EXAMDUMPS

# Microsoft

## AZ-305

### Designing Microsoft Azure Infrastructure Solutions

## QUESTION & ANSWERS

## QUESTION 1

You have the following storage accounts defined as part of your subscription.

| Name | Performance tier | Replication |
|---|---|---|
| udemytore1 | Premium | Locally-redundant storage (LRS) |
| udemytore2 | Standard | Geo-redundant storage (GRS) |
| udemytore3 | Standard | Locally-redundant storage (LRS) |

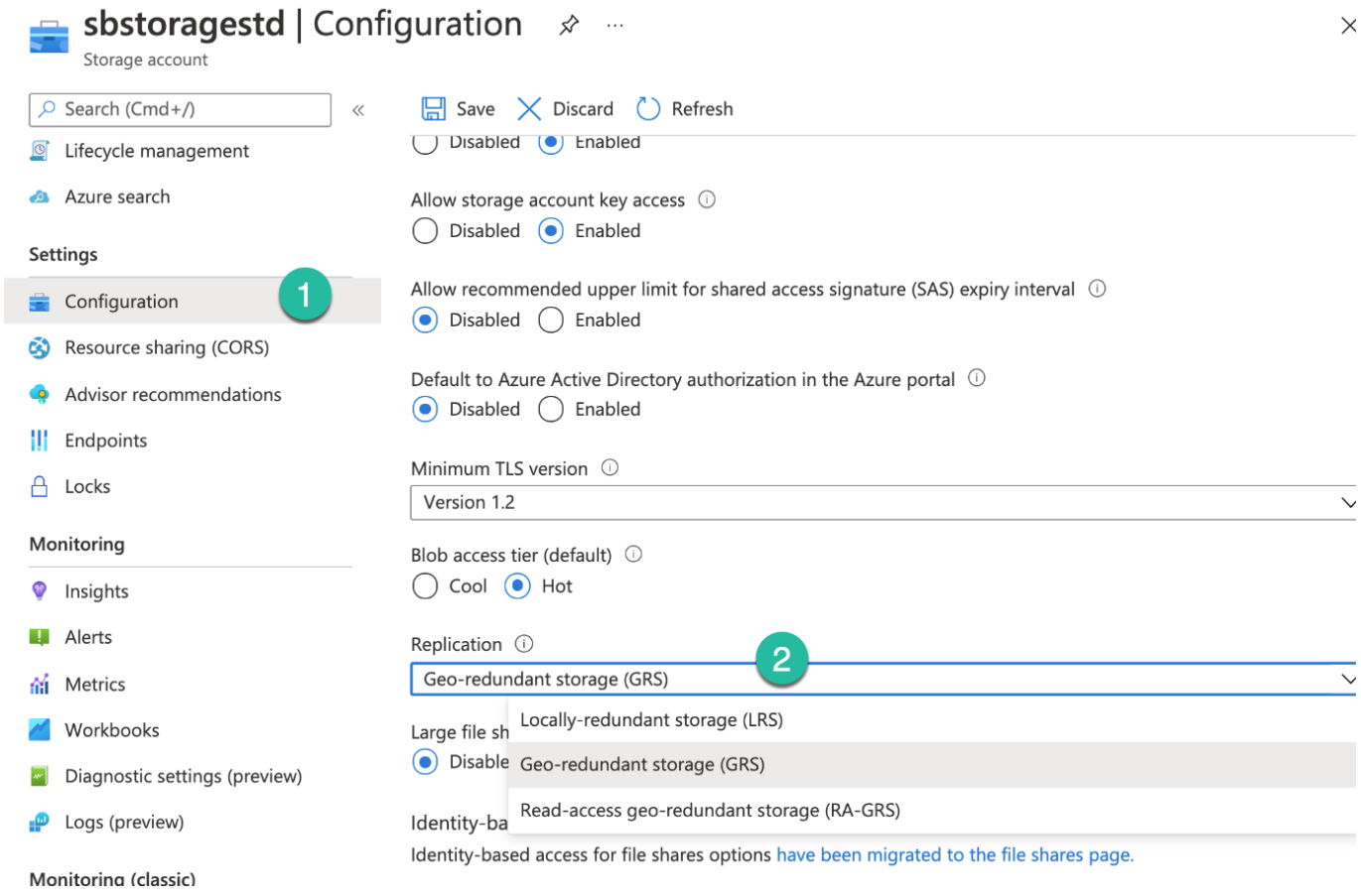
Can you convert udemytore3 to a GRS account?

A. Yes
B. No

## Correct Answer: A

### Explanation/Reference:

Azure Storage service provides several redundancy options for data availability and durability. These options include:
Locally-redundant storage (LRS) — stores three synchronous data copies within the same data center.
Zone-redundant storage (ZRS) — stores three synchronous copies within the Availability zones in the primary region. There are three availability zones per region. One copy of data is stored in one availability zone data center.
Geo-redundant storage (GRS/RA-GRS) stores six synchronous copies between primary and secondary regions. Each region has three synchronous copies stored in the same data center using LRS. First, data is stored in a primary region in three copies. Then it is asynchronously copied to the secondary region data center and stored in three synchronous copies using LRS.
Geo-zone-redundant storage (GZRS/RA-GZRS) stores four copies of the data: three synchronous copies within the Availability zones in the primary region (the same as ZRS), and one copy is replicated to the secondary region.
If you have Locally-redundant storage (LRS) account, you can change the replication type from the main storage account panel under the Settings section by selecting the Configuration item (Number 1). And then select the new replication type from the Replication dropdown (Number 2).




You can also use PowerShell or CLI to change the replication settings.
For more information on changing the storage account replication, please go to the following URL-
https://docs.microsoft.com/en-us/azure/storage/common/redundancy-migration?tabs=portal

## QUESTION 2

You have the following storage accounts defined as part of your subscription.

| Name | Performance tier | Replication |
|---|---|---|
| udemytore1 | Premium | Locally-redundant storage (LRS) |
| udemytore2 | Standard | Geo-redundant storage (GRS) |
| udemytore3 | Standard | Locally-redundant storage (LRS) |

Would udemytore2 have six copies of data?

