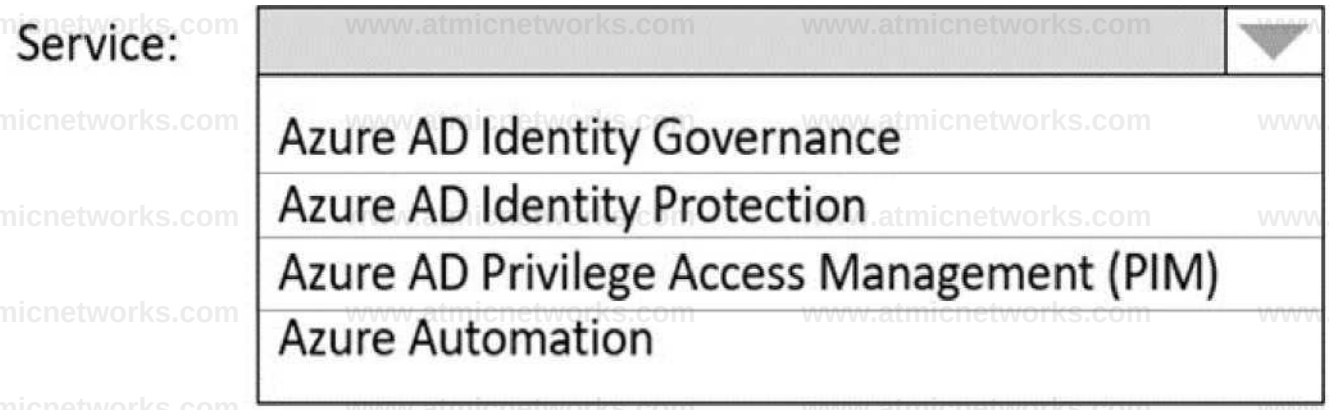
Too many users in privileged roles: It's a good idea to check how many users have administrative access, how many of them are Global Administrators, and if there are any invited guests or partners that have not been removed after being assigned to do an administrative task. You can recertify the role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

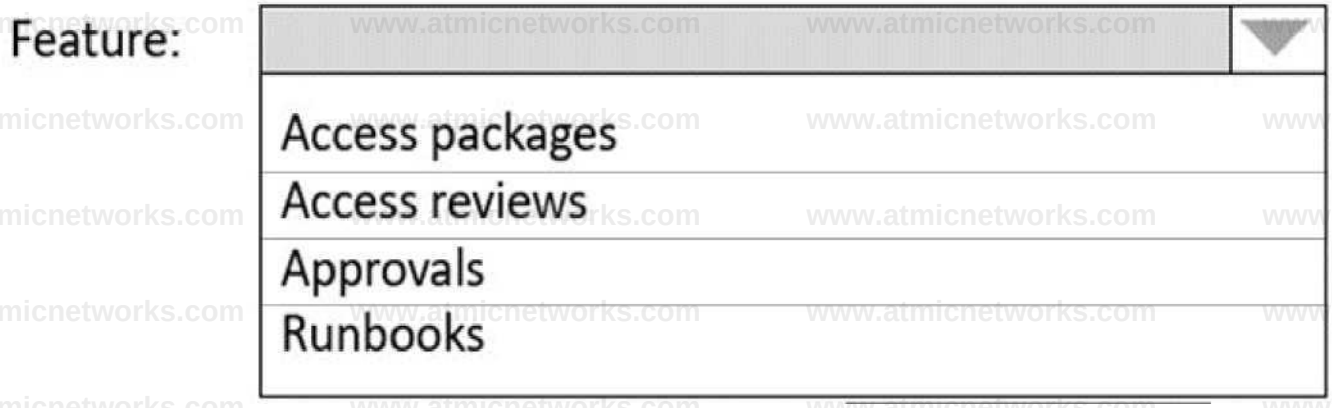
Box 2: Access reviews

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

Reference:

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





Explanation:

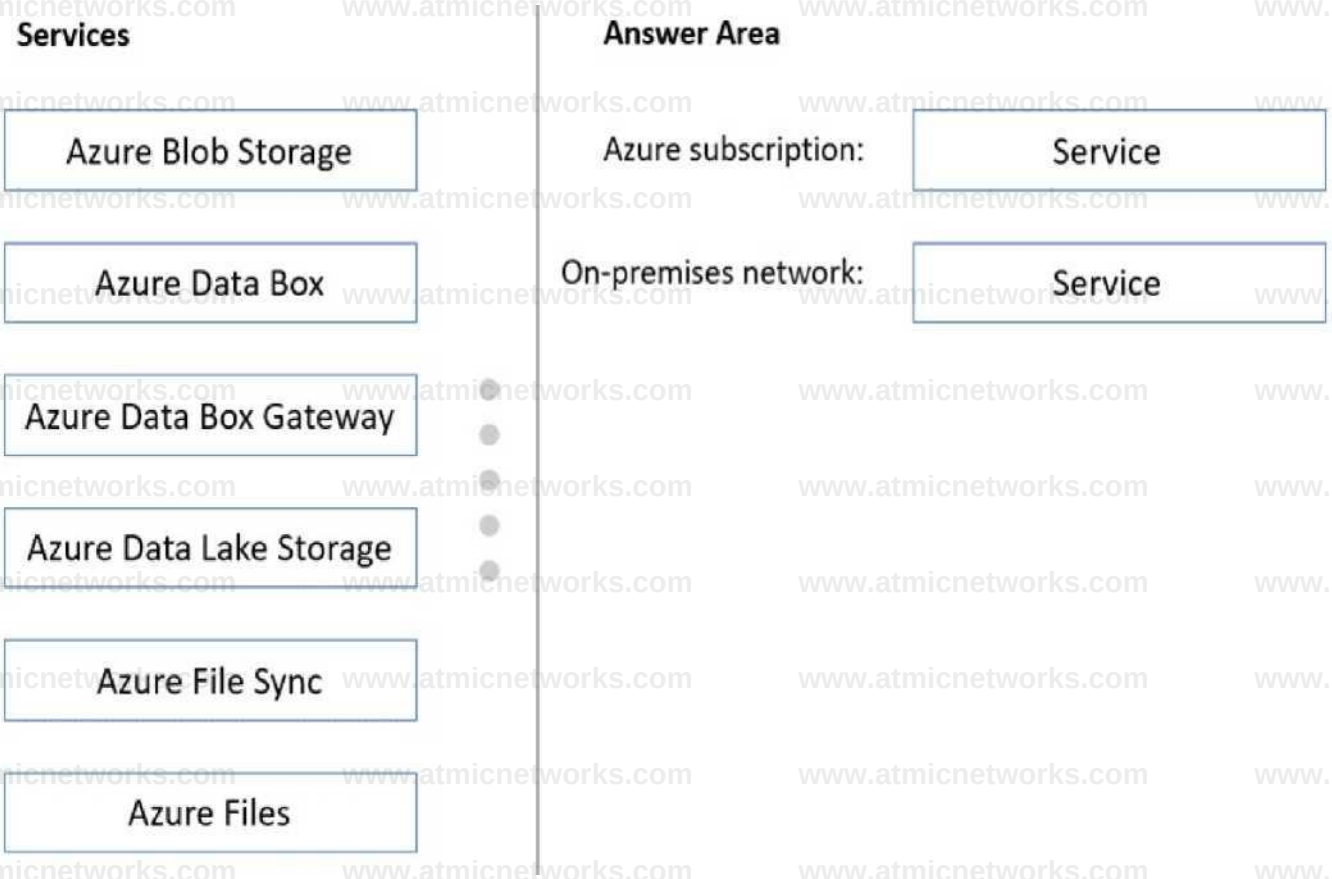
Question: 23

DRAG DROP

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

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

NOTE: Each correct selection is worth one point.



Answer:

Explanation:

Azure subscription: **Azure Files**

On-premises network: **Azure File Sync**

Box 1: Azure Files

Scenario: App2 has the following file storage requirements:

Save files to an Azure Storage account.

Replicate files to an on-premises location.

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

Box 2: Azure File Sync

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

Reference:

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

Question: 24

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

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

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

Answer: A

Explanation:

Scenario: App1 has the following data requirements:

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

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

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

Reference:

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

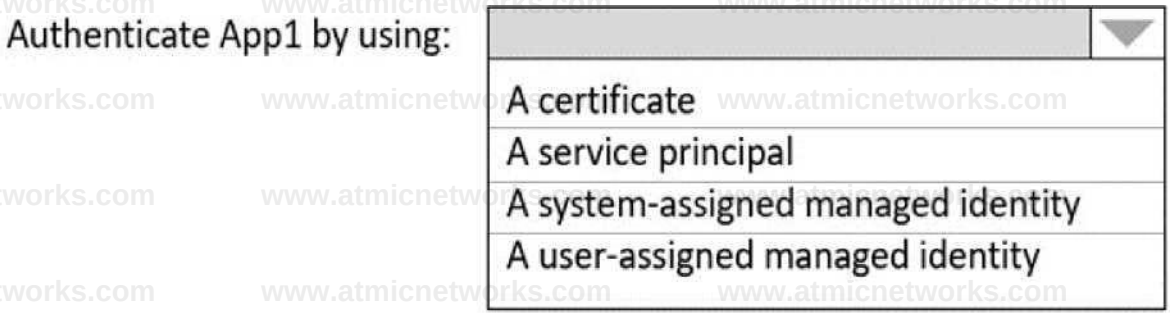
Question: 25

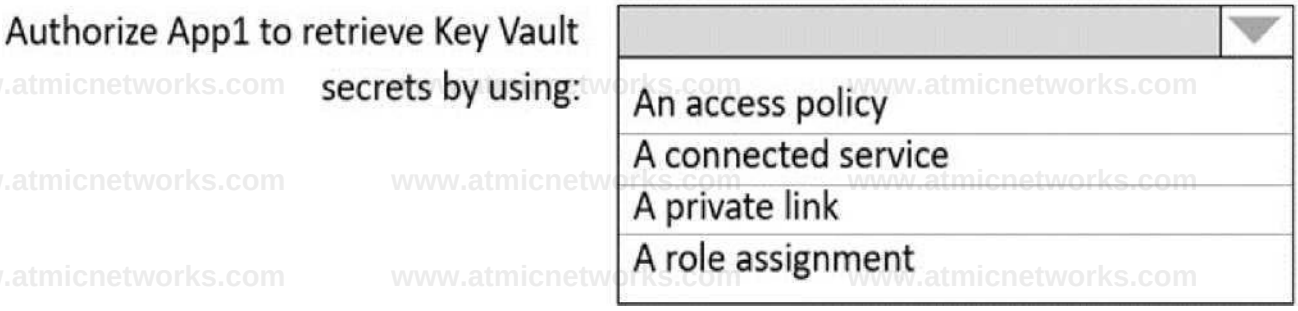
HOTSPOT

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

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

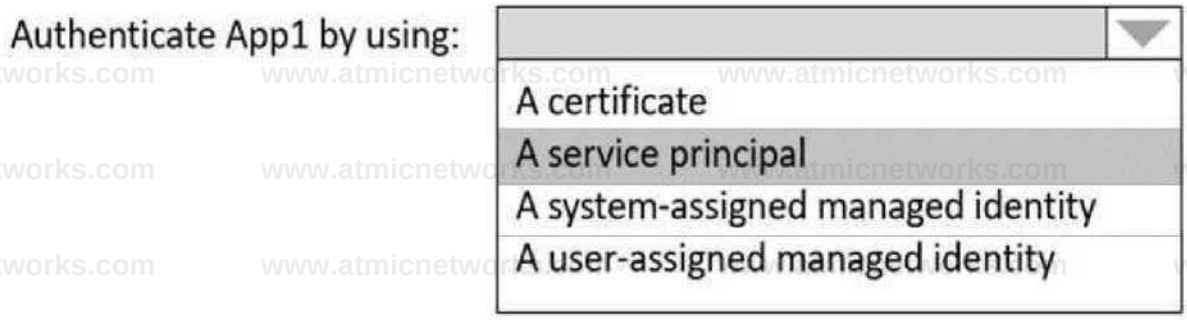
NOTE: Each correct selection is worth one point.

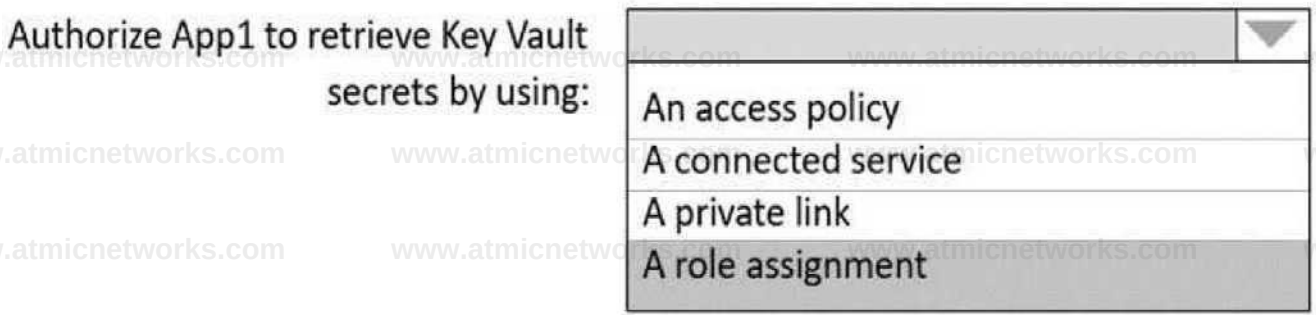




Answer:

Explanation:





Scenario: Security Requirement

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

Services that require credentials must have the credentials tied to the service instance. The

credentials must NOT be shared between services.

Box 1: A service principal
A service principal is a type of security principal that identifies an application or service, which is to say, a piece of code rather than a user or group. A service principal's object ID is known as its client ID and acts like its username. The service principal's client secret acts like its password.

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

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

Box 2: A role assignment
You can provide access to Key Vault keys, certificates, and secrets with an Azure role-based access control.

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

Question: 26

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

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

Answer: D

Explanation:

Question: 27

HOTSPOT
You are evaluating whether to use Azure Traffic Manager and Azure Application Gateway to meet the connection requirements for App1.
What is the minimum numbers of instances required for each service? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

Answer:

Explanation:

Answer Area

Azure Traffic Manager 2 v

Azure Application Gateway: 1 v

Question: 28

What should you recommend lo meet the monitoring requirements for App2?

A. Azure Application Insights
B. Container insights
C. Microsoft Sentinel
D. VM insights

Answer: A

Explanation:

Question: 29

What should you recommend to meet the monitoring requirements for App2?

A. Microsoft Sentinel
B. Azure Application Insights
C. Container insights
D. VM insights

Answer: B

Explanation:

Topic 4, HABInsurance Case Study

Overview

An insurance company, HABInsurance, operates in three states and provides home, auto, and boat insurance. Besides the head office, HABInsurance has three regional offices.

Current environment

General

An insurance company, HABInsurance, operates in three states and provides home, auto, and boat insurance. Besides the head office, HABInsurance has three regional offices.

Technology assessment

The company has two Active Directory forests: main.habinsurance.com and region.habinsurance.com. HABInsurance's primary internal system is Insurance Processing System (IPS). It is an ASP.Net/C# application running on IIS/Windows Servers hosted in a data center. IPS has three tiers: web, business logic API, and a datastore on a back end. The company uses Microsoft SQL Server and MongoDB for the backend. The system has two parts: Customer data and Insurance forms and documents. Customer data is stored in Microsoft SQL Server and Insurance forms and documents — in MongoDB. The company also has 10 TB of Human Resources (HR) data stored on NAS at the head office location.

Requirements

General

HABInsurance plans to migrate its workloads to Azure. They purchased an Azure subscription. Changes
During a transition period, HABInsurance wants to create a hybrid identity model along with a Microsoft Office 365 deployment. The company intends to sync its AD forests to Azure AD and benefit from Azure AD administrative units functionality.

HABInsurance needs to migrate the current IPSCustomers SQL database to a new fully managed SQL database in Azure that would be budget-oriented, balanced with scalable compute and storage options. The management team expects the Azure database service to scale the database resources

dynamically with minimal downtime. The technical team proposes implementing a DTU-based purchasing model for the new database.

HABInsurance wants to migrate Insurance forms and documents to Azure database service.

HABInsurance plans to move IPS first two tiers to Azure without any modifications. The technology team discusses the possibility of running IPS tiers on a set of virtual machines instances. The number of instances should be adjusted automatically based on the CPU utilization. An SLA of 99.95% must be guaranteed for the compute infrastructure.

