

**Certification Provider: Microsoft**

**Exam Code: AZ-305**

**Exam Name: Designing Microsoft Azure Infrastructure Solutions**

**Collated By: Million Zhang**

**Collated Date: 12<sup>th</sup> Jan 2023**

**Number of Question:**

<b>Topic</b>	<b>Number of Question:</b>
Case Study 1 – Litware	12
Case Study 2 - Fabrikam, Inc	9
Case Study 3 – Contoso	9
Solution Challenge	22
Common Question	177
<b>Total</b>	<b>229</b>

# Case Study 1 – Litware

## 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.

### On-Premises Environment

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

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

## Network Environment

Litware has ExpressRoute connectivity to Azure.

## Planned Changes and Requirements

- Litware plans to implement the following changes:
- Migrate DB1 and DB2 to Azure.
- Migrate App1 to Azure virtual machines.
- Migrate the external storage used by App1 to Azure Storage.
- Deploy the Azure virtual machines that will host App1 to Azure dedicated hosts.

## Authentication and Authorization Requirements

Litware identifies the following authentication and authorization requirements:

- Only 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 permissions to the network administrators for 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.
- RBAC roles must be applied at the highest level possible.

## **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.

## **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.

## **Business Requirements**

Litware identifies the following business requirements:

- Minimize administrative effort.
- Minimize costs.

## Question 1

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

ET User Answer: A

Resource lock only prevent deletion or modification of the resource, in this case the whole blob storage. You also do not get to specify how long you can lock the account. That doesn't answer the question. B cannot be the answer.

With Immutable Access Policy, you can set time-based policy.

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 2

Hotspot Question

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

### Answer Area

Database:

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

Service tier:

Hyperscale
Business Critical
General Purpose

Answer:

此题有争议： The correct answer should be: An Azure SQL Database elastic pool and Business Critical // Zone redundancy provides enhanced availability by automatically replicating data across three availability zones within a region.

### Answer Area

Database:

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

Service tier:

Hyperscale
Business Critical
General Purpose

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 3

Hotspot Question

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.

### Answer Area

Storage account type:

Premium page blobs
Premium file shares
Standard general-purpose v2

Configuration:

NFSv3
Large file shares
Hierarchical namespace

Answer:

### Answer Area

Storage account type:

Premium page blobs
Premium file shares
Standard general-purpose v2

Configuration:

NFSv3
Large file shares
Hierarchical namespace

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 4

You plan to migrate App1 to Azure.

You need to recommend a network connectivity solution for the Azure Storage account that will host the App1 data. The solution must meet the security and compliance requirements.

What should you include in the recommendation?

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

Answer: D

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.

Incorrect Answers:

A: Microsoft peering provides access to Azure public services via public endpoints with public IP addresses, which should not be allowed.

B: Azure public peering has been deprecated.

C: By default, Service Endpoints are enabled on subnets configured in Azure virtual networks. Endpoints can't be used for traffic from your premises to Azure services.

Reference:

<https://docs.microsoft.com/en-us/azure/expressroute/expressroute-circuit-peerings>

## Question 5

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

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

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

ET User Selected Answer: B

It should be B (2). When you go to Role Assignment in Azure Portal, in the Members blade you can assign the role to users, groups... So as the Litware has 2 AD tenants, so you do at least 2 assignments.

**B (79%)**

**A (21%)**

Answer: A

Explanation:

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

RBAC roles must be applied at the highest level possible.

## Question 6

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

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

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

ET User Answer: A. IMDS. Tested.

The requirement is "app1 must use the managed identity of the VM that will host the app" see here

<https://docs.microsoft.com/en-us/azure/virtual-machines/windows/instance-metadata-service?tabs=windows#managed-identity>

and then it will show the URL given by pentium75

<https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/how-to-use-vm-token>

A (57%)

D (43%)

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 7

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.

同 Q1, 应该选 A

Answer: C

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 8

Hotspot Question

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 Area

To register the users for Azure MFA, use:

Azure AD Identity Protection
Security defaults in Azure AD
Azure AD authentication methods policy

To enforce Azure MFA authentication, configure:

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

Answer:

### Answer Area

To register the users for Azure MFA, use:

Azure AD Identity Protection
Security defaults in Azure AD
Azure AD authentication methods policy

To enforce Azure MFA authentication, configure:

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

Box 1: Azure AD Identity Protection

Only 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).

Note: Policy configuration -

1. Navigate to the Azure portal.
2. Browse to Azure Active Directory > Security > Identity Protection > MFA registration policy.
3. Under Assignments
4. Users - Choose All users or Select individuals and groups if limiting your rollout.
5. Optionally you can choose to exclude users from the policy.
6. Enforce Policy - On
7. Save

Box 2: Grant control in capolicy1

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.

Note: We need to configure the policy conditions for capolicy1 that prompt for MFA.

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/authentication/tutorial-enable-azure-mfa>

## Question 9

### Drag and Drop Question

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.	
Invoke a remediation task.	
Create an Azure policy definition that uses the Modify effect	>
Create an Azure policy assignment.	<
Create a user-assigned managed identity.	

Answer:

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

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

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 10

HOTSPOT -

You plan to migrate App1 to Azure.

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

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

NOTE: Each correct selection is worth one point.

Hot Area:

### Answer Area

Number of host groups:

1
2
3
6

Number of virtual machine scale sets:

0
1
3

Answer:

有争议，ET 答案是 3/3，题库答案是 3/1.

## Answer Area

Number of host groups:

1
2
3
6

Number of virtual machine scale sets:

0
1
3

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 11

HOTSPOT -

You plan to migrate App1 to Azure.

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

What should you use to estimate the costs, and what should you implement to minimize the costs? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

### Answer Area

To estimate the costs, use:

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

Implement:

Azure Reservations
Azure Hybrid Benefit
Azure Spot Virtual Machine pricing

Answer:

Box 2: Form ET User, Azure Reservations:

[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.]  
[App1 must not share physical hardware with other workloads.]

Azure reserved instances can purchased for one year or three years. Therefore Litware can purchase 3 years Reserved instances to save cost. And reserved instances guarantees dedicated compute resources to App1.

Why not Hybrid Benefit?

this is for customers with Software Assurance. We are not sure if Litware has Software Assurance.

## Answer Area

To estimate the costs, use:

Azure Advisor
The Azure Cost Management Power BI app
<b>The Azure Total Cost of Ownership (TCO) calculator</b>

Implement:

Azure Reservations
<b>Azure Hybrid Benefit</b>
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 12

HOTSPOT -

You plan to migrate DB1 and DB2 to Azure.

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

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

NOTE: Each correct selection is worth one point.

Hot Area:

### Answer Area

Database:

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

Service tier:

- Hyperscale
- Business Critical
- General Purpose

Answer:

同 Q2, 这里跟 Q2 给的答案不一样, ET User 认为答案应该是这个。

### Answer Area

Database:

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

Service tier:

- Hyperscale
- Business Critical
- General Purpose

Box 1: An Azure SQL Database elastic pool

Scenario: \* 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.

\* Litware identifies the following business requirements:

Minimize administrative effort.

Minimize costs.

Box 2: Business Critical

# Case Study 2 - Fabrikam, Inc

## Overview

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

### Existing Environment: Active Directory Environment

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

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

Rd.fabrikam.com is used by the research and development (R&D) department only. The R&D department is restricted to using on-premises resources only.

### Existing Environment: Network Infrastructure

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

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

An existing application named WebApp1 is hosted in the data center of the London office.

WebApp1 is used by customers to place and track orders. WebApp1 has a web tier that uses Microsoft Internet Information Services (IIS) and a database tier that runs Microsoft SQL Server 2016. The web tier and the database tier are deployed to virtual machines that run on Hyper-V.

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

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

### Existing Environment: Problem Statements

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

### Requirements: Planned Changes

Fabrikam plans to move most of its production workloads to Azure during the next few years, including virtual machines that rely on Active Directory for authentication.

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

All R&D operations will remain on-premises.

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

### **Requirements: Technical Requirements**

Fabrikam identifies the following technical requirements:

- Website content must be easily updated from a single point.
- User input must be minimized when provisioning new web app instances.
- Whenever possible, existing on-premises licenses must be used to reduce cost.
- Users must always authenticate by using their corp.fabrikam.com UPN identity.
- Any new deployments to Azure must be redundant in case an Azure region fails.
- Whenever possible, solutions must be deployed to Azure by using the Standard pricing tier of Azure App Service.
- An email distribution group named IT Support must be notified of any issues relating to the directory synchronization services.
- In the event that a link fails between Azure and the on-premises network, ensure that the virtual machines hosted in Azure can authenticate to Active Directory.
- Directory synchronization between Azure Active Directory (Azure AD) and corp.fabrikam.com must not be affected by a link failure between Azure and the on-premises network.