A. Yes
B. No

## Correct Answer: A

### Explanation/Reference:

Azure Storage service provides several redundancy options for data availability and durability. These options include:
Locally-redundant storage (LRS) — stores three synchronous data copies within the same data center.
Zone-redundant storage (ZRS) — stores three synchronous copies within the Availability zones in the primary region. There are three availability zones per region. One copy of data is stored in one availability zone data center.
Geo-redundant storage (GRS/RA-GRS) stores six synchronous copies between primary and secondary regions. Each region has three synchronous copies stored in the same data center using LRS. First, data is stored in a primary region in three copies. Then it is asynchronously copied to the secondary region data center and stored in three synchronous copies using LRS.
Geo-zone-redundant storage (GZRS/RA-GZRS) stores four copies of the data: three synchronous copies within the Availability zones in the primary region (the same as ZRS), and one copy is replicated to the secondary region.
The udemytore2 storage account has Geo-redundant storage replication. Therefore, the data stored within udemytore2 account will have six copies.
For more information on storage account redundancy, please go to the following URL-
https://docs.microsoft.com/en-us/azure/storage/common/storage-redundancy

## QUESTION 3

A company needs to solution for the deployment of software for testing and production. The solution needs to adhere to the following requirements
Applications should be able to be deployed to several different environments and must run without the need of installation of dependencies
Application developers must have the flexibility when architecting their code
Which of the following would you recommend for the hosting of applications?

A. Azure worker role
B. Azure Kubernetes service
C. Azure Functions
D. Azure Batch

## Correct Answer: B

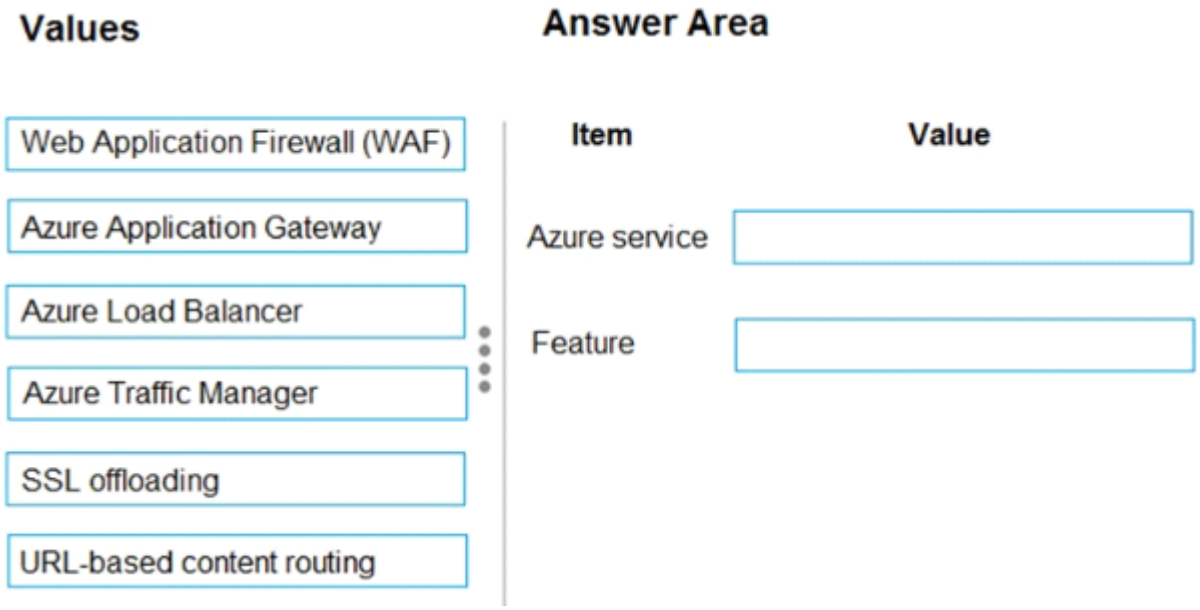
### Explanation/Reference:

Here the requirements are tending towards hosting Microservice based applications. And this is best accomplished by building container-based applications that can be deployed onto an Azure Kubernetes cluster
The other options are services that don’t provide options for ensuring application dependencies don’t need to be installed. With container-based applications, you can ensure that container images already have the dependencies pre-installed.

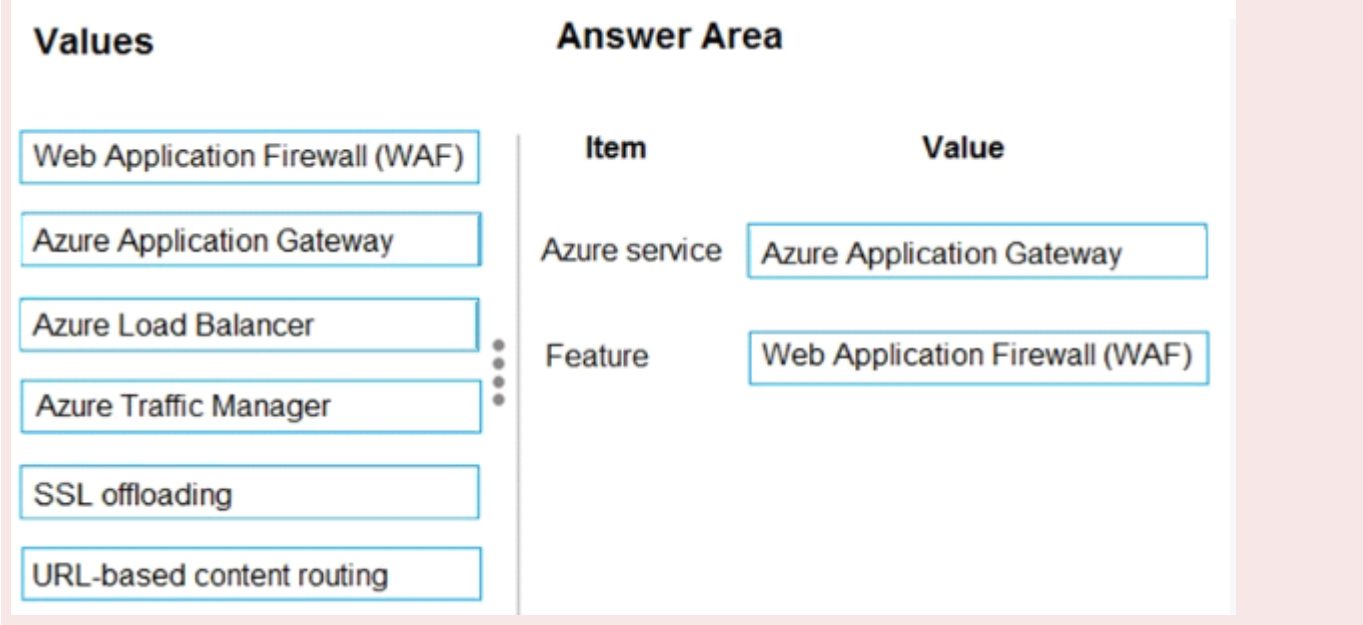
For more information on Azure Kubernetes , you can visit the below link
https://docs.microsoft.com/en-us/azure/aks/intro-kubernetes