The company needs to move HR data to Azure File shares.

In their new Azure ecosystem, HABInsurance plans to use internal and third-party applications. The company considers

adding user consent for data access to the registered applications
Later, the technology team contemplates adding a customer self-service portal to IPS and deploying a new IPS to multi-region ASK. But the management team is worried about performance and availability of the multi-region AKS deployments during regional outages.

Question: 30

What two parameters would you recommend set up to ensure that the new IPSCustomers database will scale to meet the workload demands?

A. Define the maximum of CPU cores
B. Define the maximum resource limit per group of databases
C. Define the maximum of Database Transaction Units
D. Define the maximum of the allocated storage
E. Define the maximum size for a database

Answer: C,E

Explanation:

Question: 31

A company has an on-premises file server cbflserver that runs Windows Server 2019. Windows Admin Center manages this server. The company owns an Azure subscription. You need to provide an Azure solution to prevent data loss if the file server fails.
Solution: You decide to create an Azure Recovery Services vault. You then decide to install the Azure Backup agent and then schedule the backup. Would this meet the requirement?

A. Yes
B. No

Answer: A

Explanation:

Question: 32

A company is planning on deploying an application onto Azure. The application will be based on the .Net core programming language. The application would be hosted using Azure Web apps. Below is part of the various requirements for the application
Give the ability to correlate Azure resource usage and the performance data with the actual application configuration and performance data
Give the ability to visualize the relationships between application components

Give the ability to track requests and exceptions to specific lines of code from within the application

Give the ability to actually analyse how uses return to an application and see how often they only select a particular drop-down value

Which of the following service would be best suited for fulfilling the requirement of

"Give the ability to correlate Azure resource usage and the performance data with the actual application configuration and performance data"

A. Azure Application Insights
B. Azure Service Map
C. Azure Log Analytics
D. Azure Activity Log

Answer: C

Explanation:

Question: 33

A company has an on-premises file server cbflserver that runs Windows Server 2019. Windows Admin Center manages this server. The company owns an Azure subscription. You need to provide an Azure solution to prevent data loss if the file server fails.

Solution: You decide to register Windows Admin Center in Azure and then configure Azure Backup. Would this meet the requirement?

A. Yes
B. No

Answer: A

Explanation:

Topic 5, Misc. Questions

Question: 34

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

You need to recommends a solution to verify whether the Faricak developers still require permissions to Application1. The solution must the following requirements.

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

What should you recommend?

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

Answer: D

Explanation:

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

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

management capabilities."

Question: 35

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

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

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

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

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

NOTE: Each correct selection is worth one point.

A. Azure AD Application Proxy
B. Azure AD Privileged Identity Management (PIM)
C. Conditional Access policies
D. Azure Arc
E. Azure AD enterprise applications
F. Azure Application Gateway

Answer: A,F

Explanation:

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

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

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy-config-sso-how-to

https://docs.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy-deployment-plan

Question: 36

You have an Azure Active Directory (Azure AD) tenant named contoso.com that has a security group named Group'. Group i is configured Tor assigned membership. Group I has 50 members. including 20 guest users.

You need To recommend a solution for evaluating the member ship of Group1. The solution must meet the following requirements:

- The evaluation must be repeated automatically every three months
- Every member must be able to report whether they need to be in Group1
- Users who report that they do not need to be in Group 1 must be removed from Group1 automatically
- Users who do not report whether they need to be m Group1 must be removed from Group1 automatically.

What should you include in me recommendation?

A. implement Azure AU Identity Protection.
B. Change the Membership type of Group1 to Dynamic User.
C. Implement Azure AD Privileged Identity Management.
D. Create an access review.

Answer: D

Explanation:

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

Have reviews recur periodically: You can set up recurring access reviews of users at set frequencies such as weekly, monthly, quarterly or annually, and the reviewers will be notified at the start of each review. Reviewers can approve or deny access with a friendly interface and with the help of smart recommendations.

An administrator creates an access review of Group C with 50 member users and 25 guest users.
Makes it a self-review. 50 licenses for each user as self-reviewers.* https://docs.microsoft.com/en- us/azure/active-directory/governance/access-reviews-overview#example-license-scenarios

There are 4 requirements and every single one is only met by access reviews.
https://docs.microsoft.com/en-us/azure/active-directory/governance/access-reviews-

overview#when-should-you-use-access-reviews
Dynamic User is needed if a user must be automatically granted access on base of its attributes (department, jobtitle, location, etc.) https://techcommunity.microsoft.com/t5/itops-talk- blog/dynamic-groups-in-azure-ad-and-microsoft-365/ba-p/2267494
Implementing Azure AD PIM is no solution and absolutely not necessary for access reviews.
https://docs.microsoft.com/en-us/azure/active-directory/governance/access-reviews- overview#where-do-you-create-reviews

Question: 37

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:

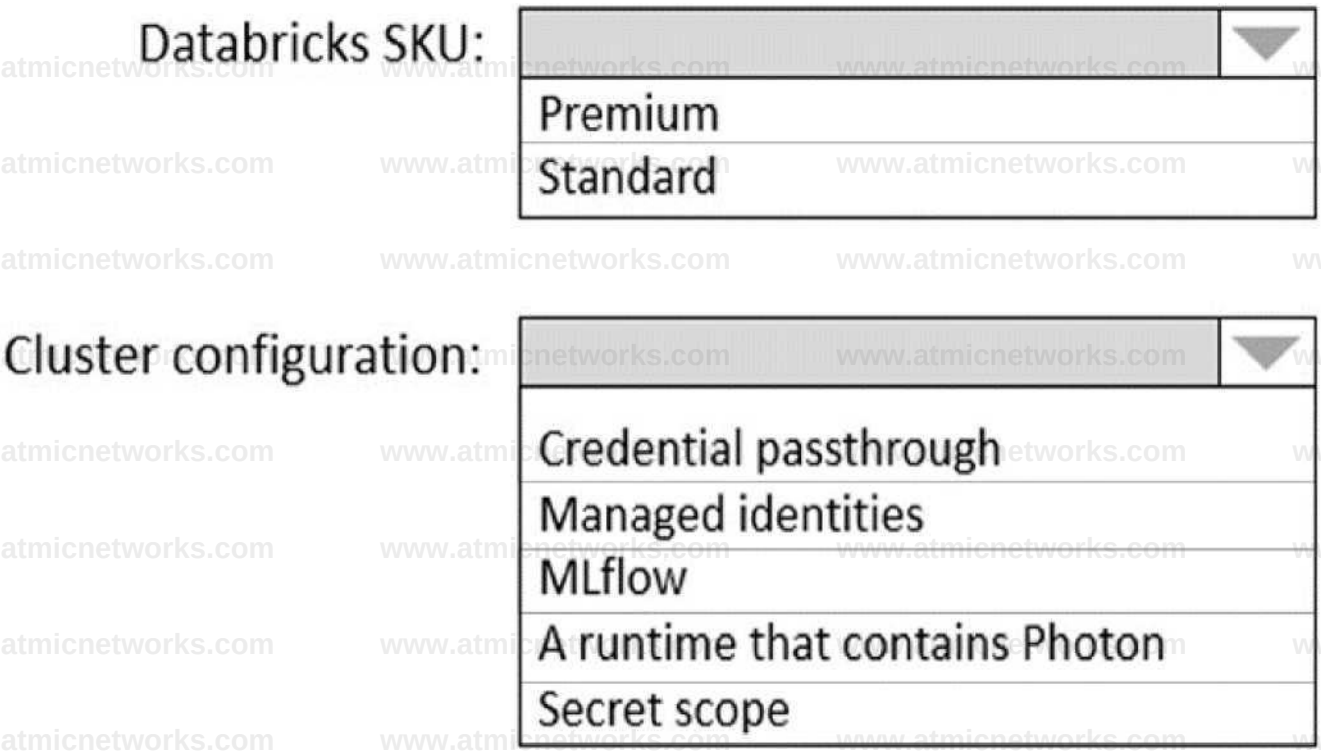
Ensure that the data engineers can only access folders to which they have permissions.

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.



Answer:

Explanation:

Box 1: Standard

Choose Standard to minimize costs.

Box 2: Credential passthrough

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

Reference:

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

Question: 38

HOTSPOT

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

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

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

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

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

Answer:

Explanation:

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

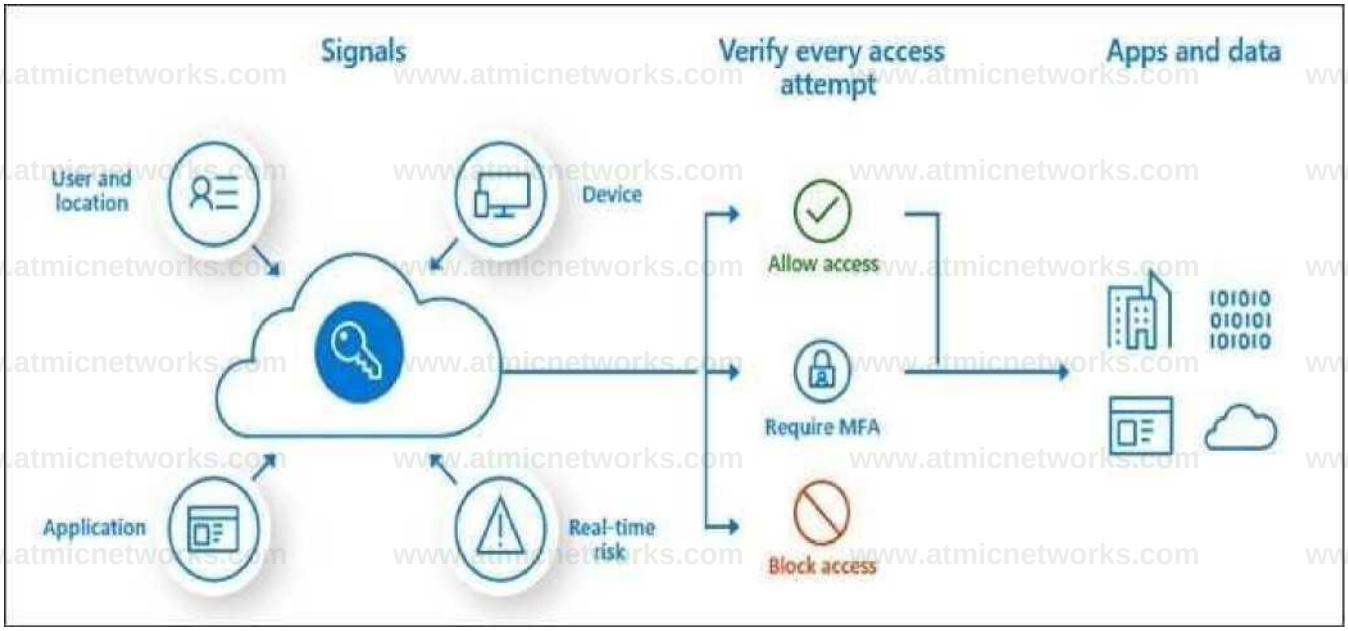
The users can access App1 only from company-owned computers:

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

Box 1: An Azure AD app registration
Azure active directory (AD) provides cloud based directory and identity management services.You can use azure AD to manage users of your application and authenticate access to your applications using azure active directory.
You register your application with Azure active directory tenant.

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

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



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

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

https://docs.microsoft.com/en-us/powerapps/developer/data-platform/walkthrough-register-app- azure-active-directory#:~:text=Create%20an%20application%20registration%201%20Create%20an%20application,the%20options%20and%20click%20on%20Add%20permissions.%20

"After consenting to use their Dataverse account with the ISV's application, end users can connect to Dataverse environment from external application. The consent form is not displayed again to other users after the first user who has already consented to use the ISV's app. Apps registered in Azure Active Directory are multi-tenant, which implies that other Dataverse users from other tenant can connect to their environment using the ISV's app."

Question: 39

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

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

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

Several virtual machines exhibit network connectivity issues.

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

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

Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:

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

Note: IP flow verify checks if a packet is allowed or denied to or from a virtual machine. The information consists of direction, protocol, local IP, remote IP, local port, and remote port. If the packet is denied by a security group, the name of the rule that denied the packet is returned. While any source or destination IP can be chosen, IP flow verify helps administrators quickly diagnose connectivity issues from or to the internet and from or to the on-premises environment.

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

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

Question: 40

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

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

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

Several VMs are exhibiting network connectivity issues.

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

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

Does the solution meet the goal?

A. Yes
B. No

Answer: B

Explanation:

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

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

With Advisor, you can:

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

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

Question: 41

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

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

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

Several VMs are exhibiting network connectivity issues.

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

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

Does the solution meet the goal?

A. Yes
B. No

Answer: A

Explanation:

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

Note:
IP flow verify checks if a packet is allowed or denied to or from a virtual machine. The information consists of direction, protocol, local IP, remote IP, local port, and remote port. If the packet is denied by a security group, the name of the rule that denied the packet is returned. While any source or destination IP can be chosen, IP flow verify helps administrators quickly diagnose connectivity issues from or to the internet and from or to the on-premises environment.

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

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

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

Question: 42

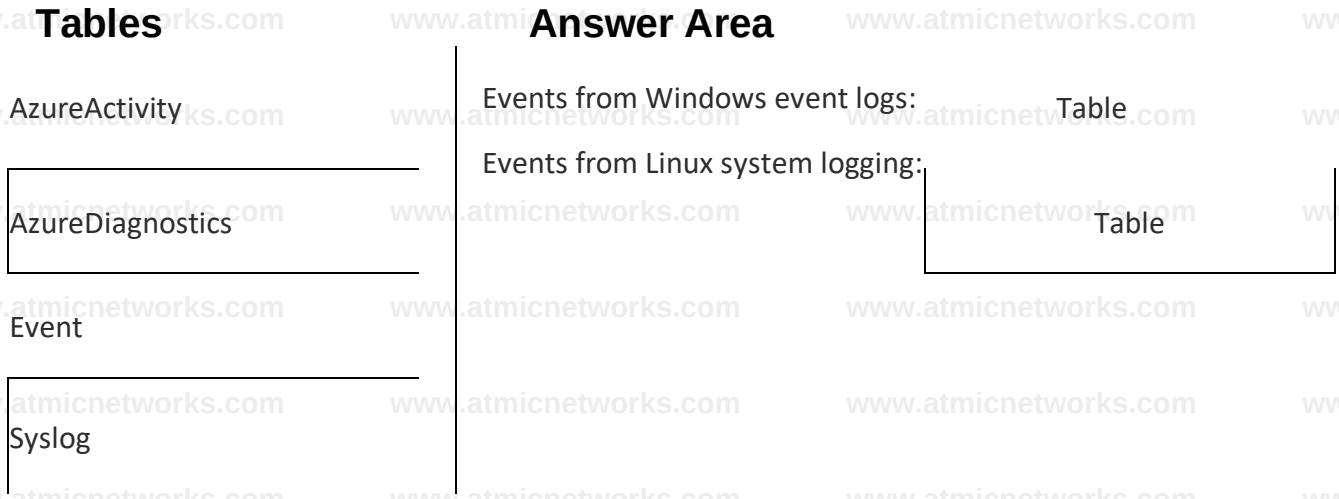
DRAG DROP

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

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

Which Log Analytics tables should you query? To answer, drag the appropriate tables to the correct log types. Each value may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.



Answer:

Explanation:

https://docs.microsoft.com/en-us/azure/azure-monitor/platform/log-analytics-agent Windows Event logs --> Information sent to the Windows event logging system. Syslog --> Information sent to the Linux event logging system.

Question: 43

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

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

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

NOTE: Each correct selection is worth one point.

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

Answer: A,B,D

Explanation:

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

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

Question: 44

DRAG DROP

Your on-premises network contains a server named Server1 that runs an ASP.NET application named App1.
You have a hybrid deployment of Azure Active Directory (Azure AD).
You need to recommend a solution to ensure that users sign in by using their Azure AD account and Azure Multi-Factor Authentication (MFA) when they connect to App1 from the internet.
Which three Azure services should you recommend be deployed and configured in sequence? To answer, move the appropriate services from the list of services to the answer area and arrange them in the correct order.

Services

an internal Azure Load Balancer

an Azure AD conditional access policy

Azure AD Application Proxy

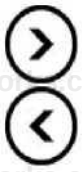
an Azure AD managed identity

a public Azure Load Balancer

an Azure AD enterprise application

an App Service plan

Answer Area



Answer:

Explanation:

AD Application Proxy
AD Enterprise Application
AD Conditional access policy
https://thesleepyadmins.com/2019/02/

Question: 45

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

A. Azure Analysis Services
B. Application Insights
C. Azure Monitor action groups
D. Azure Log Analytics

Answer: D

Explanation:

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

Through activity logs, you can determine:

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

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

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

Question: 46

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

The largest database is currently 3 TB. None of the databases will ever exceed 4 TB.