### **Requirements: Database Requirements**

Fabrikam identifies the following database requirements:

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

### **Requirements: Security Requirements**

Fabrikam identifies the following security requirements:

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

## Question 1

You need to recommend a solution to meet the database retention requirements.

What should you recommend?

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

Answer: A

Scenario: Database backups must be retained for a minimum of seven years to meet compliance requirements.

Many applications have regulatory, compliance, or other business purposes that require you to retain database backups beyond the 7-35 days provided by Azure SQL Database and Azure SQL Managed Instance automatic backups. By using the long-term retention (LTR) feature, you can store specified SQL Database and SQL Managed Instance full backups in Azure Blob storage with configured redundancy for up to 10 years. LTR backups can then be restored as a new database.

Reference:

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

## Question 2

HOTSPOT -

You are evaluating the components of the migration to Azure that require you to provision an Azure Storage account. For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

### Answer Area

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

Answer:

题库答案 YNY, ET 答案 NNY, ET User 答案 YNN

[Exam AZ-305 topic 7 question 1 discussion - ExamTopics](#)

### Answer Area

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

ox 1: No -

Online migration will work fine. It does not require an Azure Storage account.

Box 2: No -

Data for the web site can migrated to Azure app service.

Box 3: Yes -

Scenario: Database metrics for the production instance of WebApp1 must be available for analysis so that database administrators can optimize the performance settings.

Reference:

<https://azure.microsoft.com/en-au/services/sql-server-stretch-database/>

## Question 3

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

- A. Deploy domain controllers for corp.fabrikam.com to virtual networks in Azure.
- B. Move all the domain controllers from 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: A

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 4

You need to recommend a data storage strategy for WebApp1.

What should you include in the recommendation?

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

Answer: D

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

Database metrics for the production instance of WebApp1 must be available for analysis so that database administrators can optimize the performance settings.

Note: A virtual core (vCore) represents a logical CPU and offers you the option to choose between generations of hardware and the physical characteristics of the hardware (for example, the number of cores, the memory, and the storage size). The vCore-based purchasing model gives you flexibility, control, transparency of individual resource consumption, and a straightforward way to translate on-premises workload requirements to the cloud. This model optimizes price, and allows you to choose compute, memory, and storage resources based on your workload needs.

Incorrect:

Not C: Azure SQL Database elastic pools are a simple, cost-effective solution for managing and scaling multiple databases, not for a single database.

Reference:

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

## Question 5

You need to recommend a strategy for migrating the database content of WebApp1 to Azure.

What should you include in the recommendation?

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

ET User: C

Looks like answer C should be correct for the given scenario -

Req from scenario - To avoid disrupting customer access, database downtime must be minimized when databases are migrated.

<https://docs.microsoft.com/en-us/azure/azure-sql/virtual-machines/windows/migrate-to-vm-from-sql-server>

Choose a migration method

For best data transfer performance, migrate the database files into the Azure VM using a compressed backup file.

Answer: D

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 6

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

What should you recommend?

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

Answer: D

Explanation:

Scale create multiple copies of single web Instanced and does not required any additional configuration.

## Question 7

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

What should you include in the recommendation?

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

Answer: D

An email distribution group named IT Support must be notified of any issues relating to the directory synchronization services.

Note: You can configure the Azure AD Connect Health service to send email notifications when alerts indicate that your identity infrastructure is not healthy. This occurs when an alert is generated, and when it is resolved.

The screenshot shows the Azure Active Directory Connect (Sync) Alerts configuration page. The 'Notification' tab is selected. A red box highlights the 'Notifications' button in the top navigation bar. The main area shows a single active alert for 'Azure AD Connect Sync Service is not running'. The alert is set to 'ON' for notifications and is scoped to 'FABVM03'. An 'Additional Email Recipients' section lists 'varun@fabtoso.com' and 'idadmins@fabtoso.com'.

Reference:

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

## Question 8

HOTSPOT -

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

NOTE: Each correct selection is worth one point.

Hot Area:

### Answer Area

Minimum number of Azure AD tenants:

0
1
2
3
4

Minimum number of custom domains to add:

0
1
2
3
4

Minimum number of conditional access policies to create:

0
1
2
3
4

Answer:

题库答案是 110, ET 答案是 211, ET User 答案是 111

## Answer Area

Minimum number of Azure AD tenants:

0
1
2
3
4

Minimum number of custom domains to add:

0
1
2
3
4

Minimum number of conditional access policies to create:

0
1
2
3
4

Box 1: 2 -

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

Box 2: 1 -

Box 3: 1 -

Scenario:

- ⇒ Users on the on-premises network must be able to authenticate to corp.fabrikam.com if an Internet link fails.
- ⇒ Administrators must be able authenticate to the Azure portal by using their corp.fabrikam.com credentials.
- ⇒ All administrative access to the Azure portal must be secured by using multi-factor authentication.

Note:

Users must always authenticate by using their corp.fabrikam.com UPN identity.

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

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

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

Design Identity and Security

## Question 9

HOTSPOT -

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



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

NOTE: Each correct selection is worth one point.

Hot Area:

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

Answer:

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

Explanation:

Box 1: Yes

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

Box 2: Yes

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

Box 3: No

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

Reference:

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

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

# Case Study 3 – Contoso

## 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 1

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

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 multi-region writes is enabled.

Incorrect Answers:

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

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

Reference:

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

## Question 2

HOTSPOT -

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

NOTE: Each correct selection is worth one point.

Hot Area:

### Answer Area

Service:

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

Feature:

Access packages
Access reviews
Approvals
Runbooks

Answer:

ET User:

Box 1: Azure AD Identity governance

The reasoning is PIM can not be used to do access review of B2B users. The scenarios describes that Fabrikam uses B2B to access the App1.

Hence Identity governance

## Answer Area

Service:
Azure AD Identity Governance
Azure AD Identity Protection
<b>Azure AD Privilege Access Management (PIM)</b>
Azure Automation

Feature:
Access packages
<b>Access reviews</b>
Approvals
Runbooks

Requirements: Identity Requirements

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

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

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

When should you use access reviews?

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

Box 2: Access reviews -

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

Reference:

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

## Question 3

DRAG DROP -

You need to recommend a solution that meets the file storage requirements for App2. What should you deploy to the Azure subscription and the on-premises network? To answer, drag the appropriate services to the correct locations. Each service may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:

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

Answer:

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

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 4

HOTSPOT -

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

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

NOTE: Each correct selection is worth one point.

Hot Area:

### Answer Area

Authenticate App1 by using:

A certificate
A system-assigned managed identity
A user-assigned managed identity

Authorize App1 to retrieve Key Vault secrets by using:

An access policy
A connected service
A private link
A role assignment

### Answer Area

Authenticate App1 by using:

A certificate
A service principal
A system-assigned managed identity
A user-assigned managed identity

Authorize App1 to retrieve Key Vault secrets by using:

An access policy
A connected service
A private link
A role assignment

Answer:

有争议，出现过两次，选项不同，Maybe: System-assigned managed identity + Access Policy

## Answer Area

Authenticate App1 by using:

A certificate
A system-assigned managed identity
A user-assigned managed identity

Authorize App1 to retrieve Key Vault secrets by using:

An access policy
A connected service
A private link
A role assignment

## Answer Area

Authenticate App1 by using:

A certificate
A service principal
A system-assigned managed identity
A user-assigned managed identity

Authorize App1 to retrieve Key Vault secrets by using:

An access policy
A connected service
A private link
A role assignment

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 system-assigned managed identity

No one knows the credentials of managed identities.

Managed Identities exist in two formats:

\* System assigned: in this scenario, the identity is linked to a single Azure Resource, eg a Virtual Machine, a Logic App, a Storage Account, Web App, Function, so almost anything. Next, they also live with the Azure Resource, which means they get deleted when the Azure Resource gets deleted.

\* User Assigned Managed Identity (incorrect for this question), which means that you first have to create it as a stand-alone Azure resource by itself, after which it can be linked to multiple Azure Resources.

Box 2: An access policy -

Set up an access policy for the system-assigned managed identity.

Note: Grant access -

The managed identity needs to be granted access to read the secret that we'll store in the Key Vault.

1. Navigate to your newly created Key Vault
2. Select Access Policy from the menu on the left side.
3. Select Add Access Policy
4. Etc.

Reference:

<https://devblogs.microsoft.com/devops/demystifying-service-principals-managed-identities/>

<https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/tutorial-windows-vm-access-nonaad>

## Question 5

You need to recommend an App Service architecture that meets the requirements for App1.

The solution must minimize costs.

What should you recommend?

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

Answer: B

Maybe: C

**C (70%)**

**B (30%)**

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.

Note: The Azure App Service Environment v2 is an Azure App Service feature that provides a fully isolated and dedicated environment for securely running App Service apps at high scale.

Customers can create multiple ASEs within a single Azure region or across multiple Azure regions. This flexibility makes ASEs ideal for horizontally scaling stateless application tiers in support of high requests per second (RPS) workloads.