## QUESTION 4

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.




**Correct Answer:**




### Explanation/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 5

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your company has deployed several virtual machines (VMs) on-premises and to Azure. Azure ExpressRoute has been deployed and configured for on-premises to Azure connectivity.
Several VMs are exhibiting network connectivity issues.
You need to analyze the network traffic to determine whether packets are being allowed or denied to the VMs.
Solution: Use Azure Network Watcher to run IP flow verify to analyze the network traffic
Does the solution meet the goal?

A. Yes
B. No

## Correct Answer: A

### Explanation/Reference:

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.
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 6

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 |
|---|---|---|---|
| storage1 | RG1 | East US | StorageV2 (general purpose v2) |
| storage2 | RG2 | Central US | BlobStorage |

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

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

**Answer Area**

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

**Correct Answer:**

**Answer:**

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

### Explanation/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 7

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

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

## Correct Answer: D

### Explanation/Reference:

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

## QUESTION 8

You have .NeT web service named service1 that has the following requirements.
Must read and write to the local file system.
Must write to the Windows Application event log.
You need to recommend a solution to host Service1 in Azure . The solution must meet the following requirements:
Minimize maintenance overhead.
Minimize costs.
What should you include in the recommendation?

A. an Azure App Service web app
B. an Azure virtual machine scale set
C. an App Service Environment (ASE)
D. an Azure Functions app

## Correct Answer: A

### Explanation/Reference:

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 9

Case Study
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

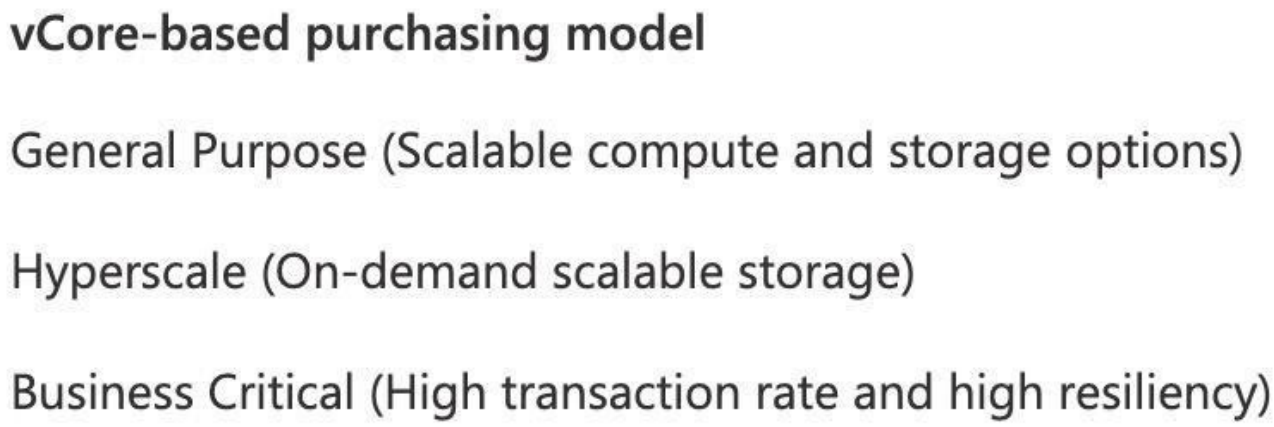
from Azure AD administrative units functionality.
HABInsurance needs to migrate the current IPSCustomers SQL database to a new fully managed SQL database in Azure that would be budget-oriented, balanced with scalable compute and storage options. The management team expects the Azure database service 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 the performance and availability of the multi-region AKS deployments during regional outages.
What purchasing model and service tier would you recommend for the IPSCustomers database?

A. vCore-based model
B. DTU-based model
C. Standard tier
D. General Purpose tier
E. Premium tier

**Correct Answer: A,D**

## Explanation/Reference:

Azure SQL Database service offers two purchasing models: DTU-based and vCore-based. Azure Managed instance service is based only on the vCore purchasing model. There are two deployment options for Azure SQL Database: Single database and Elastic pool — a collection of the single databases with shared resources. Microsoft recommends for the new projects to use the Virtual Core (v-Core)-based purchasing model. The vCore-based model gives users the flexibility to choose between provisioned compute resources, when you define the exact amount of the resources, and serverless compute resources, when you specify the autoscaling of the resources within a predefined range.
The vCore-based model has three service tiers: General purpose, Hyperscale, and Business Critical.