Stored procedures are implemented by using CLR.

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

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

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

What should you include in the recommendation?

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

Answer: B

Explanation:

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

SQL Managed Instance allows existing SQL Server customers to lift and shift their on-premises applications to the cloud with minimal application and database changes. At the same time, SQL Managed Instance preserves all PaaS capabilities (automatic patching and version updates, automated backups, high availability) that drastically reduce management overhead and TCO. https://docs.microsoft.com/en-us/azure/azure-sql/managed-instance/transact-sql-tsql-differences-sql-server#clr

https://docs.microsoft.com/en-gb/azure/azure-sql/database/transact-sql-tsql-differences-sql- server#transact-sql-syntax-

not-supported-in-azure-sql-database

Question: 47

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

You have an on-premises file server named Setver1 that runs Windows Sewer 2016. Server1 stores 500 GB of company files.

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

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

NOTE: Each correct selection is worth one point

A. an Azure Batch account
B. an integration account
C. an On-premises data gateway
D. an Azure Import/Export job
E. Azure Data factory

Answer: D,E

Explanation:

https://docs.microsoft.com/en-us/azure/storage/common/storage-import-export-data-from-blobs
https://docs.microsoft.com/en-us/answers/questions/31113/fastest-method-to-copy-500gb-table- from-on-premise.html

Question: 48

You have an Azure subscription that contains two applications named App1 and App2. App1 is a sales processing application. When a transaction in App1 requires shipping, a message is added to an Azure Storage account queue, and then App2 listens to the queue for relevant transactions.

In the future, additional applications will be added that will process some of the shipping requests based on the specific details of the transactions.

You need to recommend a replacement for the storage account queue to ensure that each additional application will be able to read the relevant transactions.

What should you recommend?

A. one Azure Service Bus queue
B. one Azure Service Bus topic

C. one Azure Data Factory pipeline

D. multiple storage account queues

Answer: B

Explanation:

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

Reference:
https://docs.microsoft.com/en-us/azure/service-bus-messaging/service-bus-queues-topics- subscriptions

Question: 49

HOTSPOT

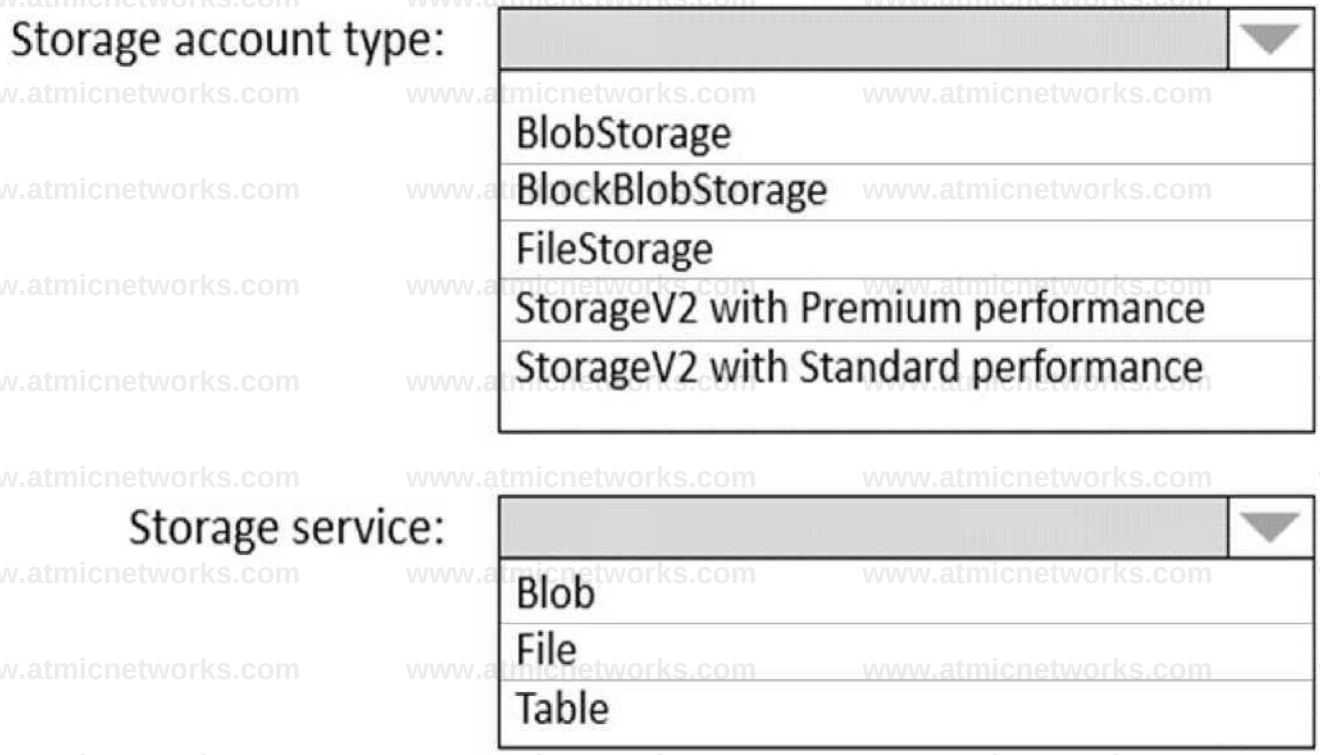
You need to design a storage solution for an app that will store large amounts of frequently used dat

a. 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.



Answer:

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 ofline 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: 50

HOTSPOT

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

Name	Type	Performance
storagel	StorageV2	Standard
storage2	SrorageV2	Premium
storages	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.

Appt _____ 2

Storage 1 and storage? only
Storage 1 and storage3 only
Storage^, storage?, and storages **only**
Storage 1. storage?, storages, and storage4

App?: _____ ,

Storage4 only
Storage 1 and storage4 only
Storagel, storage?, **and** storage4 **only**
Storage!, storage?, storages, and storage4

Answer:

Explanation:

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

https://www.edureka.co/community/40011/different-storage-accounts-there-major-difference- between

https://insidemstech.com/tag/general-purpose-v2/

In conclusion the correct answers are:

Box1 --> Storage1 and Storage3 only
Box2 --> Storage1 and Storage4 only

https://docs.microsoft.com/en-us/azure/storage/files/storage-how-to-create-file-share?tabs=azure- portal#basics

Question: 51

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

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

What should you recommend?

A. Azure Files
B. Azure Data Lake Storage Gen2
C. Azure Blob Storage

D. Azure SQL Database

Answer: C

Explanation:

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

Max file in Blob Storage. 4.77 TB.

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

Question: 52

You ate designing a SQL database solution. The solution will include 20 databases that will be 20 GB each and have varying usage patterns. You need to recommend a database platform to host the databases. The solution must meet the following requirements:

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

What should you include in the recommendation?

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

Answer: D

Explanation:

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

Guaranteed 99.995 percent uptime for SQL Database

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

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

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

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

Question: 53

HOTSPOT

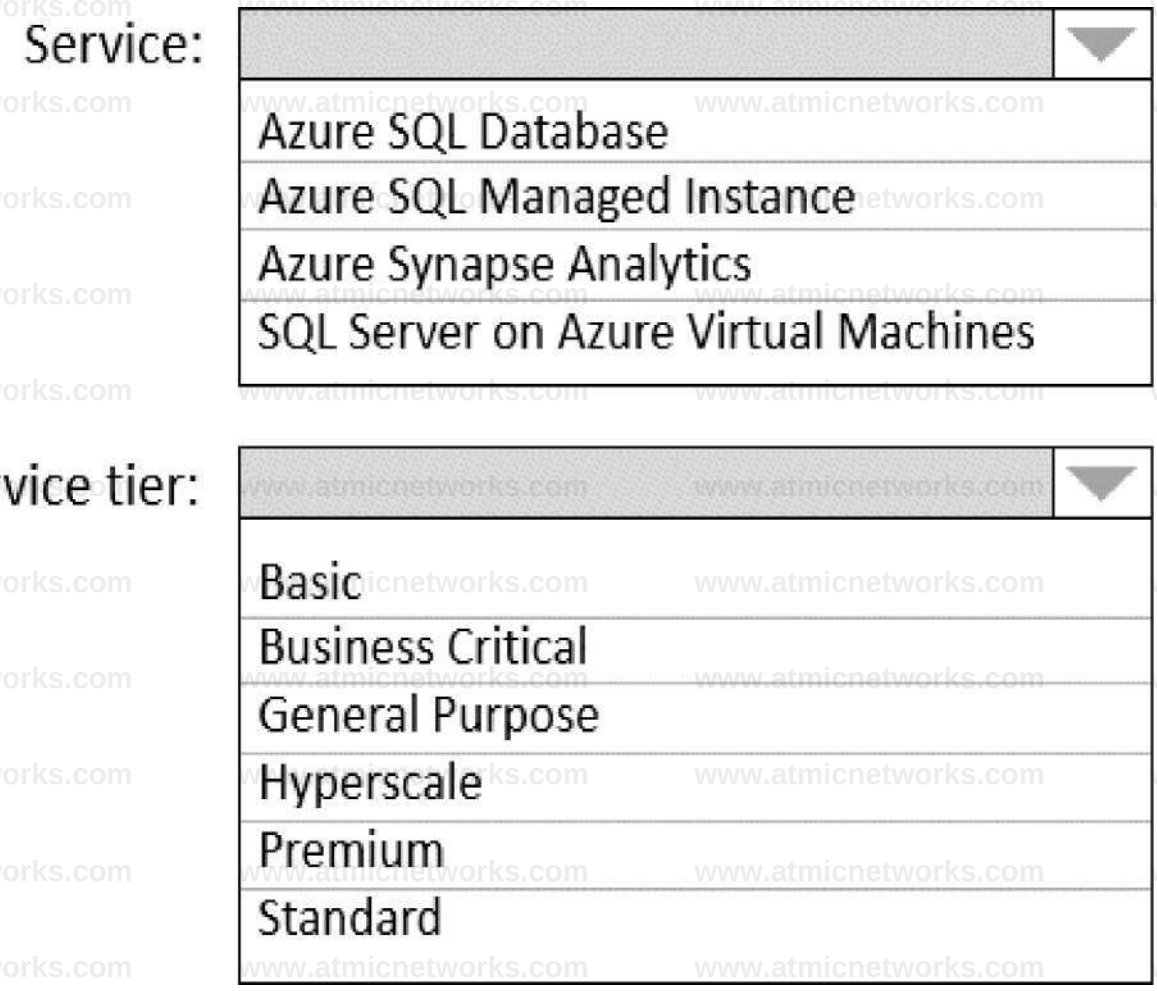
You have an on-premises database that you plan to migrate to Azure.

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.



Answer:

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

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-azure-sql-vs-sql-server-vm-cf02578a1188

Question: 54

ION NO: 9

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

Each device will stream data, including temperature, device ID, and time dat

a. Approximately 50,000 records will be written every second. The data will be visualized in near real time.

You need to recommend a service to store and query the data.

Which two services can you recommend? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

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

Answer: C,D

Explanation:

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

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

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

Question: 55

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

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

Support SQL commands.
Support multi-master writes.
Guarantee low latency read operations.

What should you include in the recommendation?

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

Answer: A

Explanation:

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

Unlimited elastic write and read scalability.
99.999% read and write availability all around the world.
Guaranteed reads and writes served in less than 10 milliseconds at the 99th percentile.

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

Question: 56

HOTSPOT

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

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

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

Name	Resource group	Location	Account kind
storage+	RG1	East US	Storage'/? (genera! purpose v2]
storage;	RG2	Central US	BibbStorage

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

Name	Resource group	Server	Pricing tier
SQLdbl	RG1	SQLsVrl	Standard

SQLdb2	RG1	SQLSVrl	Standard
SQLdb3	RG?	SQL$VT2	Premium

Answer Area

Statements	Yes	No
When you enable auditing forSQLdbl, you can store the audit information to storage!	O	O
When you enable auditing forSQLdb2, you can store the audit information to storage?.	O	O
When you enable auditing forSQLdbJ, you can store the audit information to storage?.	O	O

Answer:

Explanation:

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

Box 2: No

Box 3: Yes
https://docs.microsoft.com/en-us/azure/sql-database/sql-database-auditing

Reference:
https://docs.microsoft.com/en-us/azure/sql-database/sql-database-auditing
https://docs.microsoft.com/en-us/previous-versions/azure/dn741340(v=azure.100)?redirectedfrom=MSDN

Question: 57

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 dat

a. 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

Answer: D

Explanation:

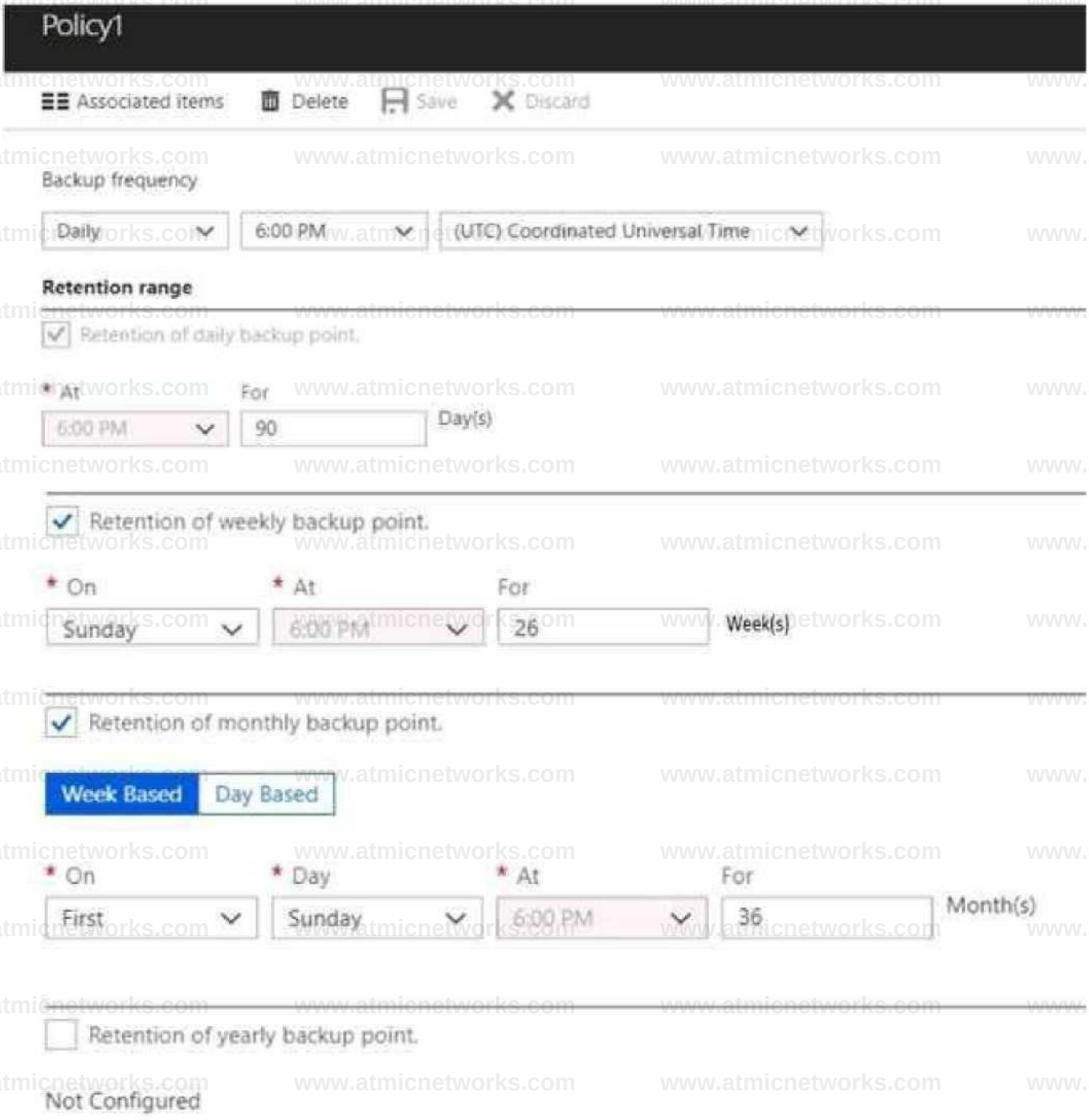
Replication with Azure Site Recover:
RTO is typically less than 15 minutes.
RPO: One hour for application consistency and five minutes for crash consistency.