Reference:

<https://docs.microsoft.com/en-us/azure/app-service/environment/intro>

## Question 6

HOTSPOT -

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

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

NOTE: Each correct selection is worth one point.

Hot Area:

### Answer Area

Azure Traffic Manager:

1
2
3
6

Azure Application Gateway:

1
2
3
6

Answer:

题库给的是 1/6, ET & ET User 是 1/2

### Answer Area

Azure Traffic Manager:

1
2
3
6

Azure Application Gateway:

1
2
3
6

Box 1: 1 -

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

- ¤ 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.

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

Note: Azure Traffic Manager is a DNS-based traffic load balancer. This service allows you to distribute traffic to your public facing applications across the global Azure regions.

Box 2: 2 -

For production workloads, run at least two gateway instances.

A single Application Gateway deployment can run multiple instances of the gateway.

Use one Application Gateway in East US Region, and one in the West Europe region.

Reference:

<https://docs.microsoft.com/en-us/azure/architecture/high-availability/reference-architecture-traffic-manager-application-gateway>

## Question 7 - New

You need to recommend a solution for the App1 maintenance task. The solution must minimize costs.

What should you include in the recommendation?

- A. an Azure logic app
- B. an Azure function
- C. an Azure virtual machine
- D. an App Service WebJob

ET User Answer: B

Azure function as a resource is created in a region but it can access data store from a different region if access is provided. A single function from a region should be able to do the job. I have no reason to believe that a logic app can access data store from two regions but a function cannot. Answer is B.

**B (80%)**

**A (20%)**

Answer: A 

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.

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

You can create and manage workflows with Azure PowerShell in Azure Logic Apps.

You can create a Consumption logic app in multi-tenant Azure Logic Apps by using the JSON file for a logic app workflow definition. You can then manage your logic app by running the cmdlets in the Az.LogicApp PowerShell module.

Reference:

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

## Question 8 - New

You need to recommend a solution that meets the application development requirements.

What should you include in the recommendation?

- A. the Azure App Configuration service
- B. an Azure Container Registry instance
- C. deployment slots
- D. Continuous Integration/Continuous Deployment (CI/CD) sources

Answer: C

When you deploy your web app, web app on Linux, mobile back end, or API app to Azure App Service, you can use a separate deployment slot instead of the default production slot when you're running in the Standard, Premium, or Isolated App Service plan tier. Deployment slots are live apps with their own host names.

App content and configurations elements can be swapped between two deployment slots, including the production slot.

Deploying your application to a non-production slot has the following benefits:

- \* You can validate app changes in a staging deployment slot before swapping it with the production slot.
- \* Deploying an app to a slot first and swapping it into production makes sure that all instances of the slot are warmed up before being swapped into production.

This eliminates downtime when you deploy your app.

- \* After a swap, the slot with previously staged app now has the previous production app. If the changes swapped into the production slot aren't as you expect, you can perform the same swap immediately to get your "last known good site" back.

Note: 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.

Reference:

<https://docs.microsoft.com/en-us/azure/app-service/deploy-staging-slots>

## Question 9 – New

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

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

Answer: B

Scenario: 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.

Unified cross-component transaction diagnostics.

The unified diagnostics experience automatically correlates server-side telemetry from across all your Application Insights monitored components into a single view. It doesn't matter if you have multiple resources. Application Insights detects the underlying relationship and allows you to easily diagnose the application component, dependency, or exception that caused a transaction slowdown or failure.

Note: Components are independently deployable parts of your distributed/microservices application. Developers and operations teams have code-level visibility or access to telemetry generated by these application components.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-monitor/app/transaction-diagnostics>

# Solution Challenge

Question 1 2 3 4 5

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

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

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

Several virtual machines exhibit network connectivity issues.

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

- A. Solution: Use Azure Traffic Analytics in Azure Network Watcher to analyze the network traffic.
- B. Solution: Use Azure Advisor to analyze the network traffic.
- C. Solution: Use Azure Network Watcher to run IP flow verify to analyze the network traffic.
- D. Solution: Install and configure the Azure Monitoring agent and the Dependency Agent on all the virtual machines. Use VM insights in Azure Monitor to analyze the network traffic.
- E. Solution: Use the Azure Traffic Analytics solution in Azure Log Analytics to analyze the network

Answer: C

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>

## Question 6 7 8 9

**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.
- A. Solution: You deploy two Azure virtual machines to two Azure regions, and you create an Azure Traffic Manager profile.
  - B. Solution: You deploy two Azure virtual machines to two Azure regions, and you deploy an Azure Application Gateway.
  - C. Solution: You deploy an Azure virtual machine scale set that uses autoscaling.
  - D. Solution: You deploy a web app in an Isolated App Service plan.

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.

## Question 10 11 12 13 14

**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.

- A. Solution: You recommend using an Azure policy initiative to enforce the location.
- B. Solution: You recommend using the Regulatory compliance dashboard in Azure Security Center.
- C. Solution: You recommend using an Azure policy to enforce the resource group location.
- D. Solution: You recommend creating resource groups based on locations and implementing resource locks on the resource groups.
- E. Solution: You recommend using the Regulatory compliance dashboard in Microsoft Defender for Cloud.

Answer: A C

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 15 16 17 18

**Note:** This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals.

**Some question sets might have more than one correct solution, while others might not have a correct solution.**

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

You plan to deploy multiple instances of an Azure web app across several Azure regions. You need to design an access solution for the app. The solution must meet the following replication requirements:

- Support rate limiting.
  - Balance requests between all instances.
  - Ensure that users can access the app in the event of a regional outage.
- A. Solution: You use Azure Traffic Manager to provide access to the app.
  - B. Solution: You use Azure Load Balancer to provide access to the app.
  - C. Solution: You use Azure Application Gateway to provide access to the app.
  - D. Solution: You use Azure Front Door to provide access to the app.

Answer: D

Azure Application Gateway and Azure Load Balancer do not support rate or connection limits.

Azure Front Door meets the requirements. The Azure Web Application Firewall (WAF) rate limit rule for Azure Front Door controls the number of requests allowed from clients during a one-minute duration.

Reference:

<https://www.nginx.com/blog/nginx-plus-and-azure-load-balancers-on-microsoft-azure/>

<https://docs.microsoft.com/en-us/azure/web-application-firewall/afds/waf-front-door-rate-limit-powershell>

## Question 19 20 21

**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.

- A. Solution: For File1, you set Access tier to Cool.
- B. Solution: You move File1 to a new storage account. For File1, you set Access tier to Archive.
- C. Solution: For File1, you set Access tier to Hot.

Answer: A C

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.

Reference:

<https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blob-storage-tiers?tabs=azure-portal>

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

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

Reference:

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

## Question 22

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

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

You are designing an Azure solution for a company that has four departments. Each department will deploy several Azure app services and Azure SQL databases.

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

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

答案：方案 A 理论上是可以这么做的，但是这道题的考点是 Tag，大 XX

Explanation:

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

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

Reference:

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

# Common Question

## Question 1

You have an Azure subscription that contains a custom application named Application1. Application1 was developed by an external company named Fabrikam, Ltd. Developers at Fabrikam were assigned role-based access control (RBAC) permissions to the Application1 components. All users are licensed for the Microsoft 365 E5 plan. You need to recommend a solution to verify whether the Fabrikam developers still require permissions to Application1. The solution must meet the following requirements:

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

What should you recommend?

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

Answer: A

Explanation:

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

<https://docs.microsoft.com/en-us/azure/active-directory/governance/manage-user-access-with-access-reviews>

## Question 2

You have an Azure subscription. The subscription has a blob container that contains multiple blobs.

Ten users in the finance department of your company plan to access the blobs during the month of April.

You need to recommend a solution to enable access to the blobs during the month of April only.

Which security solution should you include in the recommendation?

- A. shared access signatures (SAS)
- B. Conditional Access policies
- C. certificates
- D. access keys

Correct Answer: A

Shared Access Signatures (SAS) allows for limited-time fine grained access control to resources. So, you can generate URL, specify duration (for month of April) and disseminate URL to 10 team members. On May 1, the SAS token is automatically invalidated, denying team members continued access.

Reference:

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

## Question 3

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

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

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

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

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

NOTE: Each correct selection is worth one point.

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

Correct Answer: AE 

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.

E: Add an on-premises app to Azure AD

Now that you've prepared your environment and installed a connector, you're ready to add on-premises applications to Azure AD.

1. Sign in as an administrator in the Azure portal; 2. In the left navigation panel, select Azure Active Directory; 3. Select Enterprise applications, and then select New application.; 4. Select Add an on-premises application button which appears about halfway down the page in the On-premises applications section. Alternatively, you can select Create your own application at the top of the page and then select Configure Application Proxy for secure remote access to an on-premise application; 5. In the Add your own on-premises application section, provide the following information about your application; 6. Etc.