You should recommend provisioning an IPSCustomers database as an Azure SQL Database service using the vCore-based model and General purpose service tier. This tier is budget-oriented, balanced with scalable compute and storage options.
Options C and E are incorrect because these are the DTU-based service tiers.
Option B is incorrect because you need to create Azure SQL Database using the vCore-based model and not the DTU-based.
For more information about Azure SQL Database purchasing models and service tiers, please visit the below URLs:
https://docs.microsoft.com/en-us/azure/azure-sql/database/purchasing-models
https://docs.microsoft.com/en-us/azure/azure-sql/database/service-tiers-sql-database-vcore
https://docs.microsoft.com/en-us/azure/azure-sql/database/single-database-overview

## QUESTION 10

You have an on-premises network to which you deploy a virtual appliance.
You plan to deploy several Azure virtual machines and connect the on-premises network to Azure by using a Site-to-Site connection.
All network traffic that will be directed from the Azure virtual machines to a specific subnet must flow through the virtual appliance.
You need to recommend solutions to manage network traffic.
Which two options should you recommend? Each correct answer presents a complete solution.

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

## Correct Answer: C,D

### Explanation/Reference:

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

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

## QUESTION 11

You have to deploy an Azure SQL database named udemydb 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

## Correct Answer: A

### Explanation/Reference:

You can use the Always Encrypted feature to ensure that data in the database tables are encrypted at rest. This will ensure that the data values never appear in plain text in the database system. Also only client applications that have the required encryption key will be able to decrypt the data
Option B is incorrect since this is used to check for any sort of threats to the underlying database
Option C is incorrect since this is used to encrypt data at rest
Option D is incorrect since this is used to mask data in the database tables
For more information on the Always Encrypted, one can go to the following URL
https://docs.microsoft.com/en-us/sql/relational-databases/security/encryption/always-encrypted-database-engine?view=sql-server-ver15

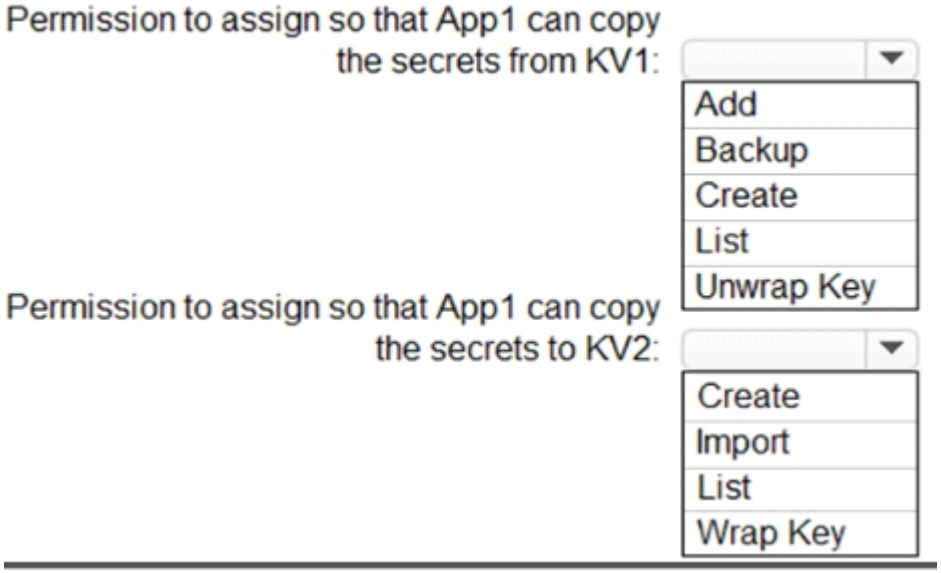
## QUESTION 12

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

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

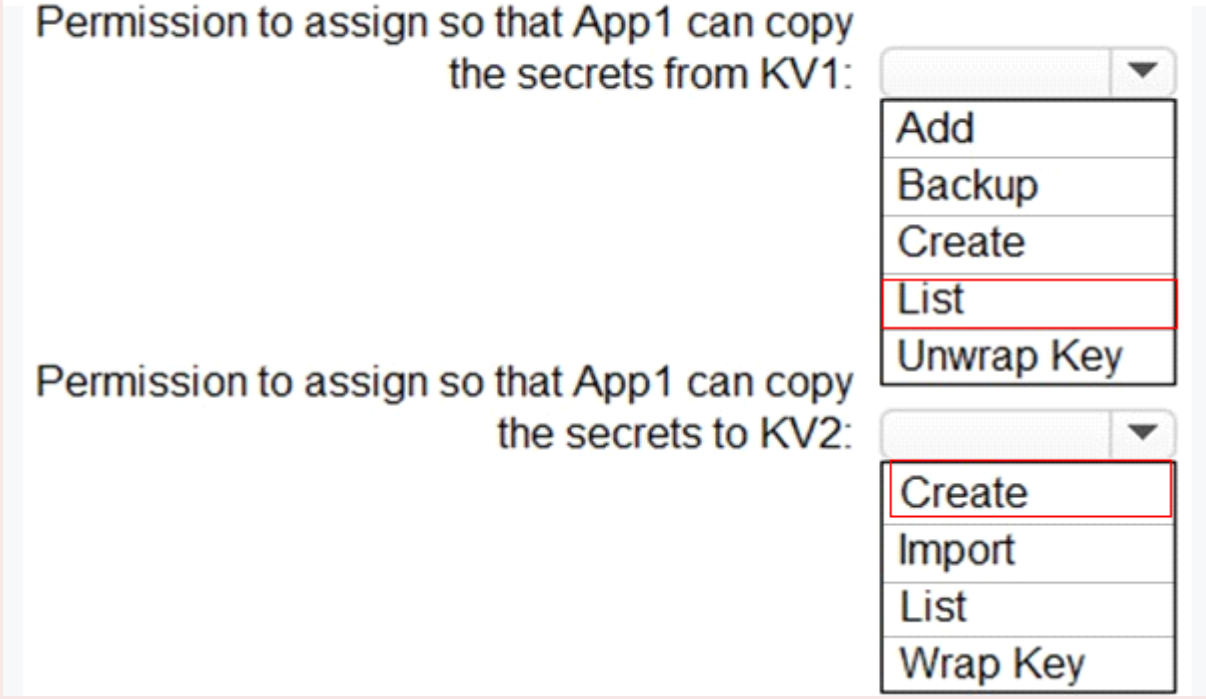
You need to configure permissions so that App1 can copy all the secrets from KV1 to KV2. App1 currently has the Get permission for the secrets in KV1.

Which additional permissions should you assign to App1? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.