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

Question: 58

HOTSPOT

You plan to deploy the backup policy 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.

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

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

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

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

Answer:

Explanation:

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

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

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

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

https://docs.microsoft.com/en-us/azure/backup/backup-azure-vm-backup-faq#what-s-the-minimum-rpo-and-rto-for-vm-backups-in-azure-backup

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.

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

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

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

Does this meet the goal?

A. Yes
B. No

Answer: A

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: 60

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

Answer: B

Explanation:

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

Question: 61

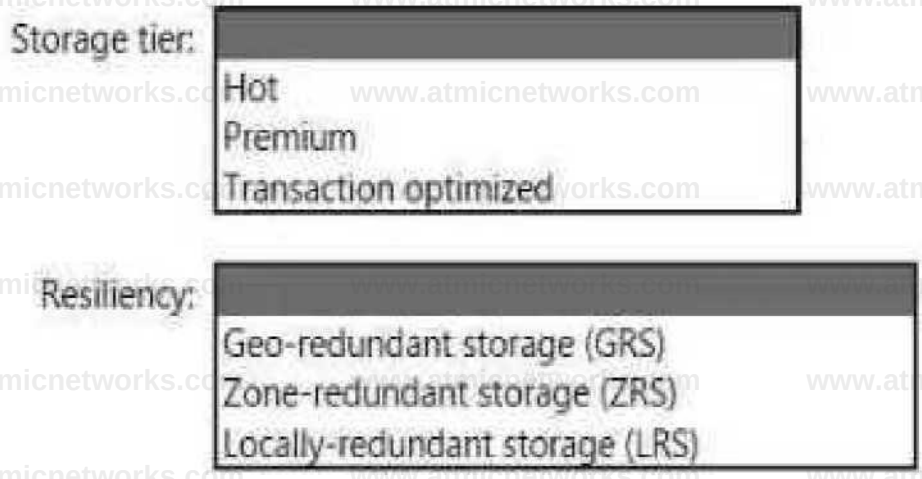
HOTSPOT

You plan to create an Azure Storage account that will host file shares. The shares will be accessed from on-premises applications that are transaction-intensive.

You need to recommend a solution to minimize latency when accessing the file shares. The solution must provide the highest-level of resiliency for the selected storage tier.

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

NOTE: Each correct selection is worth one point.



Answer:

Explanation:

Box 1: Premium

Premium: Premium file shares are backed by solid-state drives (SSDs) and provide consistent high performance and low latency, within single-digit milliseconds for most IO operations, for IO-intensive workloads.

Box 2: Zone-redundant storage (ZRS):

Premium Azure file shares only support LRS and ZRS.

Zone-redundant storage (ZRS): With ZRS, three copies of each file stored, however these copies are physically isolated in three distinct storage clusters in different Azure availability zones.

Reference:
https://docs.microsoft.com/en-us/azure/storage/files/storage-files-planning

Question: 62

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 scale set that uses autoscaling.
Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:

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

Question: 63

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.

Answer: D

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: 64

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

Name	Azutf region
Hub I	US Edit
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.

Answer: A

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: 65

You have an Azure subscription that contains a storage account.
An application sometimes writes duplicate files to the storage account.
You have a PowerShell script that identifies and deletes duplicate files in the storage account.
Currently, the script is run manually after approval from the operations manager.
You need to recommend a serverless solution that performs the following actions:

Runs the script once an hour to identify whether duplicate files exist

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

What should you include in the recommendation?

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

D. Azure Functions and Azure Batch

Answer: A

Explanation:

You can schedule a powershell script with Azure Logic Apps.

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

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

Question: 66

Your company has the infrastructure shown in the following table.

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

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

Server1 runs an application named Appl that uses LDAP queries to verify user identities in the onpremises Active Directory domain.

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

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

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

What should you include in the recommendation?

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

Answer: A

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: 67

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

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

Answer: D

Explanation:

When you create a function app in Azure, you must choose a hosting plan for your app. There are three basic hosting plans available for Azure Functions: Consumption plan, Premium plan, and Dedicated (App Service) plan.
For the Consumption plan, you don't have to pay for idle VMs or reserve capacity in advance.

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

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

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

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

Question: 68

HOTSPOT

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

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

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

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

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

NOTE: Each correct selection is worth one point.

On-premises:

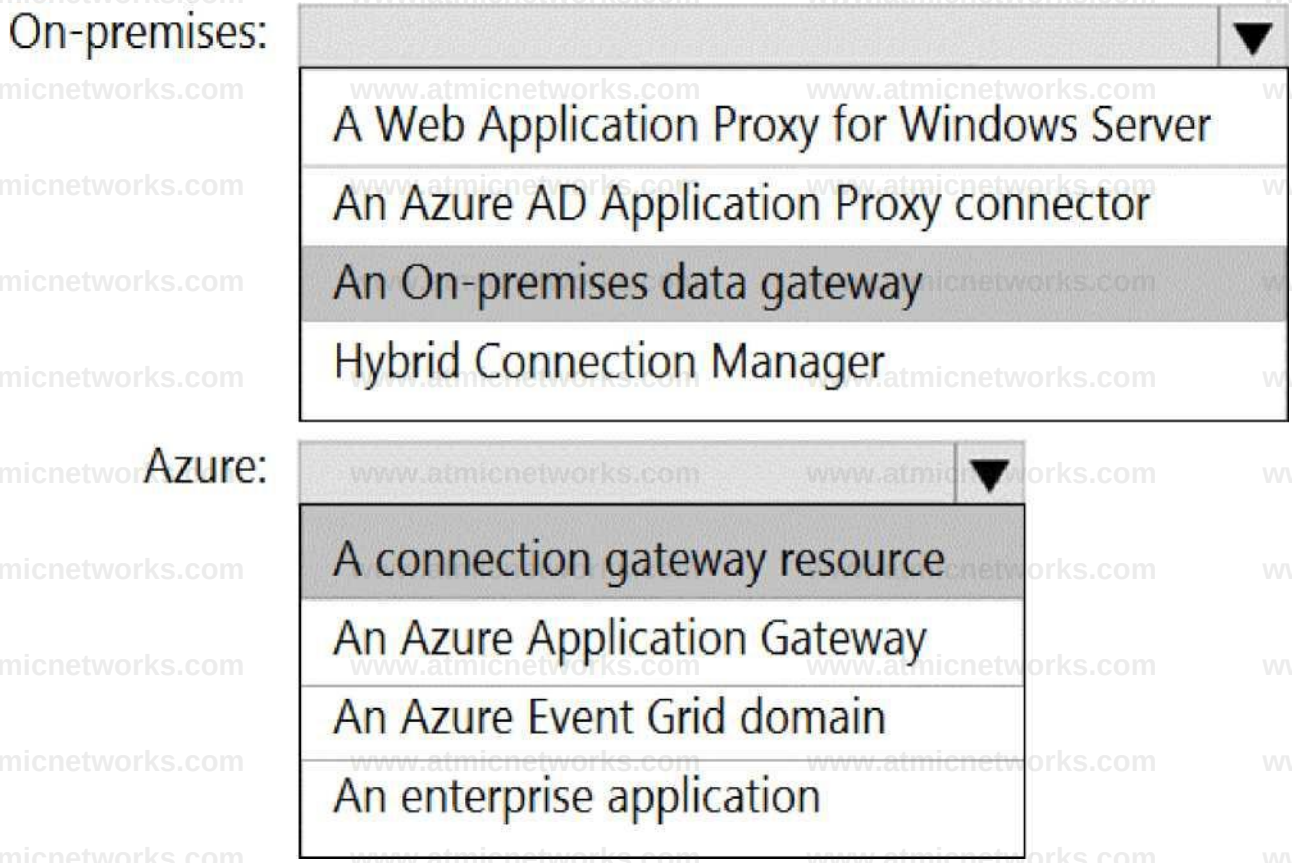
- A Web Application Proxy for Windows Server
- An Azure AD Application Proxy connector
- An On-premises data gateway
- Hybrid Connection Manager

Azure:

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

Answer:

Explanation:



Box 1: An on-premises data gateway
For logic apps in global, multi-tenant Azure that connect to on-premises SQL Server, you need to have the on-premises data gateway installed on a local computer and a data gateway resource that's already created in Azure.

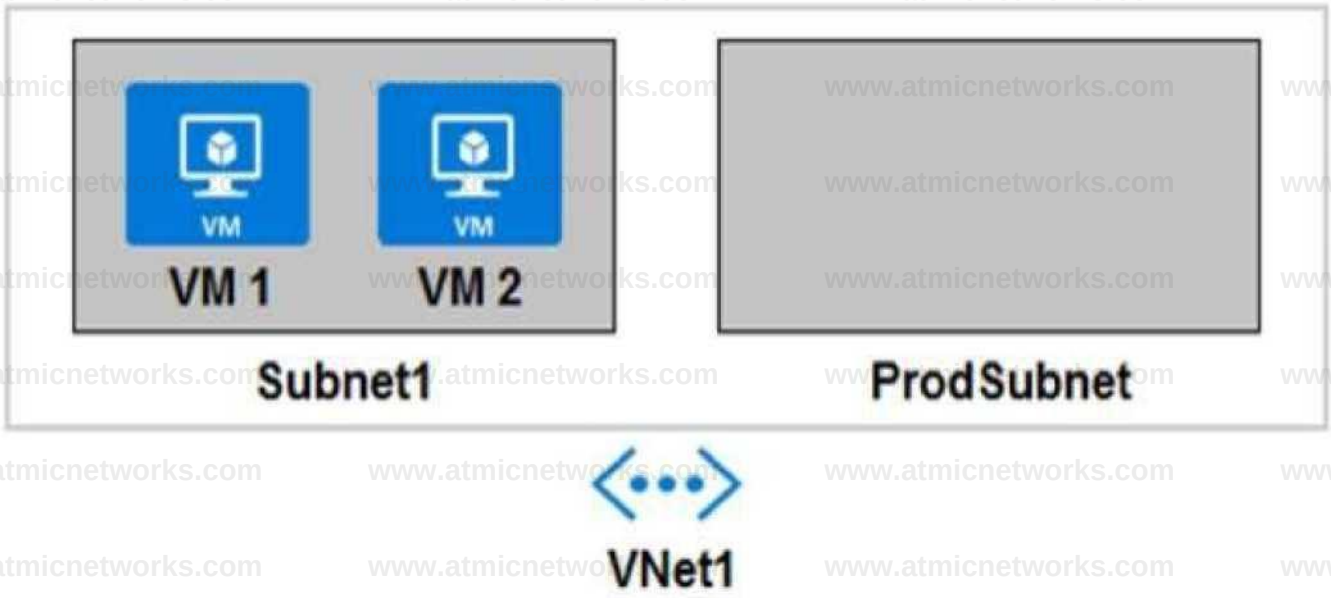
Box 2: A connection gateway resource

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

Question: 69
HOTSPOT

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

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



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

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

LOCATION	VIRTUAL NETWORK	SUBNET
West Europe	VNetl	ProdSubnet

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

NOTE: Each correct selection is worth one point.

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

Answer:

Explanation:

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

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

Question: 70

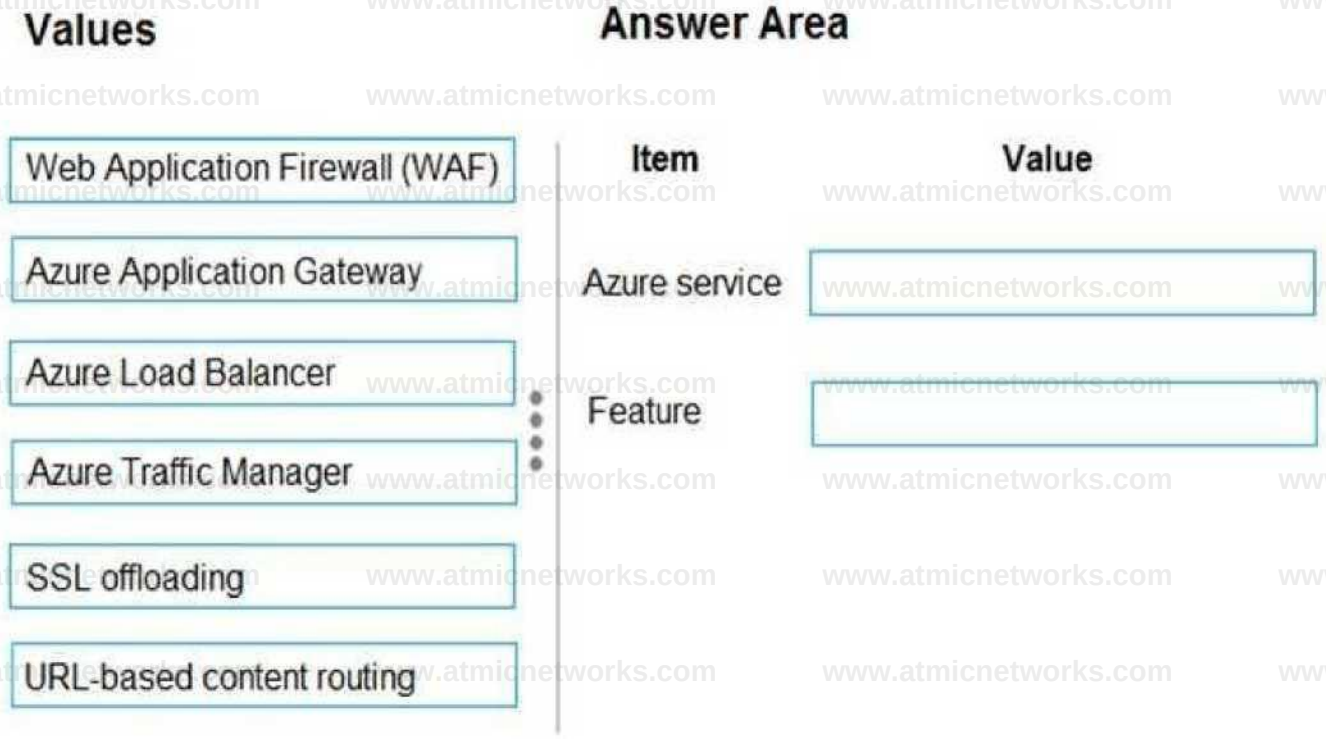
DRAG DROP

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

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

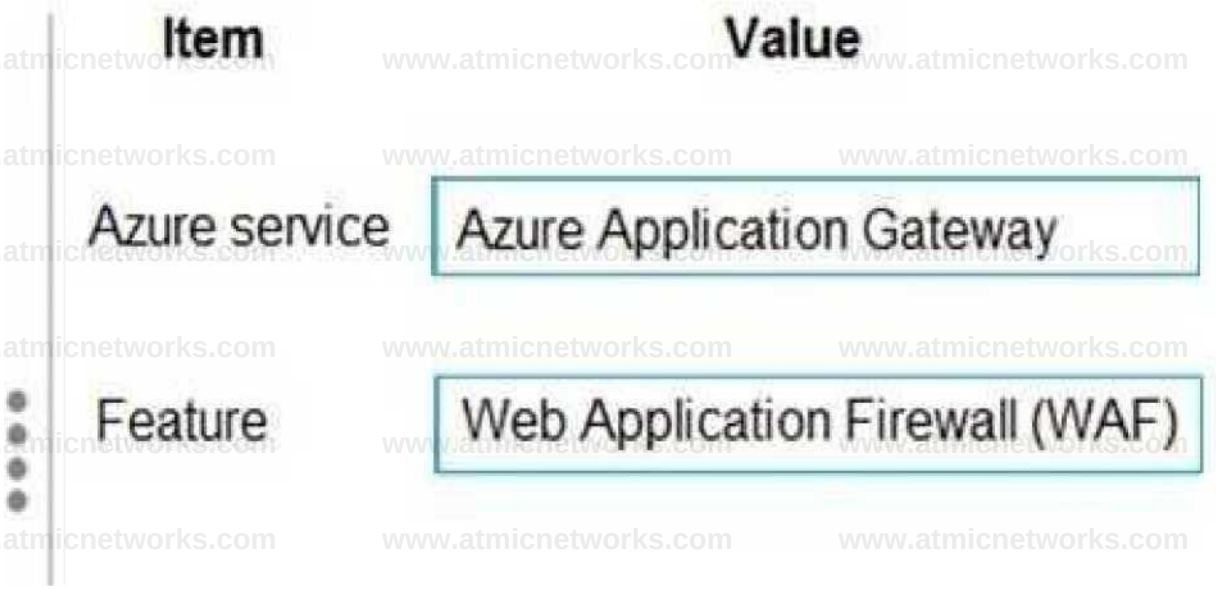
What should you recommend? To answer, drag the appropriate values to the correct items. Each value may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.