Incorrect:

Not C: Conditional Access policies are not required.

Reference:

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

## Question 4

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

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

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

What should you include in the recommendation?

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

Correct Answer: C

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

Reference:

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

## Question 5

HOTSPOT -

You plan to deploy Azure Databricks to support a machine learning application. Data engineers will mount an Azure Data Lake Storage account to the Databricks file system.

Permissions to folders are granted directly to the data engineers.

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

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

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

NOTE: Each correct selection is worth one point.

Hot Area:

### Answer Area

Databricks SKU:

Premium	
Standard	

Cluster configuration:

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

Answer:

## Answer Area

Databricks SKU:

Premium	
Standard	

Cluster configuration:

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

Box 1: Premium -

Premium Databricks SKU is required for credential passthrough.

Box 2: Credential passthrough -

Authenticate 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 6

HOTSPOT -

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

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

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

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

NOTE: Each correct selection is worth one point.

Hot Area:

### Answer Area

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

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:

### Answer Area

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

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

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

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

Box 1: An Azure AD app registration

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

You register your application with Azure active directory tenant.

Box 2: A conditional access policy

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

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

Reference:

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

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

## Question 7

DRAG DROP -

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

You need to use Azure Monitor to design an alerting strategy for security-related events. Which Azure Monitor Logs tables should you query? To answer, drag the appropriate tables to the correct log types. Each table may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:

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

Answer:

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

Reference:

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

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

## Question 8

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

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

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

NOTE: Each correct selection is worth one point.

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

Correct Answer: CEF

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

Reference:

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

## Question 9

DRAG DROP -

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

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

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

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

Select and Place:

Features	Answer Area
a public Azure Load Balancer	
a managed identity	
an internal Azure Load Balancer	
a Conditional Access policy	
an Azure App Service plan	
Azure AD Application Proxy	
an Azure AD enterprise application	



Answer:

Features	Answer Area
a public Azure Load Balancer	Azure AD Application Proxy
a managed identity	an Azure AD enterprise application
an internal Azure Load Balancer	a Conditional Access policy
an Azure App Service plan	



## Step 1: Azure AD Application Proxy

Start by enabling communication to Azure data centers to prepare your environment for Azure AD Application Proxy.

## Step 2: an Azure AD enterprise application

Add an on-premises app to Azure AD.

Now that you've prepared your environment and installed a connector, you're ready to add on-premises applications to Azure AD.

1. Sign in as an administrator in the Azure portal.
2. In the left navigation panel, select Azure Active Directory.
3. Select Enterprise applications, and then select New application.
4. Etc.

Reference:

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

## Question 10

You need to recommend a solution to generate a monthly report of all the new Azure Resource Manager (ARM) resource deployments in your Azure subscription.

What should you include in the recommendation?

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

Correct Answer: A

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

Through activity logs, you can determine:

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

Reference:

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

## Question 11

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.

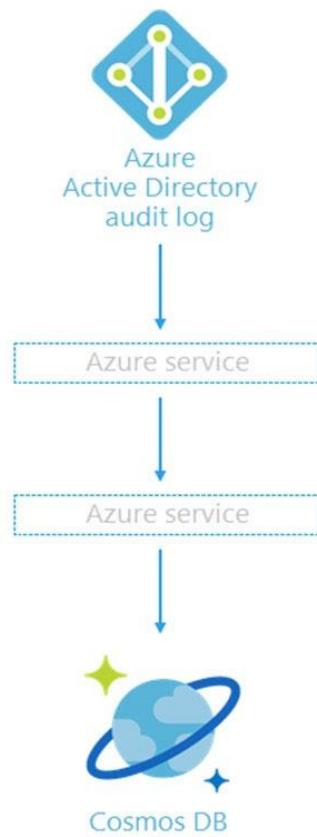
Which services should you include in the design? To answer, drag the appropriate services to the correct targets. Each service may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:

Azure Services
Azure Event Grid
Azure Event Hubs
Azure Functions
Azure Monitor Logs
Azure Notification Hubs

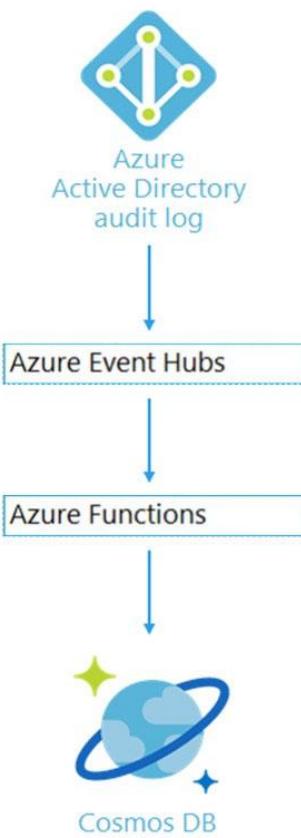
### Answer Area



Answer:

Azure Services
Azure Event Grid
Azure Event Hubs
Azure Functions
Azure Monitor Logs
Azure Notification Hubs

### Answer Area



Box 1: Azure Event Hubs -

You can route Azure Active Directory (Azure AD) activity logs to several endpoints for long term retention and data insights.

The Event Hub is used for streaming.

Box 2: Azure Function -

Use an Azure Function along with a cosmos DB change feed, and store the data in Cosmos DB.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-activity-logs-azure-monitor>

## Question 12

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

Contoso establishes a partnership with another company named Fabrikam, Inc.

Fabrikam does not have an existing Azure Active Directory (Azure AD) tenant and uses third-party OAuth 2.0 identity management to authenticate its users.

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

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

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

What should you include in the solution?

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

Correct Answer: D

Many APIs support OAuth 2.0 to secure the API and ensure that only valid users have access, and they can only access resources to which they're entitled. To use Azure API Management's interactive developer console with such APIs, the service allows you to configure your service instance to work with your OAuth 2.0 enabled API.

Incorrect:

Azure AD business-to-business (B2B) uses guest accounts.

Azure AD Application Proxy is for on-premises scenarios.

Reference:

<https://docs.microsoft.com/en-us/azure/api-management/api-management-howto-oauth2>

## Question 13

HOTSPOT -

You have an Azure subscription that contains 300 virtual machines that run Windows Server 2019.

You need to centrally monitor all warning events in the System logs of the virtual machines. What should you include in the solution? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

**Answer Area**

Resource to create in Azure:

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

Configuration to perform on the virtual machines:

- Create event subscriptions
- Configure Continuous delivery
- Install the Azure Monitor agent
- Modify the membership of the Event Log Readers group

Answer:

**Answer Area**

Resource to create in Azure:

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

Configuration to perform on the virtual machines:

- Create event subscriptions
- Configure Continuous delivery
- Install the Azure Monitor agent**
- Modify the membership of the Event Log Readers group

Box 1: A Log Analytics workspace

Send resource logs to a Log Analytics workspace to enable the features of Azure Monitor Logs.

You must create a diagnostic setting for each Azure resource to send its resource logs to a Log Analytics workspace to use with Azure Monitor Logs.

Box 2: Install the Azure Monitor agent

Use the Azure Monitor agent if you need to:

Collect guest logs and metrics from any machine in Azure, in other clouds, or on-premises.

Manage data collection configuration centrally

Reference:

<https://docs.microsoft.com/en-us/azure/azure-monitor/essentials/resource-logs>

<https://docs.microsoft.com/en-us/azure/azure-monitor/agents/agents-overview#azure-monitor-agent>

## Question 14

HOTSPOT -

You have several Azure App Service web apps that use Azure Key Vault to store data encryption keys.

Several departments have the following requests to support the web app:

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

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

NOTE: Each correct selection is worth one point.

Hot Area:

### Answer Area

Security:	<div style="border: 1px solid #ccc; padding: 5px;"><input type="checkbox"/> Azure AD Privileged Identity Management <input type="checkbox"/> Azure Managed Identity <input type="checkbox"/> Azure AD Connect <input type="checkbox"/> Azure AD Identity Protection</div>
Development:	<div style="border: 1px solid #ccc; padding: 5px;"><input type="checkbox"/> Azure AD Privileged Identity Management <input type="checkbox"/> Azure Managed Identity <input type="checkbox"/> Azure AD Connect <input type="checkbox"/> Azure AD Identity Protection</div>
Quality Assurance:	<div style="border: 1px solid #ccc; padding: 5px;"><input type="checkbox"/> Azure AD Privileged Identity Management <input type="checkbox"/> Azure Managed Identity <input type="checkbox"/> Azure AD Connect <input type="checkbox"/> Azure AD Identity Protection</div>

Answer:

## Answer Area

Security:	<ul style="list-style-type: none"><li>Azure AD Privileged Identity Management</li><li>Azure Managed Identity</li><li>Azure AD Connect</li><li>Azure AD Identity Protection</li></ul>
Development:	<ul style="list-style-type: none"><li>Azure AD Privileged Identity Management</li><li>Azure Managed Identity</li><li>Azure AD Connect</li><li>Azure AD Identity Protection</li></ul>
Quality Assurance:	<ul style="list-style-type: none"><li>Azure AD Privileged Identity Management</li><li>Azure Managed Identity</li><li>Azure AD Connect</li><li>Azure AD Identity Protection</li></ul>

### Box 1: Azure AD Privileged Identity Management

Privileged Identity Management provides time-based and approval-based role activation to mitigate the risks of excessive, unnecessary, or misused access permissions on resources that you care about. Here are some of the key features of Privileged Identity Management:

Provide just-in-time privileged access to Azure AD and Azure resources

Assign time-bound access to resources using start and end dates

Require approval to activate privileged roles

Enforce multi-factor authentication to activate any role

Use justification to understand why users activate

Get notifications when privileged roles are activated

Conduct access reviews to ensure users still need roles

Download audit history for internal or external audit

Prevents removal of the last active Global Administrator role assignment

### Box 2: Azure Managed Identity -

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. With Azure Key

Vault, developers can use managed identities to access resources. Key

Vault stores credentials in a secure manner and gives access to storage accounts.