**Correct Answer:**

**Answer:**




### Explanation/Reference:

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

## QUESTION 13

A company needs to host a set of applications on Azure virtual machines. There are different requirements for each of the applications
Maintain reliable performance on a set of virtual machines
Ensure application is running in the event of a data center failure
Which of the following services can you recommend for the “Maintain reliable performance on a set of virtual machines” requirement?

A. Azure Availability Zones
B. Azure Application Gateway
C. Azure Scale Sets
D. Azure Traffic Manager

## Correct Answer: C

### Explanation/Reference:

To ensure the reliable performance of the applications running on the set of virtual machines, you need to use Azure Scale Sets. Azure Virtual Machine Scale Sets service helps create and manage a group of VMs behind a load balancer. The configuration of these machines must be the same, and

they should run on the same base OS image. The VM scale sets can automatically increase or decrease VM instances depending on the scaling rules and resource demand. Scale sets provide high availability for your applications. You can use scale sets for large-scale services, like compute, big data, and containers.
All other options are incorrect.
For more information about Azure Virtual Machine Scale Sets, please visit the following URL:
https://docs.microsoft.com/en-us/azure/virtual-machine-scale-sets/overview

## QUESTION 14

What compute solution would you recommend for the Insurance processing system?

A. Azure App Service
B. Azure VM scale sets
C. Azure Container Instances
D. Azure Availability Zones

## Correct Answer: B

### Explanation/Reference:

From the requirements statement:
“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.”
To ensure the automatic scaling performance of the system running on the set of virtual machines, you need to use Azure Virtual Machine Scale Sets.
Azure Virtual Machine Scale Sets service helps create and manage a group of VMs behind a load balancer. The configuration of these machines must be the same, and they should run on the same base OS image. The VM scale sets can automatically increase or decrease VM instances depending on the scaling rules and resource demand. Scale sets provide high availability for your applications. You can use scale sets for large-scale services, like compute, big data, and containers.
All other options are incorrect.
For more information about Azure Virtual Machine Scale Sets, please visit the following URL:
https://docs.microsoft.com/en-us/azure/virtual-machine-scale-sets/overview

## QUESTION 15

Your organization has multiple Azure Cosmos DB accounts. You need to recommend what API to use for applications functionality. Which of the following two APIs would you use to host a JSON document?

A. SQL
B. Table
C. Gremlin
D. Cassandra
E. MongoDB

**Correct Answer: A,E**

## Explanation/Reference:

Azure Cosmos DB is a multi-model globally distributed NoSQL database. Cosmos DB stores data in atom-record-sequence
(ARS) format. It unites under one roof several data management systems and exposes them in the form of APIs. You can
select between the Core (SQL) API and MongoDB API (document model), Cassandra API (column-oriented model), Gremlin
API (graph model), and Table API (key-value model). You should select the default Cosmos DB API: Core (SQL) for the new
projects. If you have an existent database in formats that Cosmos DB API supports and do not want to deal with
application migration, the best way is to bring the data to Cosmos DB and use provided APIs for your application. For
example, suppose you have a MongoDB database with the purchase orders in different formats that are suitable for your
customers. In that case, you can bring data to Cosmos DB with native MongoDB tools, like mongodump and
mongorestore. And use all MongoDB queries in your apps for the data access now in Cosmos DB. But if the business logic
of your application will get better data representation, for example, in a graph, you should use Gremlin API in your
applications instead of the Core.
Cosmos DB Core (SQL) API and MongoDB API use the document data model and store data in JSON format. Core API
provides support for SQL queries. With SQL API, you can use stored procedures, triggers, and user-defined functions.
MongoDB API uses wire protocol for MongoDB. Using MongoDB API, you can use applications written in .Net, Node,
Python, Java, or Rubi and access the MongoDB document structures in Cosmos DB.
All other options are incorrect.
For more information on Cosmos DB – SQL and MongoDB APIs, please visit the below
URLshttps://docs.microsoft.com/en-us/azure/cosmos-db/choose-api
https://docs.microsoft.com/en-us/learn/modules/choose-api-for-cosmos-db/3-analyze-the-decision-criteria
https://docs.microsoft.com/en-us/azure/cosmos-db/mongodb/mongodb-introduction
https://docs.microsoft.com/en-us/azure/cosmos-db/sql/modeling-data

## QUESTION 16

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

**Correct Answer: A**

## Explanation/Reference:

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

## QUESTION 17

The application will host video files that range from 50 MB to 12 GB. The application will use certificate-based authentication and will be available to users on the internet.
You need to recommend a storage option for the video files. The solution must provide the fastest read performance and must minimize storage costs.
What should you recommend?

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

**Correct Answer: C**

## Explanation/Reference:

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

## QUESTION 18

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

**Correct Answer: A**

## Explanation/Reference:

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

## QUESTION 19

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

**Correct Answer: B**

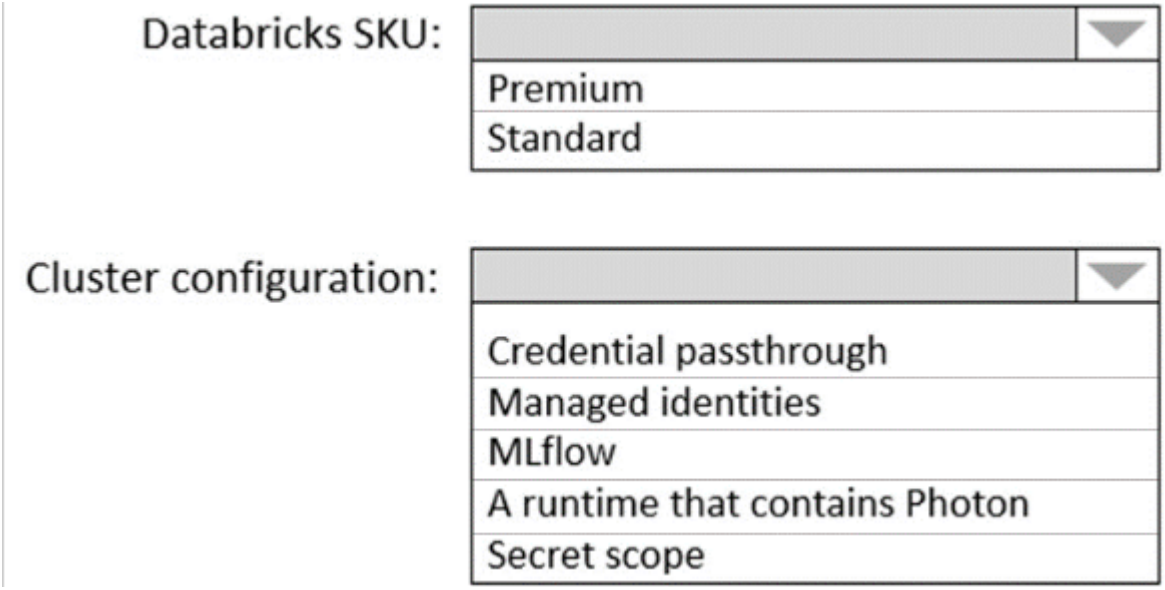
## Explanation/Reference:

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

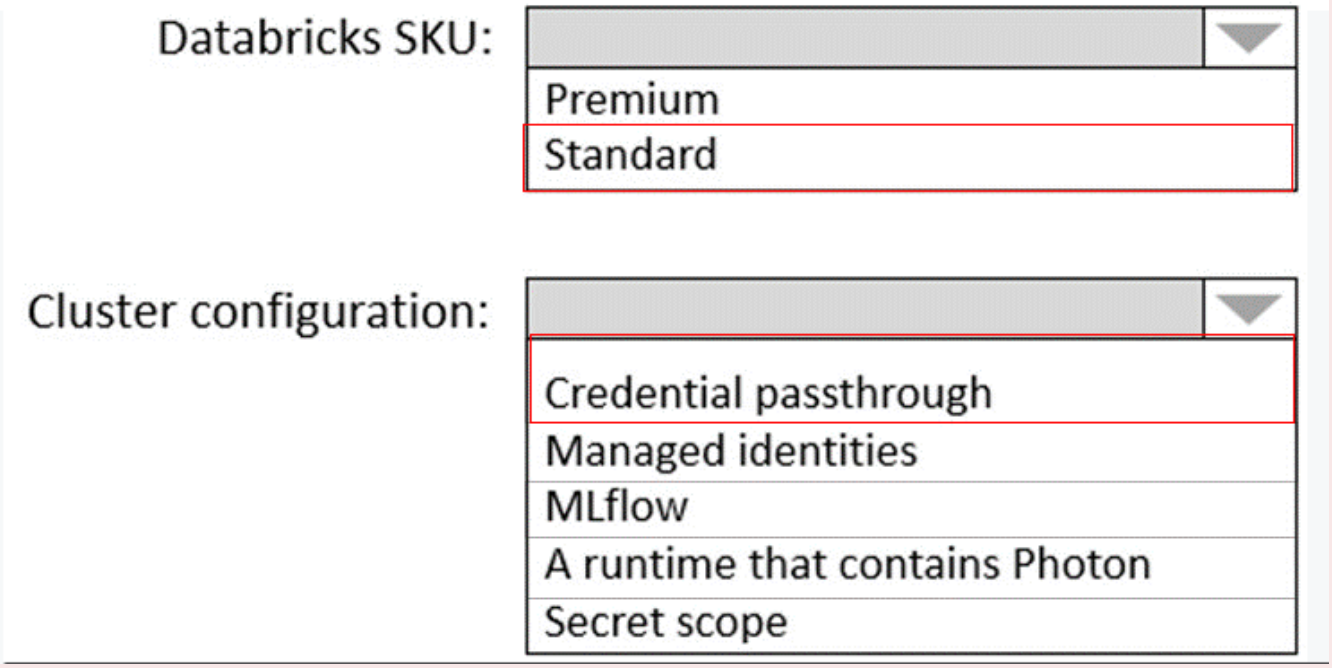
## QUESTION 20

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.




**Correct Answer:**

**Answer:**




### Explanation/Reference:

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

## QUESTION 21

Your company has offices in the United States, Europe, Asia, and Australia.
You have an on-premises app named App1 that uses Azure Table storage. Each office hosts a local instance of App1.
You need to upgrade the storage for App1. The solution must meet the following requirements:
Enable simultaneous write operations in multiple Azure regions.
Ensure that write latency is less than 10 ms.
Support indexing on all columns.
Minimize development effort.
Which data platform should you use?

A. Azure SQL Database
B. Azure SQL Managed Instance
C. Azure Cosmos DB
D. Table storage that uses geo-zone-redundant storage (GZRS) replication

## Correct Answer: D

### Explanation/Reference:

Azure Cosmos DB Table API has

Single-digit millisecond latency for reads and writes, backed with <10-ms latency reads and <15-ms latency writes at the 99th percentile, at any scale, anywhere in the world.
Automatic and complete indexing on all properties, no index management.
Turnkey global distribution from one to 30+ regions. Support for automatic and manual failovers at any time, anywhere in the world.
https://docs.microsoft.com/en-us/azure/cosmos-db/table-support

## QUESTION 22

Your company currently has an application that is hosted on their on-premises environment. The application currently connects to two databases in the on-premises environment. The databases are named whizlabdb1 and whizlabdb2.
You have to move the databases onto Azure. The databases have to support server-side transactions across both of the databases.
You decide to deploy the databases to an Azure SQL database-managed instance.
Would this fulfill the requirement?

A. Yes
B. No

## Correct Answer: A

### Explanation/Reference:

When it comes to distributed transactions, this is supported for the Azure SQL Managed Instance. If there are multiple instances, you need to create a Server Trust Group and the instances need to be added to the Server Trust group.
For more information on distributed transactions in the cloud, one can visit the following URL
https://docs.microsoft.com/en-us/azure/azure-sql/database/elastic-transactions-overview

## QUESTION 23

You are designing a microservices architecture that will be hosted in an Azure Kubernetes Service (AKS) cluster. Apps that will consume the microservices will be hosted on Azure virtual machines. The virtual machines and the AKS cluster will reside on the same virtual network.
You need to design a solution to expose the microservices to the consumer apps. The solution must meet the following requirements:
* Ingress access to the microservices must be restricted to a single private IP address and protected by using mutual TLS authentication.
* The number of incoming microservice calls must be rate-limited.
* Costs must be minimized.
What should you include in the solution?