Answer:

Explanation:



Box 1: Azure Application Gateway

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

Box 2: Web Application Firwewall (WAF)

Application Gateway web application firewall (WAF) protects web applications from common vulnerabilities and exploits.

This is done through rules that are defined based on the OWASP core rule sets 3.0 or 2.2.9. There are rules that detects SQL injection attacks.

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

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

Question: 71

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)

Answer: A

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: 72

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

Answer: A

Explanation:

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

Question: 73

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
USWestfi rewall	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

Answer: B

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: 74

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

Answer: C

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: 75

You are developing a sales application that will contain several Azure cloud services and will handle different components of a transaction. Different cloud services will process customer orders, billing, payment, inventory, and shipping.
You need to recommend a solution to enable the cloud services to asynchronously communicate transaction information by using REST messages. What should you include in the recommendation?

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

Answer: A

Explanation:

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/en- us/azure/service-bus-messaging/service-bus-messaging-overview

Question: 76

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

Answer: C

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: 77

HOTSPOT

You are designing an Azure web app.

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

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

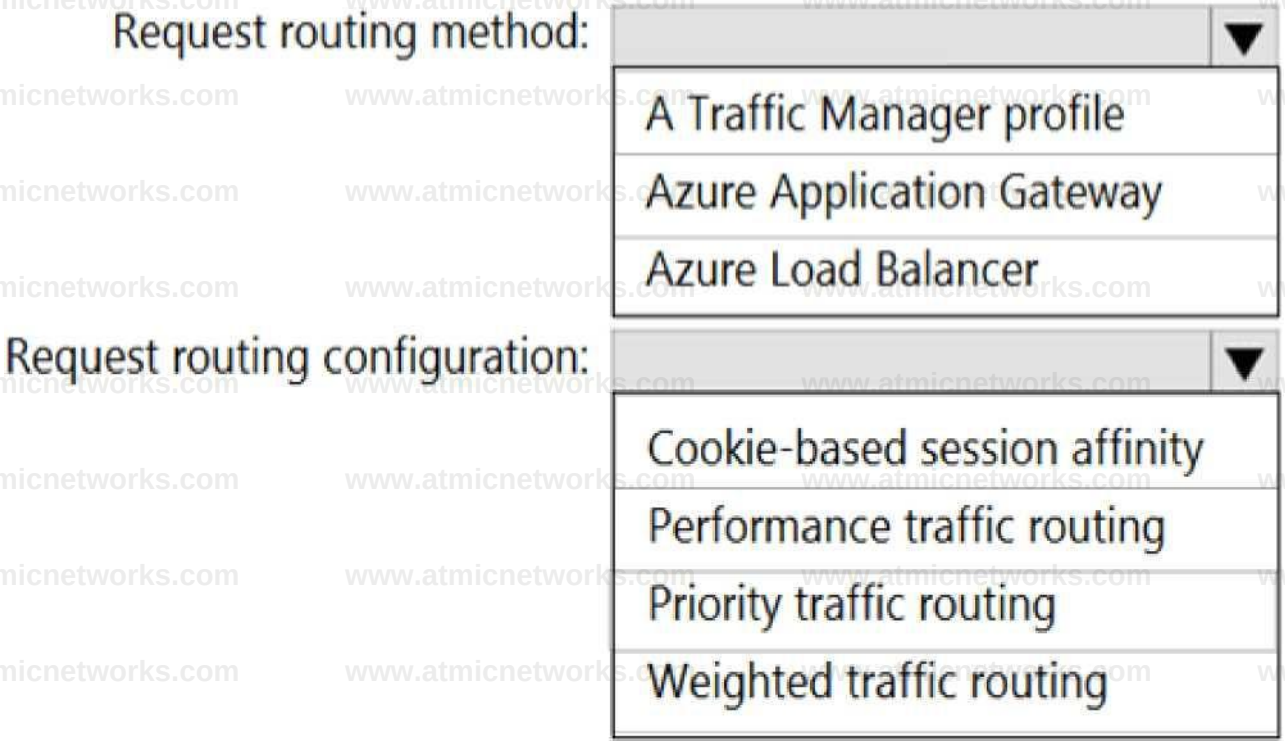
Users must always access the web app from the North Europe region, unless the region fails.

The web app must be available to users if an Azure region is unavailable.

Deployment costs must be minimized.

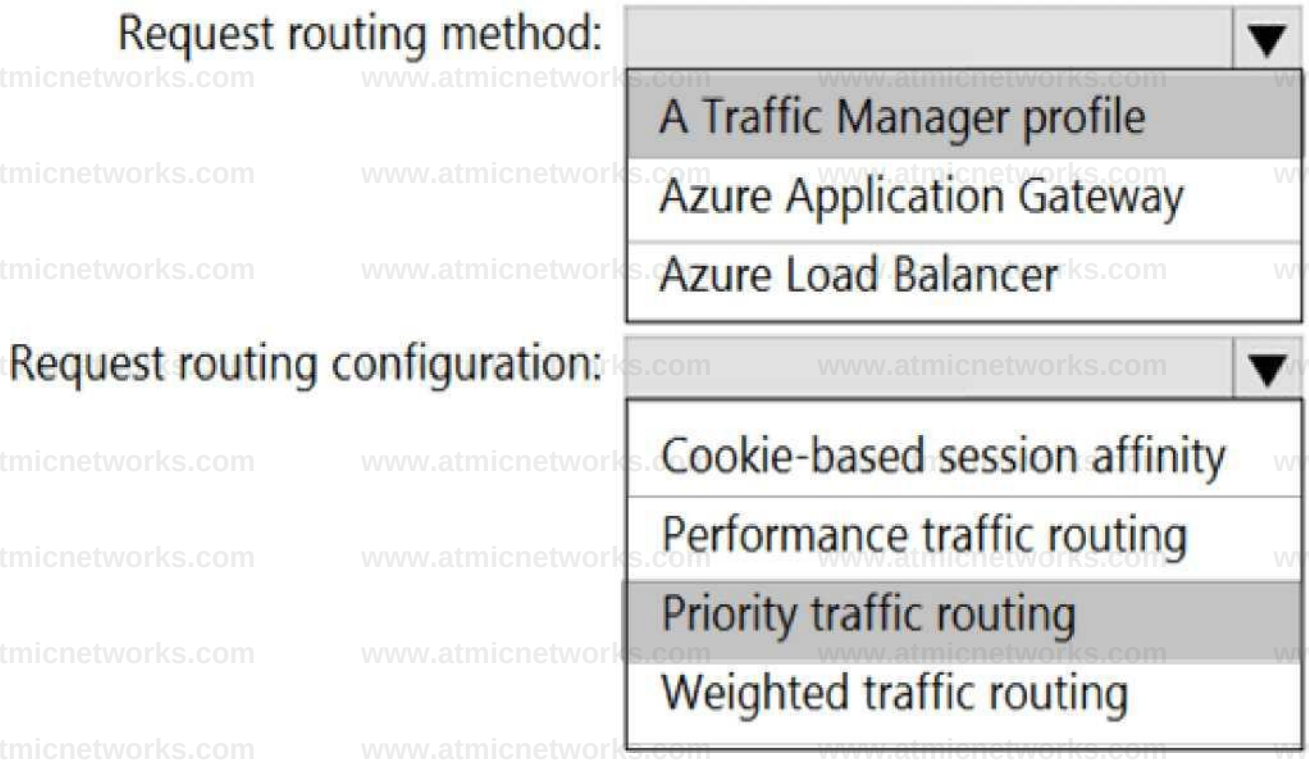
What should you include in the recommendation? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer:

Explanation:



https://docs.microsoft.com/en-us/azure/traffic-manager/traffic-manager-routing-methods#priority- traffic-routing-method

Question: 78

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

Answer: B

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: 79

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

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

Solution: You deploy a web app in an Isolated App Service plan.

Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:

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

Question: 80

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

Answer: A

Explanation:

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

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

Question: 81

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a

unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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

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

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

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

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

Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation:

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

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

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

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

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

Question: 82

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

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

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

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

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

Solution: You recommend using an Azure policy to enforce the resource group location.

Does this meet the goal?

A. Yes
B. No

Answer: A

Explanation:

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

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

Question: 83

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

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

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

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

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

Solution: You recommend creating resource groups based on locations and implementing resource locks on the

resource groups.

Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation:

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

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

Question: 84

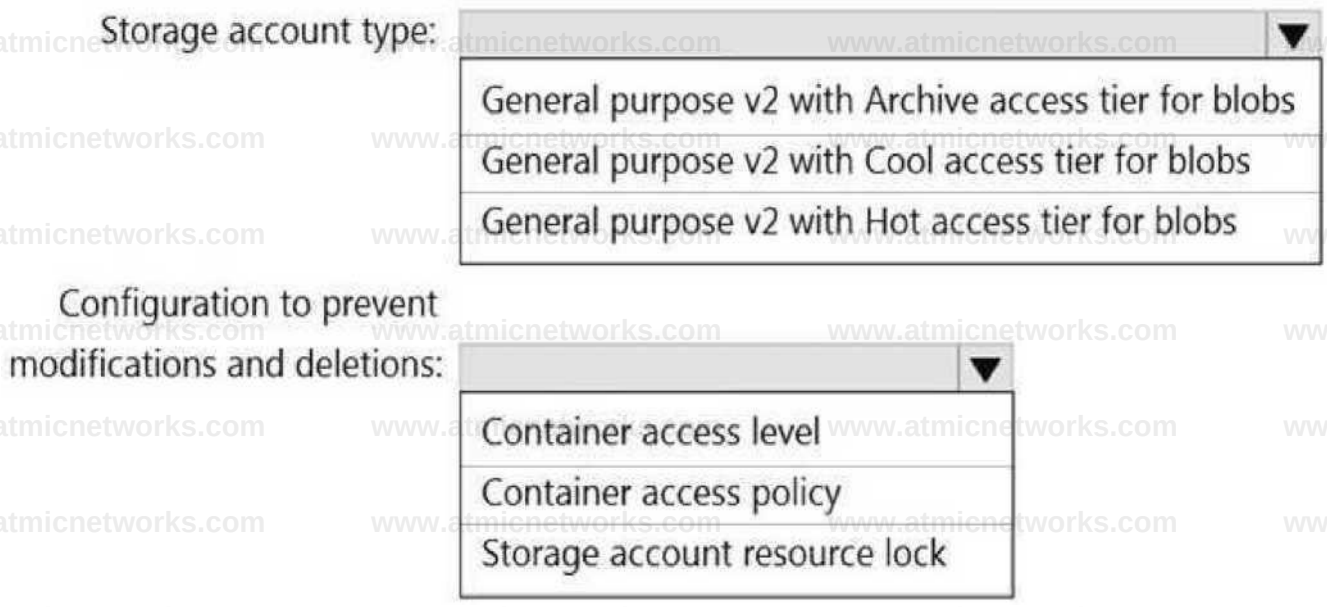
HOTSPOT

You are planning an Azure Storage solution for sensitive dat
a. The data will be accessed daily. The data set is less than 10 GB.
You need to recommend a storage solution that meets the following requirements:

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

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

NOTE: Each correct selection is worth one point.



Answer:

Explanation:

Storage account type: 1

General purpose v2 with Archive access tier for blobs

General purpose v2 with Cool access tier for blobs

General purpose v2 with Hot access tier for blobs

Configuration to prevent modifications and deletions: ▼

Container access level

Container access policy

Storage account resource lock

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

Archive - Optimized for storing data that is rarely accessed and stored for at least 180 days with flexible latency requirements, on the order of hours.

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

Hot - Optimized for storing data that is accessed frequently.

Box 2: Storage account resource lock

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

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

CanNotDelete means authorized users can still read and modify a resource, but they can't delete the resource.

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

Reference:

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

Question: 85

HOTSPOT

You have an Azure subscription that contains a virtual network named VNET1 and 10 virtual machines. The virtual machines are connected to VNET1.

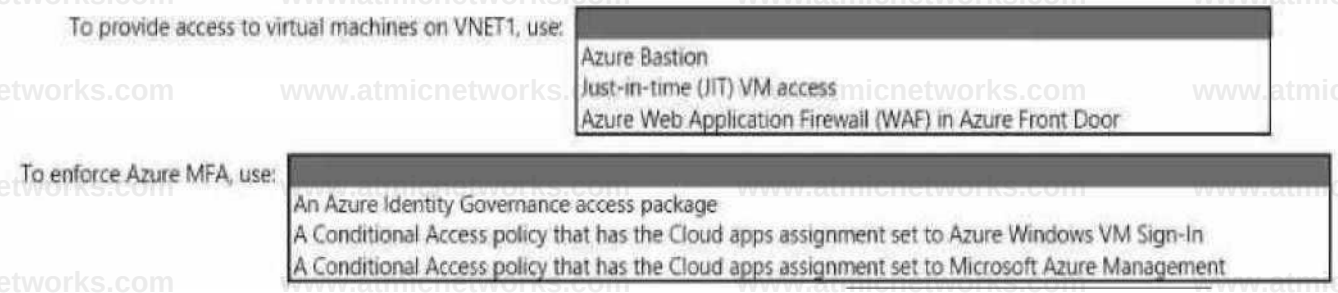
You need to design a solution to manage the virtual machines from the internet. The solution must meet the following requirements:

- Incoming connections to the virtual machines must be authenticated by using Azure Multi-Factor Authentication (MFA) before network connectivity is allowed.
- Incoming connections must use TLS and connect to TCP port 443.

• The solution must support RDP and SSH.

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

Answer Area



Answer:

Explanation:

To provide access to virtual machines on VNET1, use: Just-m-time (JIT) VM access

To enforce Azure MFA use. An Azure Identity Governance access package

Question: 86

HOTSPOT

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

The API must meet the following requirements:

Implement Azure Functions
Provide public read-only operations
Do not allow write operations
You need to recommend configuration options.

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

Topic	Value
Allowed authentication methods	All methods GET only GET and POST only GET, POST, and OPTIONS only
Authorization level	Function Anonymous Admin

Explanation:

Topic	Value
Allowed authentication methods	All methods GET only GET and POST only GET, POST, and OPTIONS only
Authorization level	Function Anonymous Admin

Allowed authentication methods: GET only

Authorization level: Anonymous

The option is Allow Anonymous requests. This option turns on authentication and authorization in App Service, but defers authorization decisions to your application code. For authenticated requests,

App Service also passes along authentication information in the HTTP headers.

This option provides more flexibility in handling anonymous requests.

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

Question: 87

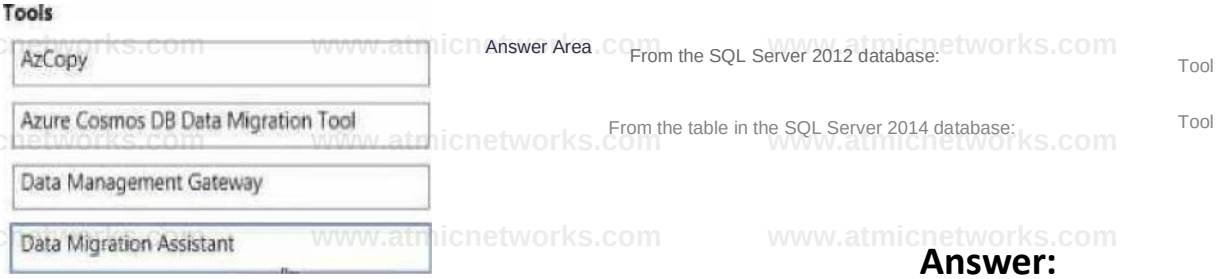
DRAG DROP

You plan to import data from your on-premises environment to Azure. The data Is shown in the following table.

On-premises source	Azure target
A Microsoft SQL Server 2012 database	An Azure SQL database
A table in a Microsoft SQL Server 2014 database	An Azure Cosmos D8 account that uses the SQL API

What should you recommend using to migrate the data? To answer, drag the appropriate tools to the correct data sources- Each tool 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.



Answer:

Explanation:

Answer Area

From the SQL Server 2012 database: Data Migration Assistant

From the table in the SQL Server 2014 database: Azure Cosmos DB Data Migration Tool

Reference:
https://docs.microsoft.com/en-us/azure/dms/tutorial-sql-server-to-azure-sql
https://docs.microsoft.com/en-us/azure/cosmos-db/import-data

Question: 88

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

Contoso establishes a partnership with another company named Fabrikam. IncL

Fabrikam does not have an existing Azure Active Directory (Azure AD) tenant and uses third-party OAuth 2.0 identity

management to authenticate its users.