### Box 3: Azure AD Privileged Identity Management

Privileged Identity Management provides time-based and approval-based role activation to mitigate the risks of excessive, unnecessary, or misused access permissions on resources that you care about. Here are some of the key features of Privileged Identity Management:

Provide just-in-time privileged access to Azure AD and Azure resources

Assign time-bound access to resources using start and end dates

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/>

[management/pim-configure](#)

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

此题的另外一个题干：

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:

[这里是相同的表]

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.

## Question 15

Your company has the divisions shown in the following table.

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

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

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

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

What is the minimum number of objects required to deploy the application? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

### Answer Area

Management groups:

1
2
3
4

Blueprint definitions:

1
2
3
4

Blueprint assignments:

1
2
3
4

Answer:

Management groups:

1
2
3
4

Blueprint definitions:

1
2
3
4

Blueprint assignments:

1
2
3
4

B 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 16

HOTSPOT -

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

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

The solution must use the principle of least privilege.

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

NOTE: Each correct selection is worth one point.

Hot Area:

**Answer Area**

Azure Policy effect to use:

Append
EnforceOPAConstraint
EnforceRegoPolicy
Modify

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

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

Answer:

**Answer Area**

Azure Policy effect to use:

Append
EnforceOPAConstraint
EnforceRegoPolicy
Modify

Azure Active Directory (Azure AD) object and role-based access control (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

ox 1: Modify -

Modify is used to add, update, or remove properties or tags on a subscription or 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. Policy assignments with effect set as Modify require a managed identity to do remediation.

Incorrect:

- \* The following effects are deprecated: EnforceOPAConstraint EnforceRegoPolicy
- \* Append is used to add additional fields to the requested resource during creation or update. A common example is specifying allowed IPs for a storage resource.

Append is intended for use with non-tag properties. While Append can add tags to a

resource during a create or update request, it's recommended to use the Modify effect for tags instead.

Box 2: A managed identity with the Contributor role

The managed identity needs to be granted the appropriate roles required for remediating resources to grant the managed identity.

Contributor - Can create and manage all types of Azure resources but can't grant access to others.

Incorrect:

User Access Administrator: lets you manage user access to Azure resources.

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/role-based-access-control/built-in-roles>

## Question 17

HOTSPOT -

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

Name	Type	Account Kind	Location
storage1	Azure Storage account	Storage (general purpose v1)	East US
storage2	Azure Storage account	StorageV2 (general purpose v2)	East US
Workspace1	Azure Log Analytics workspace	<b>Not applicable</b>	East US
Workspace2	Azure Log Analytics workspace	<b>Not applicable</b>	East US
Hub1	Azure event hub	<b>Not applicable</b>	East US

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

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

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

Hot Area:

### Answer Area

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

Answer:

### Answer Area

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

Box 1: Yes -

A single diagnostic setting can define no more than one of each of the destinations. If you

want to send data to more than one of a particular destination type (for example, two different Log Analytics workspaces), then create multiple settings.

Each resource can have up to 5 diagnostic settings.

Note: This diagnostic telemetry can be streamed to one of the following Azure resources for analysis.

- \* Log Analytics workspace
- \* Azure Event Hubs
- \* Azure Storage

Box 2: Yes -

Box 3: Yes -

Reference:

<https://docs.microsoft.com/en-us/azure/azure-monitor/essentials/diagnostic-settings>

<https://docs.microsoft.com/en-us/azure/azure-sql/database/metrics-diagnostic-telemetry-logging-streaming-export-configure?tabs=azure-portal>

## Question 18

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

Correct Answer: A

Dynamic data masking limits sensitive data exposure by masking it to non-privileged users.

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

Reference:

<https://docs.microsoft.com/en-us/azure/azure-sql/database/dynamic-data-masking-overview>

## Question 19

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

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

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

What should you deploy?

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

Correct Answer: B

You can specify a customer-provided key on Blob storage operations. A client making a read or write request against Blob storage can include an encryption key on the request for granular control over how blob data is encrypted and decrypted.

Reference:

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

## Question 20

HOTSPOT -

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

You need to recommend a solution to store the 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.

NOTE: Each correct selection is worth one point.

Hot Area:

### **Answer Area**

Key Vault integration method:

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

Key Vault permissions for the managed identity:

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

Answer:

### **Answer Area**

Key Vault integration method:

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

Key Vault permissions for the managed identity:

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

Box 1: Key Vault references in Application settings

Source Application Settings from Key Vault.

Key Vault references can be used as values for Application Settings, allowing you to keep secrets in Key Vault instead of the site config. Application Settings are securely encrypted at rest, but if you need secret management capabilities, they should go into Key Vault.

To use a Key Vault reference for an app setting, set the reference as the value of the setting. Your app can reference the secret through its key as normal. No code changes are required.

Box 2: Secrets: Get -

In order to read secrets from Key Vault, you need to have a vault created and give your app

permission to access it.

1. Create a key vault by following the Key Vault quickstart.
2. Create a managed identity for your application.
3. Key Vault references will use the app's system assigned identity by default, but you can specify a user-assigned identity.
4. Create an access policy in Key Vault for the application identity you created earlier. Enable the "Get" secret permission on this policy.

Reference:

<https://docs.microsoft.com/en-us/azure/app-service/app-service-key-vault-references>

<https://docs.microsoft.com/en-us/azure/app-service/app-service-key-vault-references>

## Question 21

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

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

- Ensure that the virtual machines can authenticate to Azure Active Directory (Azure AD) to gain access to an Azure key vault, Azure Logic Apps instances, and an Azure SQL database.
- Avoid assigning new roles and permissions for Azure services when you deploy additional virtual machines.
- Avoid storing secrets and certificates on the virtual machines.
- Minimize administrative effort for managing identities.

Which type of identity should you include in the recommendation?

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

Correct Answer: D

Managed identities provide an identity for applications to use when connecting to resources that support Azure Active Directory (Azure AD) authentication.

A user-assigned managed identity:

Can be shared.

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

Common usage:

Workloads that run on multiple resources and can share a single identity.

For example, a workload where multiple virtual machines need to access the same resource.

Incorrect:

Not A: A system-assigned managed identity can't be shared. It can only be associated with a single Azure resource.

Typical usage:

Workloads that are contained within a single Azure resource.

Workloads for which you need independent identities.

For example, an application that runs on a single virtual machine.

Reference:

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

## Question 22

You have the resources shown in the following table:

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

CDB1 hosts a container that stores continuously updated operational data.

You are designing a solution that will use AS1 to analyze the operational data daily.

You need to recommend a solution to analyze the data without affecting the performance of the operational data store.

What should you include in the recommendation?

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

Correct Answer: C

注：此题出现过两次，一次没有选项 C 答案给的是 PolyBase

Azure Synapse Link for Azure Cosmos DB creates a tight integration between Azure Cosmos DB and Azure Synapse Analytics. It enables customers to run near real-time analytics over their operational data with full performance isolation from their transactional workloads and without an ETL pipeline.

Reference:

<https://docs.microsoft.com/en-us/azure/cosmos-db/synapse-link-frequently-asked-questions>

## Question 23

HOTSPOT -

You deploy several Azure SQL Database instances.