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

**Correct Answer: A**

## Explanation/Reference:

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

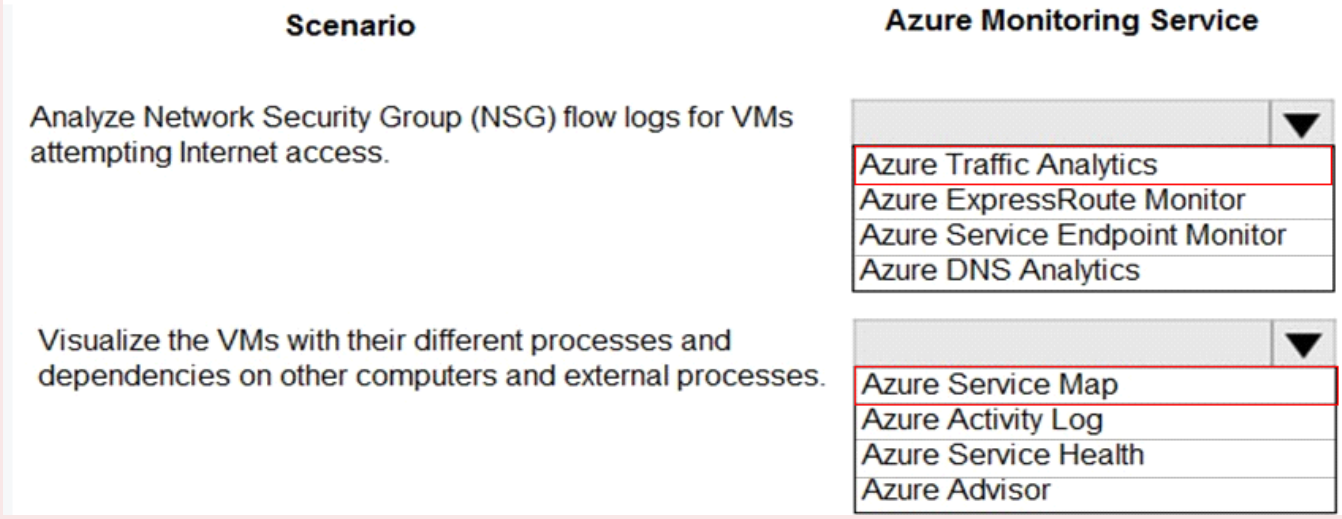
## QUESTION 24

Your company deploys several Linux and Windows virtual machines (VMs) to Azure. The VMs are deployed with the Microsoft Dependency Agent and the Log Analytics Agent installed by using Azure VM extensions. On-premises connectivity has been enabled by using Azure ExpressRoute.
You need to design a solution to monitor the VMs.
Which Azure monitoring services should you use? To answer, select the appropriate Azure monitoring services in the answer area.
NOTE: Each correct selection is worth one point.

| Scenario | Azure Monitoring Service |
|---|---|
| Analyze Network Security Group (NSG) flow logs for VMs attempting Internet access. | Azure Traffic Analytics / Azure ExpressRoute Monitor / Azure Service Endpoint Monitor / Azure DNS Analytics |
| Visualize the VMs with their different processes and dependencies on other computers and external processes. | Azure Service Map / Azure Activity Log / Azure Service Health / Azure Advisor |

**Correct Answer:**

Answer:




## Explanation/Reference:

https://docs.microsoft.com/en-us/azure/network-watcher/traffic-analytics
https://docs.microsoft.com/en-us/azure/azure-monitor/insights/service-map

## QUESTION 25

You plan to deploy an application named App1 that will run on five Azure virtual machines. Additional virtual machines will be deployed later to run App1.
You need to recommend a solution to meet the following requirements for the virtual machines that will run App1:
Ensure that the virtual machines can authenticate to Azure Active Directory (Azure AD) to gain access to
an Azure key vault, Azure Logic Apps instances, and an Azure SQL database.
Avoid assigning new roles and permissions for Azure services when you deploy additional virtual machines.
Avoid storing secrets and certificates on the virtual machines.
Which type of identity should you include in the recommendation?

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

## Correct Answer: D

## Explanation/Reference:

Managed identities for Azure resources is a feature of Azure Active Directory.
User-assigned managed identity can be shared. The same user-assigned managed identity can be

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

## QUESTION 26

# Case Study: 1

### Litware, Inc

### Overview. General Overview

Litware, Inc. is a medium-sized finance company

### Overview. Physical Locations

Litware has a main office in Boston.

### Existing Environment. Identity Environment

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

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

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

### Existing Environment

Azure Environment

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

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

Existing Environment. On-premises Environment

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

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

Existing Environment. Network Environment

Litware has ExpressRoute connectivity to Azure.

Planned Changes and Requirements. Planned Changes

Litware plans to implement the following changes:

Migrate DB1 and DB2 to Azure.

Migrate App1 to Azure virtual machines.

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

Planned Changes and Requirements. Authentication and Authorization Requirements

Litware identifies the following authentication and authorization requirements:

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

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

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

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

RBAC roles must be applied at the highest level possible.

Planned Changes and Requirements. Resiliency Requirements

Litware identifies the following resiliency requirements:

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

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

- Fail over automatically.

- Minimize I/O latency.

App1 must meet the following requirements:

- Be hosted in an Azure region that supports availability zones.

- Be hosted on Azure virtual machines that support automatic scaling.

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

Planned Changes and Requirements. Security and Compliance Requirements

Litware identifies the following security and compliance requirements:

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

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

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

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

App1 must not share physical hardware with other workloads.