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

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

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

What should you include in the solution?

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

Answer: B

Explanation:

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

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

Reference:

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

Question: 89

DRAG DROP

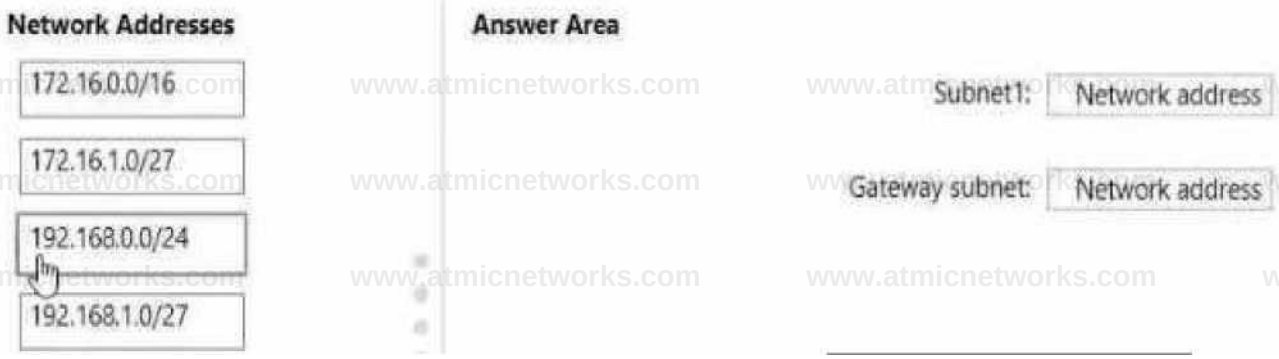
You have an on-premises network that uses an IP address space of 172.16.0.0/16. You plan to deploy 25 virtual machines to a new Azure subscription. You identify the following technical requirements:

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

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

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

NOTE: Each correct selection is worth one point.



Answer:

Explanation:

Question: 90

You have an Azure subscription.

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

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

Which scaling option should you recommend?

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

Answer: B

Explanation:

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

Question: 91

You have an Azure subscription.

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

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

Which scaling option should you recommend?

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

Answer: C

Explanation:

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

Question: 92

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

Name	Type	Purpose
Appl	Web app	Processes customer orders
Functionl	Function	Check product availability at vendor 1
Function	Function	Check product availability at vendor 2
storagel	Storage account	Stores order processing logs

The order processing system will have the following transaction flow:

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

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

D18912E1457D5D1DDCBD40AB3BF70D5D

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

A. an Azure Data Factory pipeline
B. an Azure Service Bus queue

C. an Azure Event Grid domain
D. an Azure Event Hubs capture

Answer: A

Explanation:

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

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

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

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

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

Question: 93

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

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

Which service should you include in the recommendation?

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

Answer: C

Explanation:

"Azure Front Door, which focuses on global load-balancing and site acceleration, and Azure CDN Standard, which offers static content caching and acceleration. The new Azure Front Door brings

together security with CDN technology for a cloud-based CDN with threat protection and additional capabilities. "

Question: 94

HOTSPOT

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

App1 stores database connection strings in KV1.

App1 performs the following types of requests to KV1:

Get
List
Wrap
Delete
Unwrap
Backup
Decrypt
Encrypt

You are evaluating the continuity of service for App1.

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

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

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

NOTE: Each correct selection is worth one point.

To where will KV1 fail over?

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

During the failover, which request type will be unavailable?

Backup Decrypt Delete Encrypt
Get
List
Unwrap
Wrap

Answer:

Explanation:

To where will KV1 fail over?

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

During the failover, which request type will be unavailable?

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

Box 1: A server in the same paired region

The contents of your key vault are replicated within the region and to a secondary region at least 150 miles away, but within the same geography to maintain high durability of your keys and secrets.

Box 2: Delete

During failover, your key vault is in read-only mode. Requests that are supported in this mode are: List certificates
Get certificates
List secrets
Get secrets
List keys
Get (properties of) keys
Encrypt
Decrypt
Wrap
Unwrap
Verify
Sign
Backup

ence:

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

Question: 95

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 West Europe Azure region,

You need to recommend a storage account type to store the data files and a replication solution for the storage account.

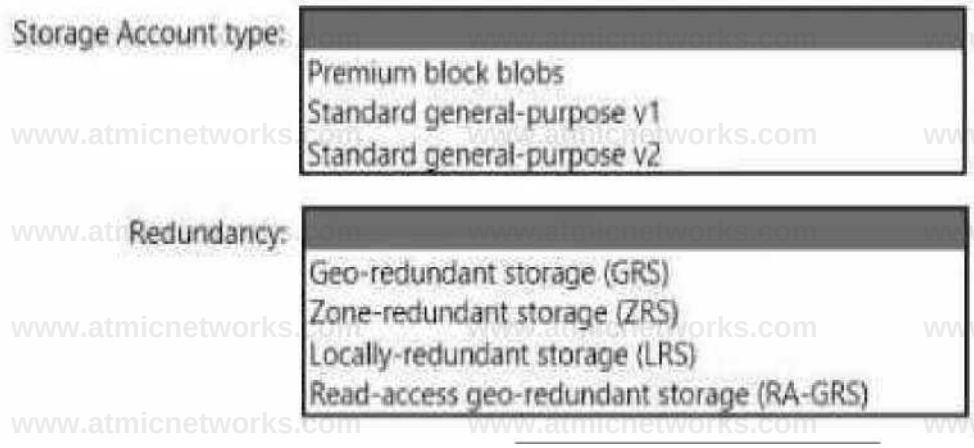
The solution must meet the following requirements:

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

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

NOTE: Each correct selection is worth one

Answer Area



Explanation:

Answer:

Account Type: StorageV2

Replication solution: Zone-redundant storage (ZRS)

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

https://docs.microsoft.com/en-us/azure/storage/common/storage-redundancy#supported-azure- storage-services

https://docs.microsoft.com/en-us/azure/storage/common/storage-account-overview#types-of- storage-accounts

Data must be available if a single Azure datacenter fails. It means the storage account must support ZRS replication. Also, solution should support storage tiers. Only General-purpose V2 supports ZRS and storage tiers.

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

Question: 96

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.

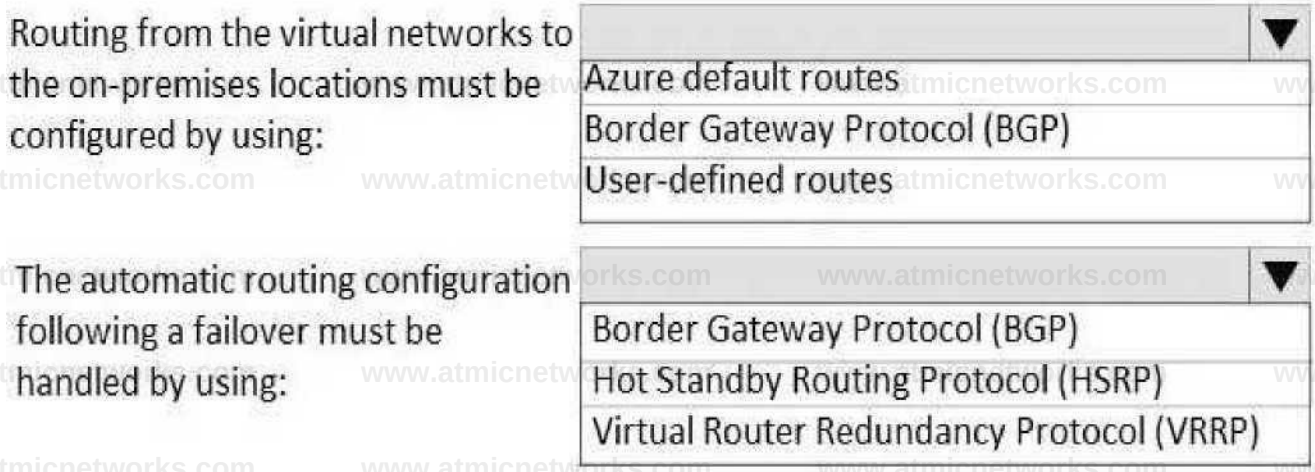
You need to recommend a solution that meets the following requirements:

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.

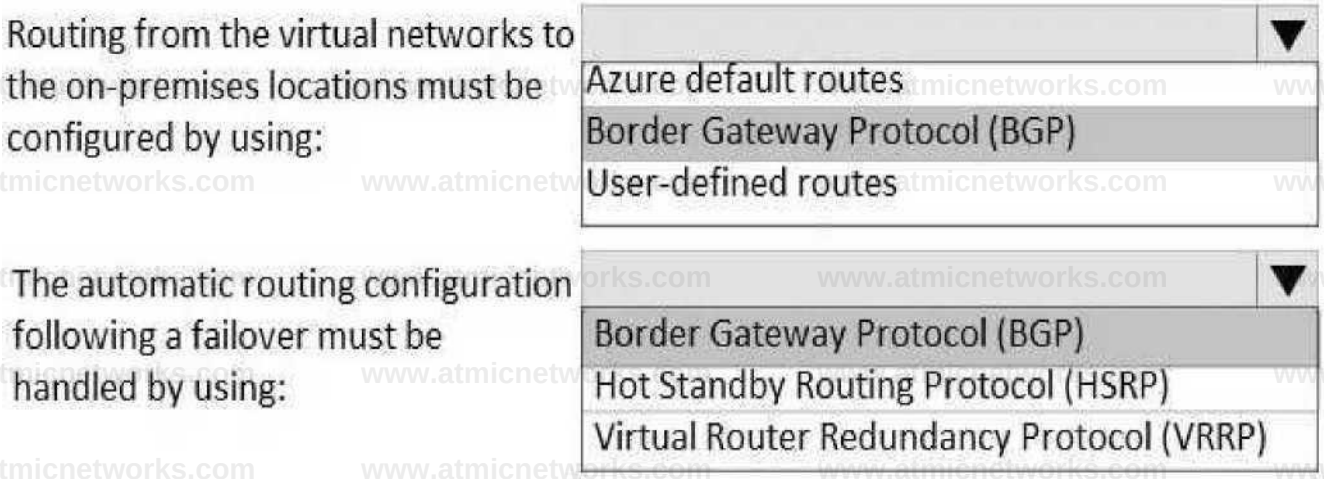
What should you include in the recommendation? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer:

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-with- expressroute-privatepeering

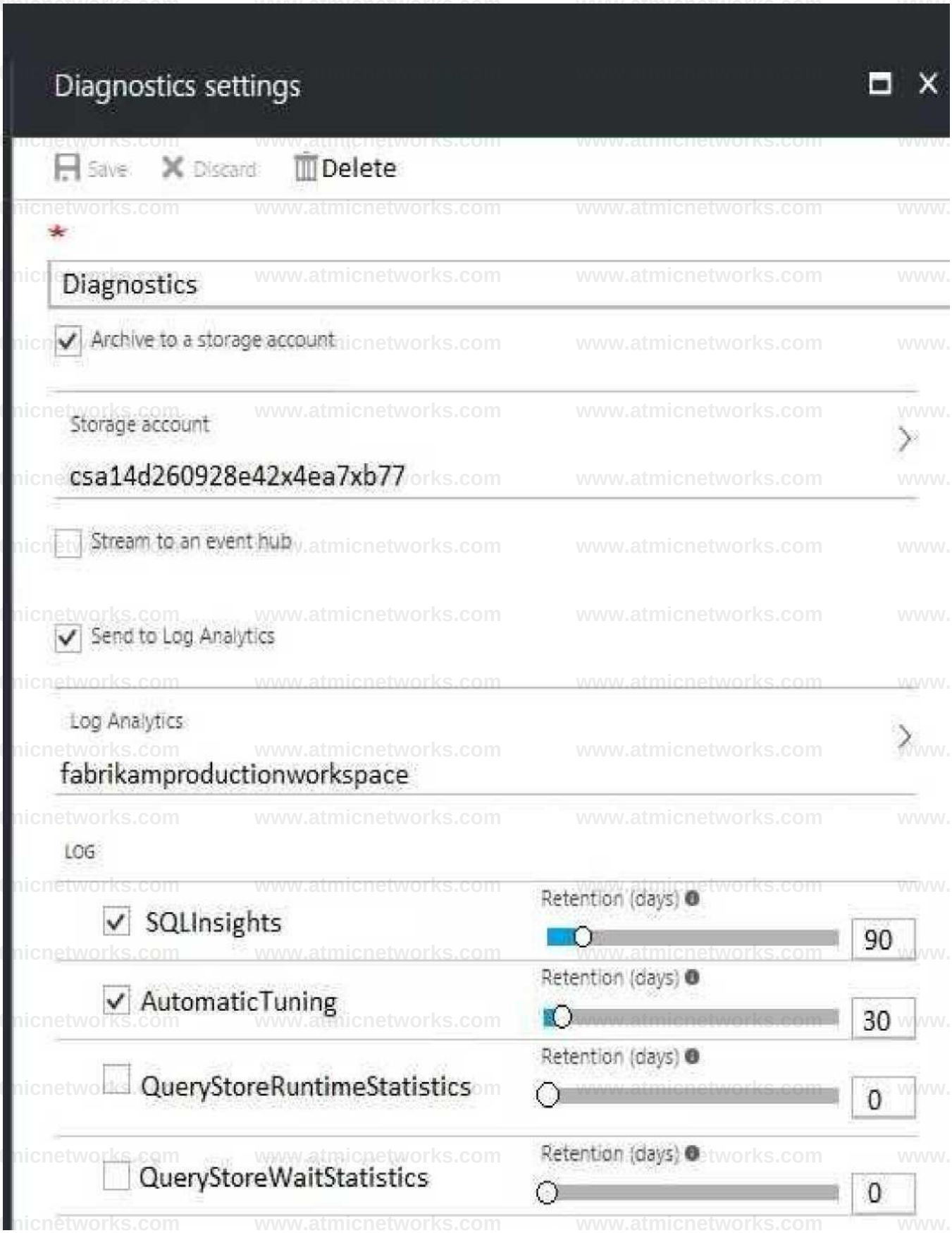
https://docs.microsoft.com/en-us/azure/expressroute/expressroute-optimize-routing#suboptimal- routing-from-customer-to-microsoft

Question: 97

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.

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:

Explanation:

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**

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: 98

You have an Azure subscription.

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

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

What should you include in the recommendation?

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

Answer: D

Explanation:

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

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

Question: 99

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.

Answer Area

Key Vault integration method: I

- Key Vault references in Application settings
- Key Vault references in Appsettingsjson
- Key Vault references in Web,config
- Key Vault SDK

Key Vault permissions for the managed identity: I

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

Answer:

Explanation:

Answer Area

Key Vault Integration method; Key Vault references in Web,config

Key Vault permissions for the managed identity: Secrets: Get

Question: 100

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.

Azure Policy effect to use:
Append
EnforceOPAConstraint
EnforceRegoPolicy
Modify

Azure Active Directory (Azure AD) object and R8AC 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

Answer:

Explanation:

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

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: 101

HOTSPOT

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

Name	Type	Kind	Location
storage 1	Azure Storage account	Storage	East US
storage2	Azure Storage account	Storage V2	East US
Workspace 1	Azure Log .Analytics workspace	Not *applicable*	East US
Workspace2	Azure Log .Analytics workspace	*Not applicable*	East US
Hub!	Azure event hub	*Not applicable*	East US

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

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

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

NOTE: Each correct selections is worth one point.

Statements	Yes	No
You can add a new diagnostic setting that archives SQLInsights logs to storage2.	Q	Q
You canadd a new diagnostic setting that sends SQLI nsights logs to Workspace?.	Q	O
You can add a new diagnostic setting that sends SQLInsights logs to Hubl.	Q	Q

Answer:

Explanation:

Answer Area

Statements	Yes	No
You can add a new diagnostic setting that archives SQL Insights logs to storage!	®	
You can add a new diagnostic setting that sends SQL Insights logs to Workspace!	®>	
You can add a new diagnostic setting that sends SQL Insights logs to Hubl.	®	O

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-logging- streaming-export-configure

Question: 102

You plan to deploy an application named App1 that will run on five Azure virtual machines.

Additional virtual machines will be deployed later to run App1.