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

### Diagnostics setting

Save Discard Delete Provide feedback

A diagnostic setting specifies a list of categories of platform logs and/or metrics that you want to collect from a resource, and one or more destinations that you would stream them to. Normal usage charges for the destination will occur. [Learn more about the different log categories and contents of those logs](#)

Diagnostic setting name	Diagnostic1
Category details	
<b>log</b>	
<input checked="" type="checkbox"/> SQLInsights	Retention (days) 90
<input checked="" type="checkbox"/> AutomaticTuning	Retention (days) 30
<input type="checkbox"/> QueryStoreRuntimeStatistics	Retention (days) 0
<input type="checkbox"/> QueryStoreWaitStatistics	Retention (days) 0
<input type="checkbox"/> Errors	Retention (days) 0
<input type="checkbox"/> DatabaseWaitStatistics	Retention (days) 0
<input type="checkbox"/> Timeouts	Retention (days) 0
<input type="checkbox"/> Blocks	Retention (days) 0
<input type="checkbox"/> Deadlocks	Retention (days) 0
<b>metric</b>	
<input type="checkbox"/> Basic	Retention (days) 0
Destination details	
<input checked="" type="checkbox"/> Send to Log Analytics	
Subscription Azure Pass - Sponsorship	
Log Analytics workspace sk200814 ( eastus )	
<input checked="" type="checkbox"/> Archive to a storage account	
Showing all storage accounts including classic storage accounts	
Location East US	
Subscription Azure Pass - Sponsorship	
Storage account * contoso20	
<input type="checkbox"/> Stream to an event hub	

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

NOTE: Each correct selection is worth one point.

Hot Area:

### Answer Area

The 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:

### Answer Area

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

▼
30 days
90 days
730 days
indefinite

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

▼
30 days
90 days
730 days
indefinite

Box 1: 90 days -

As per exhibit.

Box 2: 730 days -

How long is the data kept?

Raw data points (that is, items that you can query in Analytics and inspect in Search) are kept for up to 730 days.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-monitor/app/data-retention-privacy>

## Question 24

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

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

Correct Answer: C

Password - On-premises applications can use a password-based method for SSO. This choice works when applications are configured for Application Proxy.

With password-based SSO, users sign in to the application with a username and password the first time they access it. After the first sign-on, Azure AD provides the username and password to the application. Password-based SSO enables secure application password storage and replay using a web browser extension or mobile app. This option uses the existing sign-in process provided by the application, enables an administrator to manage the passwords, and doesn't require the user to know the password.

Incorrect:

Choosing an SSO method depends on how the application is configured for authentication.

Cloud applications can use federation-based options, such as OpenID

Connect, OAuth, and SAML.

Federation - When you set up SSO to work between multiple identity providers, it's called federation.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/what-is-single-sign-on>

## Question 25

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.

Hot Area:

**Answer Area**

To provide access to virtual machines on VNET1, use:

Azure Bastion
Just-in-time (JIT) VM access
Azure Web Application Firewall (WAF) in Azure Front Door

To enforce Azure MFA, use:

An Azure Identity Governance access package
A Conditional Access policy that has the Cloud apps assignment set to Azure Windows VM Sign-In
A Conditional Access policy that has the Cloud apps assignment set to Microsoft Azure Management

Answer:

Box 1: From ET User

Answer is Azure Bastion.

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

It provides secure and seamless RDP/SSH connectivity to your virtual machines directly from the Azure portal over TLS.

While JIT access allows access via RDP or SSH, incoming connections is not TLS tcp 443 (but RDP or SSH when the inbound port is temporarily authorized)

<https://docs.microsoft.com/en-us/azure/defender-for-cloud/just-in-time-access-usage?tabs=jit-config-avm%2Cjit-request-asc>

**Answer Area**

To provide access to virtual machines on VNET1, use:

Azure Bastion
Just-in-time (JIT) VM access
Azure Web Application Firewall (WAF) in Azure Front Door

To enforce Azure MFA, use:

An Azure Identity Governance access package
A Conditional Access policy that has the Cloud apps assignment set to Azure Windows VM Sign-In
A Conditional Access policy that has the Cloud apps assignment set to Microsoft Azure Management

#### Box 1: Just-in-time (JIT) VN access

Lock down inbound traffic to your Azure Virtual Machines with Microsoft Defender for Cloud's just-in-time (JIT) virtual machine (VM) access feature. This reduces exposure to attacks while providing easy access when you need to connect to a VM.

Note: Threat actors actively hunt accessible machines with open management ports, like RDP or SSH. Your legitimate users also use these ports, so it's not practical to keep them closed.

When you enable just-in-time VM access, you can select the ports on the VM to which inbound traffic will be blocked.

To solve this dilemma, Microsoft Defender for Cloud offers JIT. With JIT, you can lock down the inbound traffic to your VMs, reducing exposure to attacks while providing easy access to connect to VMs when needed.

#### Box 2: A conditional Access policy that has Cloud Apps assignment set to Azure Windows VM Sign-In

You can enforce Conditional Access policies such as multi-factor authentication or user sign-in risk check before authorizing access to Windows VMs in Azure that are enabled with Azure AD sign in. To apply Conditional Access policy, you must select the "Azure Windows VM Sign-In" app from the cloud apps or actions assignment option and then use Sign-in risk as a condition and/or require multi-factor authentication as a grant access control.

Reference:

<https://docs.microsoft.com/en-us/azure/defender-for-cloud/just-in-time-access-overview>

<https://docs.microsoft.com/en-us/azure/active-directory/devices/howto-vm-sign-in-azure-ad-windows>

## Question 26

You are designing an Azure governance solution.

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

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

What should you include in the solution?

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

Correct Answer: C

You apply tags to your Azure resources, resource groups, and subscriptions to logically organize them into a taxonomy. Each tag consists of a name and a value pair.

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.

Reference:

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

## Question 27

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

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

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

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

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

What should you recommend?

- A. In the Azure AD tenant of Contoso, create cloud-only user accounts for the Fabrikam developers.
- B. Configure a forest trust between the on-premises Active Directory forests of Contoso and Fabrikam.
- C. Configure an organization relationship between the Microsoft 365 tenants of Fabrikam and Contoso.
- D. In the Azure AD tenant of Contoso, create guest accounts for the Fabrikam developers.

Correct Answer: D

You can use the capabilities in Azure Active Directory B2B to collaborate with external guest users and you can use Azure RBAC to grant just the permissions that guest users need in your environment.

Incorrect:

Not B: Forest trust is used for internal security, not external access.

Reference:

<https://docs.microsoft.com/en-us/azure/role-based-access-control/role-assignments-external-users>

## Question 28

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

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

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

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

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

What should you recommend?

- A. 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: A

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 30 - New

Your company has the divisions shown in the following table.

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

Sub1 contains an Azure App Service web app named App1. App1 uses Azure AD for single-tenant user authentication. Users from contoso.com can authenticate to App1.

You need to recommend a solution to enable users in the fabrikam.com tenant to authenticate to App1.

What should you recommend?

- A. Configure the Azure AD provisioning service.
- B. Enable Azure AD pass-through authentication and update the sign-in endpoint.
- C. Use Azure AD entitlement management to govern external users.
- D. Configure Azure AD join.

Correct Answer: C

Entitlement management is an identity governance capability that enables organizations to manage identity and access lifecycle at scale by automating access request workflows, access assignments, reviews, and expiration. Entitlement management allows delegated non-admins to create access packages that external users from other organizations can request access to. One and multi-stage approval workflows can be configured to evaluate requests, and provision users for time-limited access with recurring reviews. Entitlement management enables policy-based provisioning and deprovisioning of external accounts.

Note: Access Packages -

An access package is the foundation of entitlement management. Access packages are groupings of policy-governed resources a user needs to collaborate on a project or do other tasks. For example, an access package might include: access to specific SharePoint sites, enterprise applications including your custom in-house and SaaS apps like Salesforce, Microsoft Teams.

Microsoft 365 Groups.

Incorrect:

Not A: Automatic provisioning refers to creating user identities and roles in the cloud applications that users need access to. In addition to creating user identities, automatic

provisioning includes the maintenance and removal of user identities as status or roles change.

Not B: Privileged Identity Management provides time-based and approval-based role activation to mitigate the risks of excessive, unnecessary, or misused access permissions on resources that you care about. Here are some of the key features of Privileged Identity Management:

Provide just-in-time privileged access to Azure AD and Azure resources

Assign time-bound access to resources using start and end dates

Etc.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/6-secure-access-entitlement-management>

<https://docs.microsoft.com/en-us/azure/active-directory/app-provisioning/how-provisioning-works>

<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure>

## Question 31 – New

HOTSPOT -

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

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

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

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

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

NOTE: Each correct selection is worth one point.

### Answer Area

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

Azure AD
Azure API Management
The web APIs

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

Azure AD
Azure API Management
The web APIs

Answer:

### Answer Area

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

Azure AD
Azure API Management
The web APIs

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

Azure AD
Azure API Management
The web APIs

Box 1: Azure AD -

Grant permissions in Azure AD.

Box 2: Azure API Management -

Configure a JWT validation policy to pre-authorize requests. Pre-authorize requests in API Management with the Validate JWT policy, by validating the access tokens of each incoming request. If a request does not have a valid token, API Management blocks it.