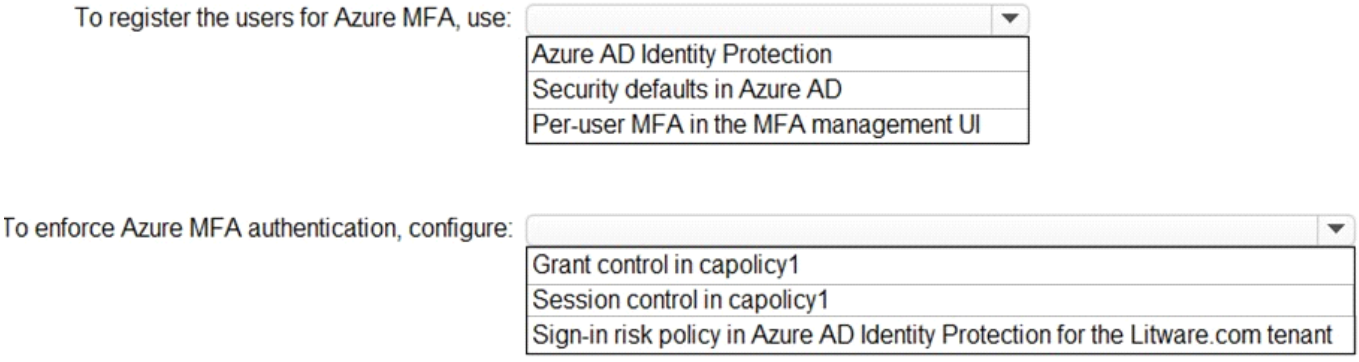
Planned Changes and Requirements. Business Requirements

Litware identifies the following business requirements:

Minimize administrative effort.

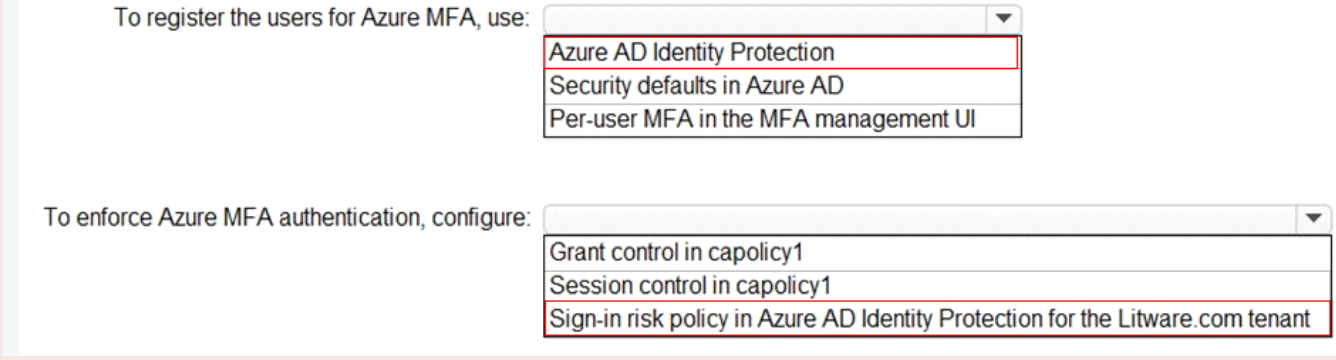
Minimize costs.

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.




**Correct Answer:**

**Answer:**




**Explanation/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 27

Case Study
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.
What two services would you recommend for HR data migration to Azure file share?

A. AzCopy
B. RoboCopy
C. Azure Data Factory
D. DataBox

**Correct Answer: B,D**

## Explanation/Reference:

Correct Answers: B and D
Azure provides tools for migrating unstructured data (files and objects) from on-premises to the cloud. You can migrate directly to the cloud or use the instructed data in a hybrid mode when data on-premises is in-sync with the cloud data. For several Azure Storage target services, like Azure Blob Storage, Data Lake Storage, Azure Files, etc., you need to select the best Azure migration or synchronization tools to match the storage target with the source.
To move files from on-premises Network Access Storage to Azure Files, you can use two tools: RoboCopy and DataBox.
RoboCopy is a Windows-based seasoned tool that copies files in full fidelity. You can create an Azure Storage account and Azure File shares. Then mount a share as a local drive on an on-premises Windows server and use RoboCopy to copy files from NAS to the local share.
DataBox is an offline appliance that Microsoft sends to you. After copying the files to the DataBox from on-premises NAS using RoboCopy, you send it back to Microsoft. Microsoft loads the files to your

Azure File Share. Depending on the total size of your files, you can select from three DataBox options:
DataBox Disks — up to 5 SSDs with a total storage of 40 TiB.
DataBox appliance — similar to NAS ruggedized device with a typical storage capacity of 80 TiB.
DataBox Heavy — similar to NAS ruggedized appliance on wheels with a total storage of 1 PiB.
Option A is incorrect because AzCopy is the tool for copying data in a cloud but not on-premises.
Option C is incorrect because Azure Data Factory is managed cloud service for extract-transform-load (ETL), extract-load-transform (ELT), and data integration operations, but it does not support the full fidelity of the files. It cannot copy the file's metadata.
For more information about file migration from on-premises NAS to Azure File shares, please visit the below URLs:
https://docs.microsoft.com/en-us/azure/storage/common/storage-migration-overview
https://docs.microsoft.com/en-us/azure/storage/files/storage-files-migration-overview
https://docs.microsoft.com/en-us/azure/storage/files/storage-files-migration-robocopy
https://docs.microsoft.com/en-us/azure/storage/files/storage-files-migration-nas-cloud-databox

## QUESTION 28

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen
Your company plans to deploy various Azure App Service instances that will use Azure SQL databases. The App Service instances will be deployed at the same time as the Azure SQL databases.
The company has a regulatory requirement to deploy the App Service instances only to specific Azure regions. The resources for the App Service instances must reside in the same region.
You need to recommend a solution to meet the regulatory requirement.
Solution: You recommend using an Azure policy to enforce the resource group location.
Does this meet the goal?

A. Yes
B. No

## Correct Answer: A

## Explanation/Reference:

Azure Resource Policy Definitions can be used which can be applied to a specific Resource Group with the App Service instances.
https://docs.microsoft.com/en-us/azure/governance/policy/overview