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

Ensure that the virtual machines can authenticate to Azure Active Directory (Azure AD) to gain access to an Azure key vault, Azure Logic Apps instances, and an Azure SQL database.

Avoid assigning new roles and permissions for Azure services when you deploy additional virtual machines.

Avoid storing secrets and certificates on the virtual machines.

Which type of identity should you include in the recommendation?

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

Answer: D

Explanation:

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

Incorrect Answers:
8: System-assigned managed identity cannot be shared. It can only be associated with a single Azure resource.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure- resources/overview

Question: 103

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:

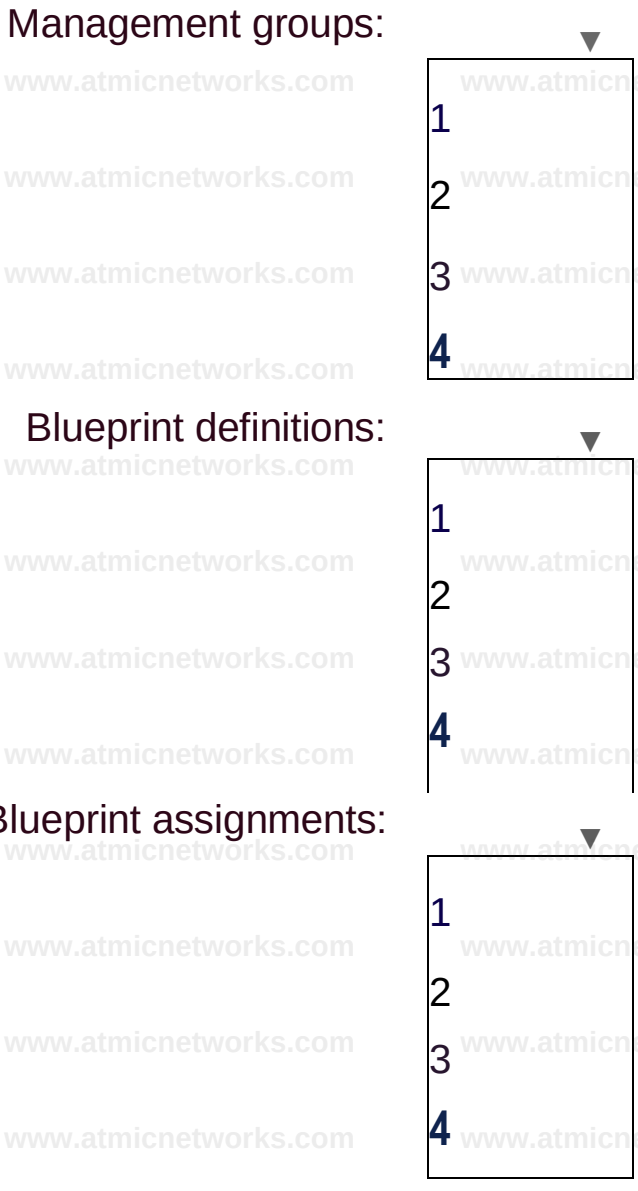
A resource group
An Azure web app
Custom role assignments
An Azure Cosmos DB account

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.



Answer:

Explanation:

Box 1: 2

One management group for East, and one for West.

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

Box 2: 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: 104

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.

Configuration to perform on the virtual machines:

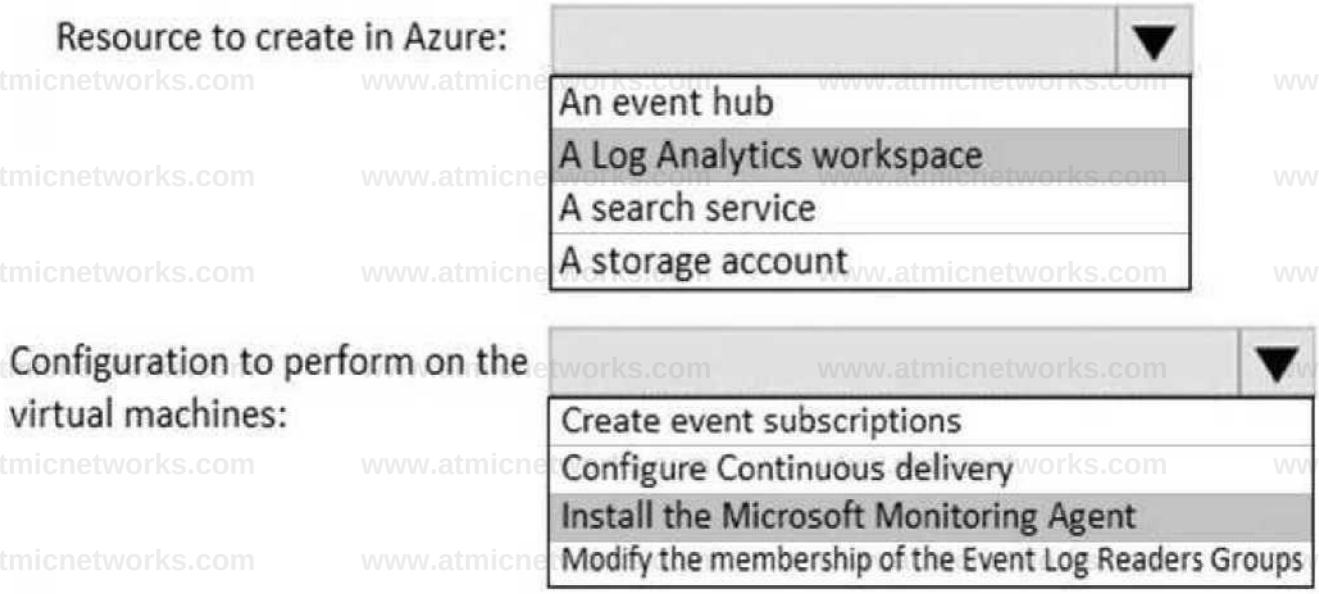
Create event subscriptions
Configure Continuous
Install the Microsoft Monitoring Agent
Modify the membership of the Event Log Readers Groups

Resource to create in Azure:

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

Answer:

Explanation:



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

Question: 105
HOTSPOT

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

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

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

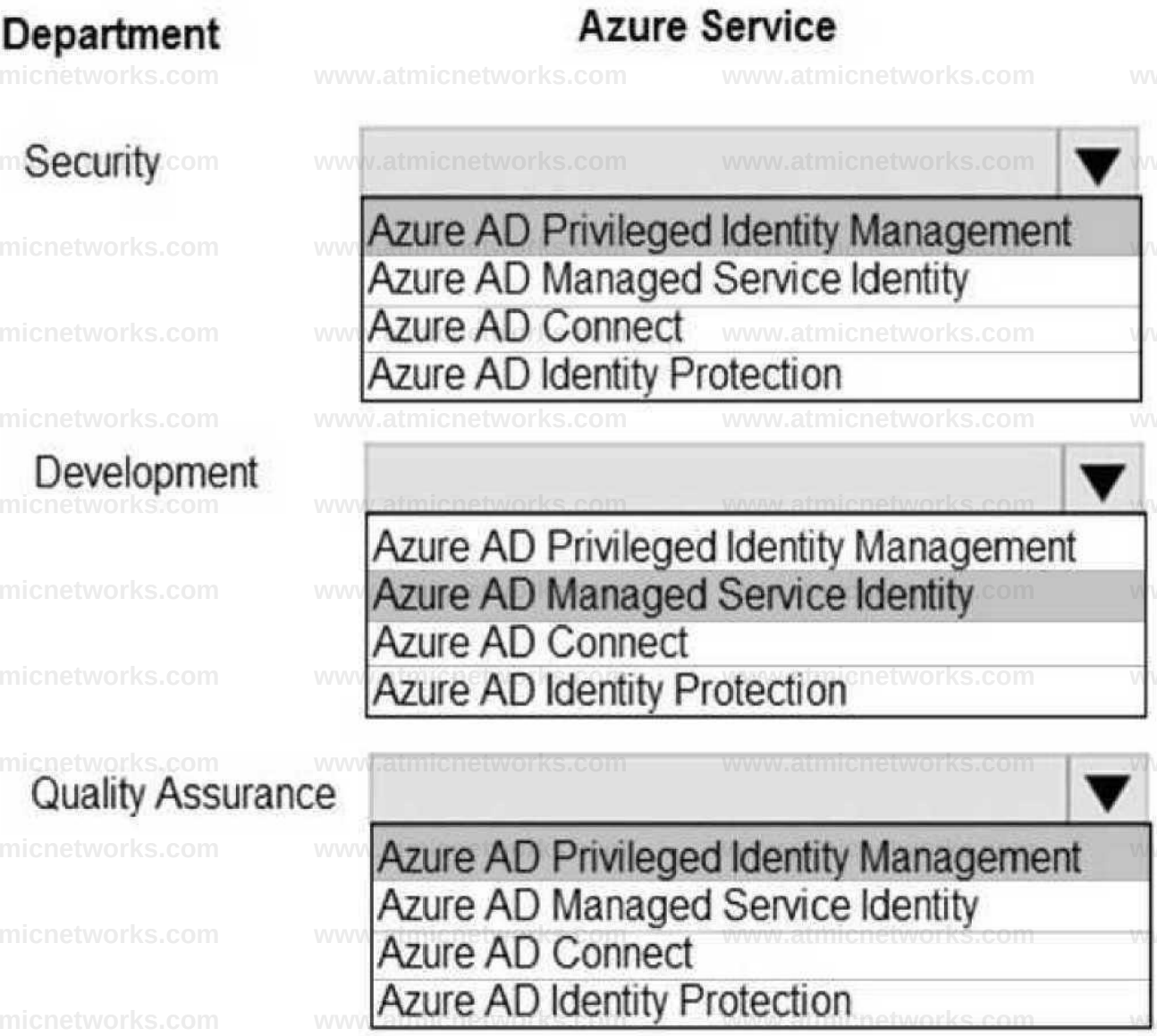
What should you recommend? To answer, configure the appropriate options in the dialog box in the answer area.

NOTE: Each correct selection is worth one point.

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

Answer:

Explanation:



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

Question: 106

You have an application that is used by 6,000 users to validate their vacation requests. The application manages its own credential

Users must enter a username and password to access the application. The application does NOT support identity providers.

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

Which SSO method should you use?

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

Answer: A

Explanation:

Question: 107

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.

Azure Services

Azure Event Grid

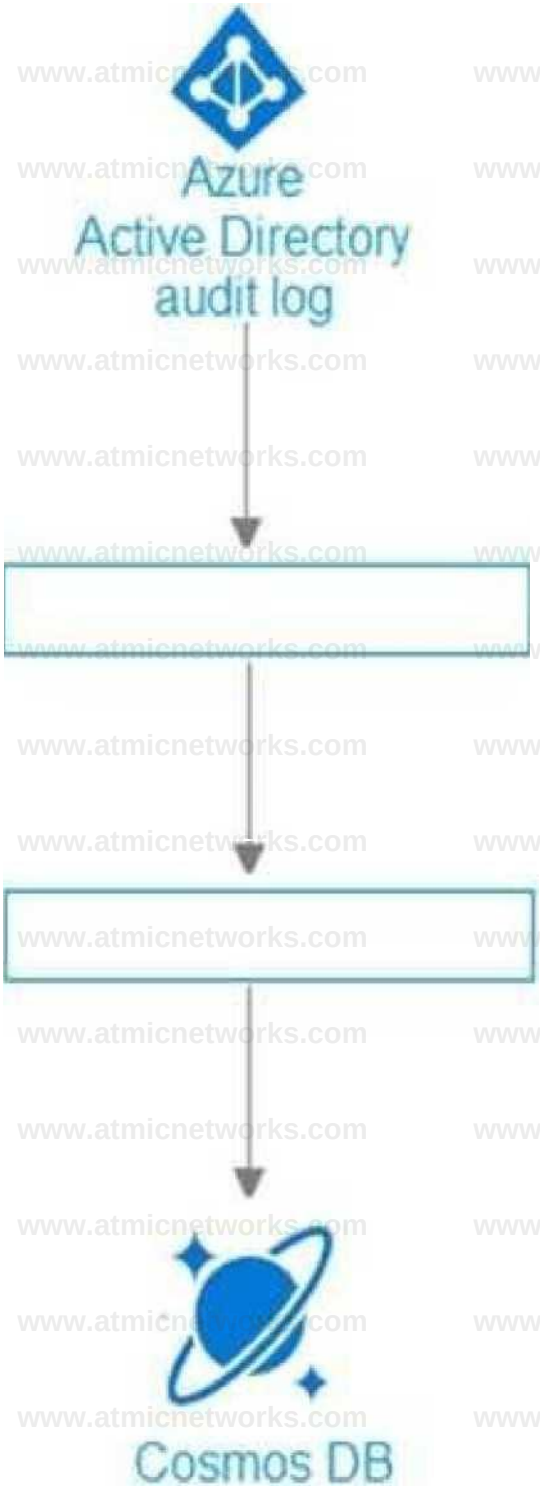
Azure Event Hubs

Azure Functions

Azure Log

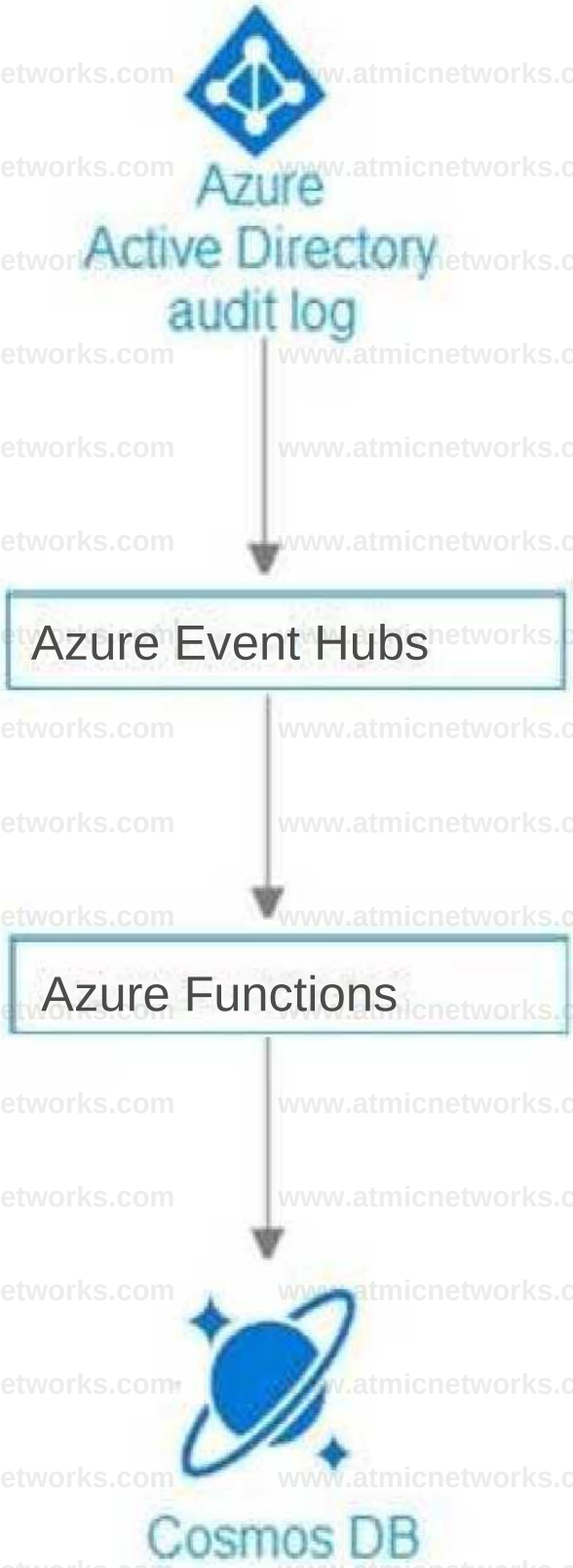
Azure Notification Hubs

Answer Area



Answer:

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-azure- monitor-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-hubs-trigger?tabs=csharp

Question: 108

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.