Reference: <https://docs.microsoft.com/en-us/azure/api-management/api-management-howto-protect-backend-with-aad>

## Question 33 - New

You need to recommend a solution to generate a monthly report of all the new Azure Resource Manager (ARM) resource deployments in your Azure subscription.

What should you include in the recommendation?

- A. Azure Log Analytics
- B. Azure Arc
- C. Azure Analysis Services
- D. Application Insights

Correct Answer: A

The Activity log is a platform log in Azure that provides insight into subscription-level events. Activity log includes such information as when a resource is modified or when a virtual machine is started.

Activity log events are retained in Azure for 90 days and then deleted.

For more functionality, you should create a diagnostic setting to send the Activity log to one or more of these locations for the following reasons: to Azure Monitor Logs for more complex querying and alerting, and longer retention (up to two years) to Azure Event Hubs to forward outside of Azure to Azure Storage for cheaper, long-term archiving

Note: Azure Monitor builds on top of Log Analytics, the platform service that gathers log and metrics data from all your resources. The easiest way to think about it is that Azure Monitor is the marketing name, whereas Log Analytics is the technology that powers it.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-monitor/essentials/activity-log>

## Question 34

You need to recommend a solution to generate a monthly report of all the new Azure Resource Manager (ARM) resource deployments in your Azure subscription.

What should you include in the recommendation?

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

Answer: A

Explanation:

Activity logs are kept for 90 days. You can query for any range of dates, as long as the starting

date isn't more than 90 days in the past.

Through activity logs, you can determine:

what operations were taken on the resources in your subscription

who started the operation

when the operation occurred

the status of the operation

the values of other properties that might help you research the operation

Reference:

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

## Question 35 - New

You are developing an app that will read activity logs for an Azure subscription by using Azure Functions.

You need to recommend an authentication solution for Azure Functions. The solution must minimize administrative effort.

What should you include in the recommendation?

- A. an enterprise application in Azure AD
- B. system-assigned managed identities
- C. shared access signatures (SAS)
- D. application registration in Azure AD

Answer: B

✉️  **lmy** 6 days, 13 hours ago

Should be A

   upvoted 1 times

✉️  **dank42** 6 days, 14 hours ago

Correct

   upvoted 1 times

✉️  **maku067** 6 days, 16 hours ago

**Selected Answer: B**

Seems correct.

   upvoted 1 times

✉️  **Aziza\_Adam** 6 days, 19 hours ago

A first you need to register the App

   upvoted 1 times

✉️  **IRISone** 2 days, 19 hours ago

it doesn't say what needs to be done, but what is to be recommended. It's designing. B is correct

   upvoted 1 times

✉️  **Clarkszw** 6 days, 20 hours ago

B, tested in the lab! :p

   upvoted 1 times

## Question 37

You have 100 servers that run Windows Server 2012 R2 and host Microsoft SQL Server 2014 instances. The instances host databases that have the following characteristics:

- ☞ Stored procedures are implemented by using CLR.
- ☞ The largest database is currently 3 TB. None of the databases will ever exceed 4 TB.

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

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

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

What should you include in the recommendation?

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

Correct Answer: B

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.

Reference:

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

## Question 38

You have an Azure subscription that contains an Azure Blob Storage account named store1. You have an on-premises file server named Server1 that runs Windows Server 2016. Server1 stores 500 GB of company files.

You need to store a copy of the company files from Server1 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 Logic Apps integration account
- B. an Azure Import/Export job
- C. Azure Data Factory
- D. an Azure Analysis services On-premises data gateway
- E. an Azure Batch account

Correct Answer: BC

B: You can use the Azure Import/Export service to securely export large amounts of data from Azure Blob storage. The service requires you to ship empty drives to the Azure datacenter. The service exports data from your storage account to the drives and then ships the drives back.

C: Big data requires a service that can orchestrate and operationalize processes to refine these enormous stores of raw data into actionable business insights.

Azure Data Factory is a managed cloud service that's built for these complex hybrid extract-transform-load (ETL), extract-load-transform (ELT), and data integration projects.

Reference:

<https://docs.microsoft.com/en-us/azure/storage/common/storage-import-export-data-from-blobs>

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

## Question 39

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

Correct Answer: D

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 40

HOTSPOT -

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

- ⇒ Maximize data throughput.
- ⇒ Prevent the modification of data for one year.
- ⇒ Minimize latency for read and write operations.

Which Azure Storage account type and storage service should you recommend? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

### Answer Area

Storage account type:

BlobStorage
BlockBlobStorage
FileStorage
StorageV2 with Premium performance
StorageV2 with Standard performance

Storage service:

Blob
File
Table

Answer:

### Answer Area

Storage account type:

BlobStorage
BlockBlobStorage
FileStorage
StorageV2 with Premium performance
StorageV2 with Standard performance

Storage service:

Blob
File
Table

Box 1: BlockBlobStorage -

Block Blob is a premium storage account type for block blobs and append blobs.

Recommended for scenarios with high transaction rates, or scenarios that use smaller objects or require consistently low storage latency.

Box 2: Blob -

The Archive tier is an offline tier for storing blob data that is rarely accessed. The Archive tier offers the lowest storage costs, but higher data retrieval costs and latency compared to the online tiers (Hot and Cool). Data must remain in the Archive tier for at least 180 days or be subject to an early deletion charge.

Reference:

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

## Question 41

HOTSPOT -

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

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

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

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

Which storage accounts should you recommend using for each app? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

### Answer Area

App1:

Storage1 and storage2 only
Storage1 and storage3 only
Storage1, storage2, and storage3 only
Storage1, storage2, storage3, and storage4

App2:

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

Answer:

## Answer Area

App1:

Storage1 and storage2 only
Storage1 and storage3 only
Storage1, storage2, and storage3 only
Storage1, storage2, storage3, and storage4

App2:

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

Box 1: Storage1 and storage3 only

Need to use Standard accounts.

Data stored in a premium block blob storage account cannot be tiered to hot, cool, or archive using Set Blob Tier or using Azure Blob Storage lifecycle management

Box 2: Storage1 and storage4 only

Azure File shares requires Premium accounts. Only Storage1 and storage4 are premium.

Reference:

<https://docs.microsoft.com/en-us/azure/storage/blobs/access-tiers-overview#feature-support>

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

## Question 42

You are designing an application that will be hosted in Azure.

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

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 43

You are designing a SQL database solution. The solution will include 20 databases that will be 20 GB each and have varying usage patterns.

You need to recommend a database platform to host the databases. The solution must meet the following requirements:

- ☞ The solution must meet a Service Level Agreement (SLA) of 99.99% uptime.
- ☞ The compute resources allocated to the databases must scale dynamically.
- ☞ The solution must have reserved capacity.
- ☞ Compute charges must be minimized.

What should you include in the recommendation?

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

Correct Answer: A

The compute and storage redundancy is built in for business critical databases and elastic pools, with a SLA of 99.99%.

Reserved capacity provides you with the flexibility to temporarily move your hot databases in and out of elastic pools (within the same region and performance tier) as part of your normal operations without losing the reserved capacity benefit.

Reference:

<https://azure.microsoft.com/en-us/blog/understanding-and-leveraging-azure-sql-database-sla/>

## Question 44

HOTSPOT -

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

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

- ☞ Support scaling up and down.
- ☞ Support geo-redundant backups.
- ☞ Support a database of up to 75 TB.
- ☞ Be optimized for online transaction processing (OLTP).

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

NOTE: Each correct selection is worth one point.

Hot Area:

### Answer Area

Service:

Azure SQL Database
Azure SQL Managed Instance
Azure Synapse Analytics
SQL Server on Azure Virtual Machines

Service tier:

Basic
Business Critical
General Purpose
Hyperscale
Premium
Standard

Answer:

## Answer Area

Service:

Azure SQL Database
Azure SQL Managed Instance
Azure Synapse Analytics
SQL Server on Azure Virtual Machines

Service tier:

Basic
Business Critical
General Purpose
Hyperscale
Premium
Standard

Box 1: Azure SQL Database -

Azure SQL Database:

Database size always depends on the underlying service tiers (e.g. Basic, Business Critical, Hyperscale).

It supports databases of up to 100 TB with Hyperscale service tier model.

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

Azure SQL Database and SQL Managed Instance enable you to dynamically add more resources to your database with minimal downtime.

Box 2: Hyperscale -

Incorrect Answers:

- ☞ SQL Server on Azure VM: geo-replication not supported.
- ☞ Azure Synapse Analytics is not optimized for online transaction processing (OLTP).
- ☞ Azure SQL Managed Instance max database size is up to currently available instance size (depending on the number of vCores).

Max instance storage size (reserved) - 2 TB for 4 vCores

- 8 TB for 8 vCores
- 16 TB for other sizes

Reference:

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

<https://medium.com/awesome-azure/azure-difference-between-azure-sql-database-and-sql-server-on-vm-comparison-azure-sql-vs-sql-server-vm-cf02578a1188>

## Question 45

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

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

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

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

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

NOTE: Each correct selection is worth one point.