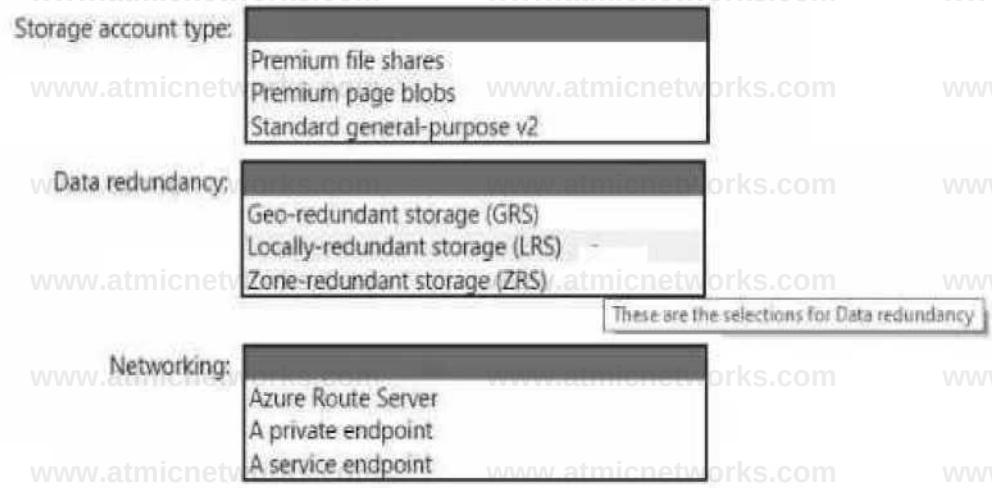
You need to ensure that the storage account meets the following requirements:

- 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.

Answer Area



Answer:

Explanation:

Answer Area

Storage account type: Premium file shares

Data redundancy: Locally-redundant storage LRS)

Networking: Azure Route Server

Question: 109

You have data files in Azure Blob Storage.

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

You need to transform the data by using mapping data flow.
Which service should you use?

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

Answer: C

Explanation:

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

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

Question: 110

You plan to deploy an app that will use an Azure Storage account.
You need to deploy the storage account. The solution must meet the following requirements:

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

What should you deploy?

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

Answer: D

Explanation:

Question: 111

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)

Answer: C

Explanation:

Question: 112

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

Answer Area

Applicationl

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 vl 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:

Explanation:

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

Box 1: BloblBlobStorage with Premium performance and Zone-redundant storage (ZRS) replication.
BlockBlobStorage accounts: Storage accounts with premium performance characteristics for block blobs and append blobs. Recommended for scenarios with high transactions rates, or scenarios that use smaller objects or require consistently low storage latency.
Premium: optimized for high transaction rates and single-digit consistent storage latency.

Box 2: General purpose v2 with Standard performance..
General-purpose v2 accounts: Basic storage account type for blobs, files, queues, and tables. Recommended for most scenarios using Azure Storage.

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: 113

You have the resources shown in the following table.

Name	Type
ASI	Azure Synapse Analytics instance
CDBI	Azure Cosmos M SQL API Account

CDB1 hosts a container that stores continuously updated operational data.

You are designing a solution that will use ASI 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

Answer: D

Explanation:

Question: 114

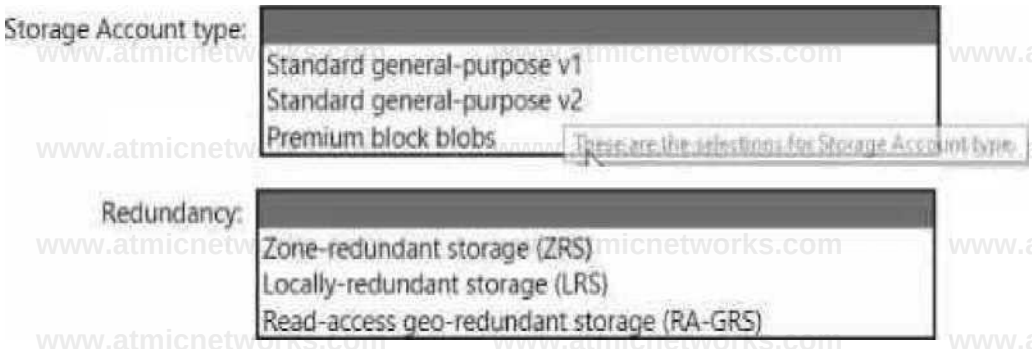
HOTSPOT

You plan to develop a new app that will store business critical dat a. 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.

Answer Area



Answer:

Explanation:

Answer Area

Storage Account type Standard general-purpose v2

Redundancy Read-access geo-redundant storage (RA-GRS)

Question: 115

HOTSPOT
O: 241
HOTSPOT

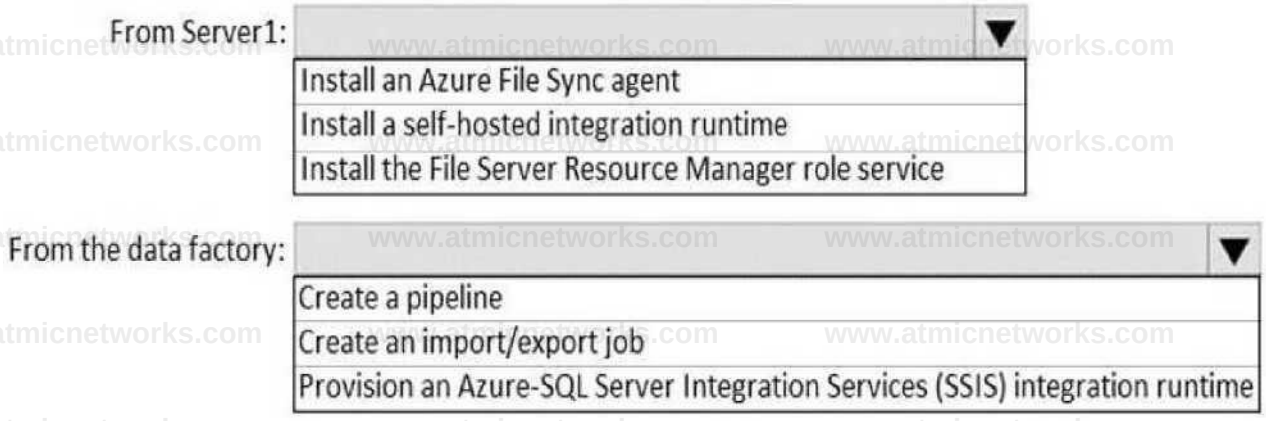
Your on-premises network contains a file server named Server1 that stores 500 GB of data.

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

You add a new data factory.

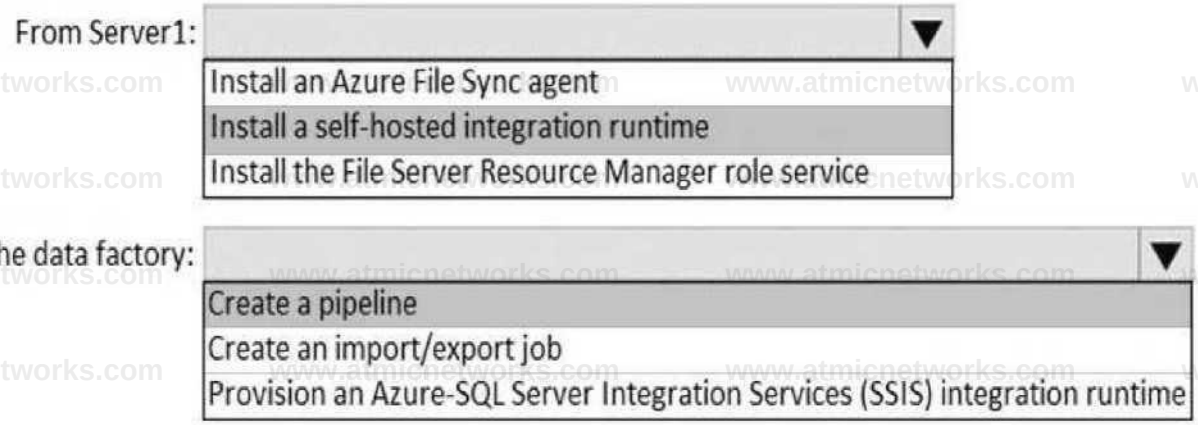
What should you do next? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer:

Explanation:



Box 1: Install a self-hosted integration runtime

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

Box 2: Create a pipeline

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

Reference:

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

https://docs.microsoft.com/pl-pl/azure/data-factory/tutorial-hybrid-copy-data-tool

syu31svc 3 months, 4 weeks ago

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

"A self-hosted integration runtime can run copy activities between a cloud data store and a data store 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 onpremises and cloud source data stores to a centralization data store in the cloud for further analysis"

Question: 116

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

Answer: A

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: 117

Your company has an Azure Web App that runs via the Premium App Service Plan. A development team will be using the Azure Web App. You have to configure the Azure Web app so that it can fulfil the below requirements.
Provide the ability to switch the web app from the current version to a newer version
Provide developers with the ability to test newer versions of the application before the switch to the newer version occurs
Ensure that the application version can be rolled back
Minimize downtime
Which of the following can be used for this requirement?

A. Create a new App Service Plan
B. Make use of deployment slots
C. Map a custom domain
D. Backup the Azure Web App

Answer: B

Explanation:

Question: 118

You have to deploy an Azure SQL database named db1 for your company. The databases must meet the following security requirements

When IT help desk supervisors query a database table named customers, they must be able to see the full number of each credit card
When IT help desk operators query a database table named customers, they must only see the last four

digits of each credit card number

A column named Credit Card rating in the customers table must never appear in plain text in the database system. Only client applications must be able to decrypt the information that is stored in this column

Which of the following can be implemented for the Credit Card rating column security requirement?

A. Always Encrypted
B. Azure Advanced Threat Protection
C. Transparent Data Encryption
D. Dynamic Data Masking

Answer: A

Explanation:

https://docs.microsoft.com/en-us/sql/relational-databases/security/encryption/always-encrypted-database-engine?view=sql-server-ver15

Question: 119

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

Your company has a line-of-business (LOB) application that was developed internally.

You need to implement. SAML single sign-on (SSO) and enforce multi-factor authentication (MFA) when users attempt to access the application from an unknown location.

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

NOTE: Each correct selection is worth one point.

A. Azure AD enterprise applications
B. Azure AD Identity Protection
C. Azure Application Gateway
D. Conditional Access policies
E. Azure AD Privileged Identity Management (PIM)

Answer: A,D

Explanation:

Question: 120

You ate designing an Azure governance solution.

All Azure resources must be easily identifiable based on the following operational information

environment, owner, department and cost center

You need 10 ensure that you can use the operational information when you generate reports for the Azure resources.

What should you include in the solution?

A. Azure Active Directory (Azure AD) administrative units
B. an Azure data catalog that uses the Azure REST API as a data source
C. an Azure policy that enforces tagging rules
D. an Azure management group that uses parent groups to create a hierarchy

Answer: C

Explanation:

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

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

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

Reference:
https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/decision-guides/resource- tagging

https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/tag-policies

Question: 121

You plan to automate the deployment of resources to Azure subscriptions.

What is a difference between using Azure Blueprints and Azure Resource Manager (ARM) templates?

A. ARM templates remain connected to the deployed resources.
B. Only ARM templates can contain policy definitions.
C. Blueprints remain connected to the deployed resources.
D. Only Blueprints can contain policy definitions.

Answer: C

Explanation:

With Azure Blueprints, the relationship between the blueprint definition (what should be deployed) and the blueprint assignment (what was deployed) is preserved. This connection supports improved tracking and auditing of deployments. Azure Blueprints can also upgrade several subscriptions at once that are governed by the same blueprint.

Reference:
https://docs.microsoft.com/en-us/answers/questions/26851/how-is-azure-blue-prints-different- from-resource-m.html

Question: 122

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

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

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

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

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

What should you recommend?

A. Configure a forest trust between the on-premises Active Directory forests of Contoso and Fabrikam.
B. Configure an organization relationship between the Office 365 tenants of Fabrikam and Contoso.
C. In the Azure AD tenant of Contoso, use MIM to create guest accounts for the Fabrikam developers.
D. Configure an AD FS relying party trust between the fabrikam and Contoso AD FS infrastructures.

Answer: C

Explanation:

Trust configurations - Configure trust from managed forests(s) or domain(s) to the administrative forest
A one-way trust is required from production environment to the admin forest.
Selective authentication should be used to restrict accounts in the admin forest to only logging on to the appropriate production hosts.

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

Question: 123

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

The solution must meet the following requirements:
Allow independent upgrades to each microservice
Deploy the solution on-premises and to Azure
Set policies for performing automatic repairs to the microservices
Support low-latency and hyper-scale operations
You need to recommend a technology.
What should you recommend?

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

Answer: A

Explanation:

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

Question: 124

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

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

Maintain access to the app in the event of a regional outage.
Support Azure Web Application Firewall (WAF).
Support cookie-based affinity.
Support URL routing.
What should you include in the recommendation?

A. Azure Front Door
B. Azure Load Balancer
C. Azure Traffic Manager
D. Azure Application Gateway

Answer: A

Explanation:

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

routing, cookie-based session affinity among others.

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

Question: 125

You have an Azure subscription.

Your on-premises network contains a file server named Server1. Server 1 stores 5 TB of company files that are accessed rarely.

You plan to copy the files to Azure Storage.

You need to implement a storage solution for the files that meets the following requirements:

- The files must be available within 24 hours of being requested.
- Storage costs must be minimized.

Which two possible storage solutions achieve this goal? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. Create a general-purpose v1 storage account. Create a blob container and copy the files to the blob container.

B. Create a general-purpose v2 storage account that is configured for the Hot default access tier. Create a blob container, copy the files to the blob container, and set each file to the Archive access tier.

C. Create a general-purpose v1 storage account. Create a file share in the storage account and copy the files to the file share.

D. Create a general-purpose v2 storage account that is configured for the Cool default access tier. Create a file share in the storage account and copy the files to the file share.

E. Create an Azure Blob storage account that is configured for the Cool default access tier. Create a blob container, copy the files to the blob container, and set each file to the Archive access tier.

Answer: B,E

Explanation:

https://docs.microsoft.com/en-us/azure/storage/blobs/manage-access-tier?tabs=portal

Question: 126

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

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

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

What should you include in the recommendation?

A. SQL Server Migration Assistant (SSMA)

B. Azure Data Catalog

C. Data Migration Assistant

D. Azure Data Factory

Answer: D

Explanation:

https://docs.microsoft.com/bs-cyrl-ba/azure/sql-database/sql-database-managed-instance-migrate

Quote from that page "Azure SQL Database and SQL Server databases in an Azure Virtual Machine. DMS is the recommended method of migration for your enterprise workloads.

If you use SQL Server Integration Services (SSIS) on your SQL Server on premises, DMS does not yet support migrating SSIS catalog (SSISDB) that stores SSIS packages, but you can provision Azure-SSIS Integration Runtime (IR) in Azure Data Factory (ADF) that will create a new SSISDB in a managed instance and then you can redeploy your packages to it, see Create Azure-SSIS IR in ADF.

To learn more about this scenario and configuration steps for DMS, see Migrate your on-premises database to managed instance using DMS."

https://docs.microsoft.com/en-us/azure/data-factory/how-to-migrate-ssis-job-ssms

Question: 127

HOTSPOT
You have the resources shown in the following table.

Name	Type	Resource group
VM1	Azure virtual machine	RG1
VW	On premises virtual machine	Wot *a^icab^*

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.

Answer:

Explanation:

VM1: Azure Lighthouse

VM2; Azure Migrate

Question: 128

HOTSPOT

You have the Azure resources shown in the following table.

Name	■ - Typ*	Description
VNET1	Virtual network	Connected to an on-premises network by using Express Route
VM1	Virtual machine	Configured as a DNS server
SQLD81	Azure SQL Database	Single instance
PEI	Private endpoint	Provides connectivity to SQL DEI
contoso.com	Private DNS zone	Linked to VNET1 and contains an A record for PEI
contoso.com	Public DNS zone	Contains a CNAME record for SQLD81

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.

Azure configuration: I

Configure VM1 to forward contoso.com to the public DNS zone.
Configure VM1 to forward contoso.com to the Azure-provided DNS at 16863.129.16.
In VNetl, configure a custom DNS server set to the Azure-provided DNS at 168.63.129.16.

On-premises DNS configuration: I

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:

Explanation:

Azure configuration: Configure VM1 to forward contoso.com to the public DNS zone. On-Premises DNS configuration: Forward contoso to the public DNS zone.

Question: 129

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

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

You have an Azure Storage account that contains two 1-GB data files named File1 and File2. The data files are set to use the archive access tier.

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

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

Does this meet the goal?

A. Yes
B. No

Answer: A

Explanation:

The data in the cool tier is "considered / intended to be stored for 30 days". But this is not a must. You can store data indefinitely in the cool tier. The mentioned reference (see below) even gives an example of large scientific or otherwise large data which is stored for long duration in the cool tier. https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blob-storage-tiers?tabs=azure-portal