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

Correct Answer: CD

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 46

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

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

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

What should you include in the recommendation?

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

Correct Answer: A

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 47

HOTSPOT -

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

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

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

Name	Resource group	Location	Account kind
storage1	RG1	East US	StorageV2 (general purposev2)
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

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

NOTE: Each correct selection is worth one point.

Hot Area:

### Answer Area

Statements	Yes	No
When you enable auditing for SQLdb1, you can store the audit information to storage1.	<input type="radio"/>	<input type="radio"/>
When you enable auditing for SQLdb2, you can store the audit information to storage2.	<input type="radio"/>	<input type="radio"/>
When you enable auditing for SQLdb3, you can store the audit information to storage2.	<input type="radio"/>	<input type="radio"/>

Answer:

**Answer Area**

Statements	Yes	No
When you enable auditing for SQLdb1, you can store the audit information to storage1.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
When you enable auditing for SQLdb2, you can store the audit information to storage2.	<input type="checkbox"/>	<input checked="" type="checkbox"/>
When you enable auditing for SQLdb3, you can store the audit information to storage2.	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Box 1: Yes -

Auditing works fine for a Standard account.

Box 2: No -

Auditing limitations: Premium storage is currently not supported.

Box 3: No -

Auditing limitations: Premium storage is currently not supported.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-sql/database/auditing-overview#auditing-limitations>

## Question 48

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 DB 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.

Select and Place:

Tools	Answer Area
AzCopy	From the SQL Server 2012 database: <input type="text"/> Tool
Azure Cosmos DB Data Migration Tool	From the table in the SQL Server 2014 database: <input type="text"/> Tool
Data Management Gateway	
Data Migration Assistant	

Answer:

Tools	Answer Area
AzCopy	From the SQL Server 2012 database: <input type="text"/> Data Migration Assistant
Azure Cosmos DB Data Migration Tool	From the table in the SQL Server 2014 database: <input type="text"/> Azure Cosmos DB Data Migration Tool
Data Management Gateway	
Data Migration Assistant	

Box 1: Data Migration Assistant -

The Data Migration Assistant (DMA) helps you upgrade to a modern data platform by detecting compatibility issues that can impact database functionality in your new version of SQL Server or Azure SQL Database. DMA recommends performance and reliability improvements for your target environment and allows you to move your schema, data, and uncontained objects from your source server to your target server.

Incorrect:

AzCopy is a command-line utility that you can use to copy blobs or files to or from a storage account.

Box 2: Azure Cosmos DB Data Migration Tool

Azure Cosmos DB Data Migration Tool can be used to migrate a SQL Server Database table to Azure Cosmos.

Reference:

<https://docs.microsoft.com/en-us/sql/dma/dma-overview>

<https://docs.microsoft.com/en-us/azure/cosmos-db/cosmosdb-migrationchoices>

## Question 49

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

Correct Answer: D

You can create Data Factory pipelines that copies data from Azure Blob Storage to Azure SQL Database. The configuration pattern applies to copying from a file-based data store to a relational data store.

Required steps:

Create a data factory.

Create Azure Storage and Azure SQL Database linked services.

Create Azure Blob and Azure SQL Database datasets.

Create a pipeline contains a Copy activity.

Start a pipeline run.

Monitor the pipeline and activity runs.

Reference:

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

## Question 50

You have an Azure subscription.

Your on-premises network contains a file server named Server1. Server1 stores 500 GB data 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 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.
- B. Create a general-purpose v1 storage account. Create a blob container and copy the files to the blob container.
- C. 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.
- D. 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.
- E. Create a general-purpose v1 storage account. Create a file share in the storage account and copy the files to the file share.

Correct Answer: AD

To minimize costs: The Archive tier is optimized for storing data that is rarely accessed and stored for at least 180 days with flexible latency requirements (on the order of hours).

Reference:

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

## Question 51

You have an app named App1 that uses two on-premises Microsoft SQL Server databases named DB1 and DB2.

You plan to migrate DB1 and DB2 to Azure

You need to recommend an Azure solution to host DB1 and DB2. The solution must meet the following requirements:

- ☞ Support server-side transactions across DB1 and DB2.
- ☞ Minimize administrative effort to update the solution.

What should you recommend?

- A. two Azure SQL databases in an elastic pool
- B. two databases on the same Azure SQL managed instance
- C. two databases on the same SQL Server instance on an Azure virtual machine
- D. two Azure SQL databases on different Azure SQL Database servers

Correct Answer: B

Elastic database transactions for Azure SQL Database and Azure SQL Managed Instance allow you to run transactions that span several databases.

SQL Managed Instance enables system administrators to spend less time on administrative tasks because the service either performs them for you or greatly simplifies those tasks.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-sql/database/elastic-transactions-overview?view=azuresql>

## Question 52

You need to design a highly available Azure SQL database that meets the following requirements:

- ☞ Failover between replicas of the database must occur without any data loss.
- ☞ The database must remain available in the event of a zone outage.
- ☞ Costs must be minimized.

Which deployment option should you use?

- A. Azure SQL Database Hyperscale
- B. Azure SQL Database Premium
- C. Azure SQL Database Basic
- D. Azure SQL Managed Instance General Purpose

Correct Answer: B

Azure SQL Database Premium tier supports multiple redundant replicas for each database that are automatically provisioned in the same datacenter within a region. This design leverages the SQL Server AlwaysON technology and provides resilience to server failures with 99.99% availability SLA and RPO=0.

With the introduction of Azure Availability Zones, we are happy to announce that SQL Database now offers built-in support of Availability Zones in its Premium service tier.

Incorrect:

Not A: Hyperscale is more expensive than Premium.

Not C: Need Premium for Availability Zones.

Not D: Zone redundant configuration that is free on Azure SQL Premium is not available on Azure SQL Managed Instance.

Reference:

<https://azure.microsoft.com/en-us/blog/azure-sql-database-now-offers-zone-redundant-premium-databases-and-elastic-pools/>

## Question 53

You need to design a highly available Azure SQL database that meets the following requirements:

- Failover between replicas of the database must occur without any data loss.
- The database must remain available in the event of a zone outage.
- Costs must be minimized.

Which deployment option should you use?

- A. Azure SQL Database Business Critical
- B. Azure SQL Database Managed Instance Business Critical
- C. Azure SQL Database Hyperscale
- D. Azure SQL Database Standard

Answer: A

Answer: D

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/azure-sql/database/service-tier-business-critical>

## Question 54

You need to design a highly available Azure SQL database that meets the following requirements:

- ⇒ Failover between replicas of the database must occur without any data loss.
- ⇒ The database must remain available in the event of a zone outage.
- ⇒ Costs must be minimized.

Which deployment option should you use?

- A. Azure SQL Managed Instance Business Critical
- B. Azure SQL Database Premium
- C. Azure SQL Database Basic
- D. Azure SQL Managed Instance General Purpose

ET User: B

<https://docs.microsoft.com/en-us/azure/azure-sql/database/high-availability-sla?view=azuresql&tabs=azure-powershell>

Zone-redundant configuration is not available in SQL Managed Instance. In SQL Database this feature is only available when the Gen5 hardware is selected.

To prevent Data Loss, Premium/Business Critical is required:

The primary node constantly pushes changes to the secondary nodes in order and ensures that the data is persisted to at least one secondary replica before committing each transaction. This process guarantees that if the primary node crashes for any reason, there is always a fully synchronized node to fail over to.

Suggested Answer: D

General Purpose service tier provides zone redundant availability.

There are two high availability architectural models:

- \* Standard availability model that is based on a separation of compute and storage. It relies on high availability and reliability of the remote storage tier. This architecture targets budget-oriented business applications that can tolerate some performance degradation during maintenance activities.
- \* Premium availability model that is based on a cluster of database engine processes. It relies on the fact that there is always a quorum of available database engine nodes. This architecture targets mission-critical applications with high IO performance, high transaction rate and guarantees minimal performance impact to your workload during maintenance activities.

Note: Zone-redundant configuration for the general purpose service tier is offered for both serverless and provisioned compute. This configuration utilizes Azure Availability Zones to replicate databases across multiple physical locations within an

Azure region. By selecting zone-redundancy, you can make your new and existing serverless and provisioned general-purpose single databases and elastic pools resilient to a much larger set of failures, including catastrophic datacenter outages, without any changes of the application logic.

Incorrect:

Not A: Azure SQL Managed Instance Business Critical is more expensive.

Not B: Premium is more expensive.

Not C: Azure SQL Database Basic, and General purpose provide only locally redundant availability.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-sql/database/high-availability-sl>

## Question 55

You need to design a highly available Azure SQL database that meets the following requirements:

- ⇒ Failover between replicas of the database must occur without any data loss.
- ⇒ The database must remain available in the event of a zone outage.
- ⇒ Costs must be minimized.

Which deployment option should you use?

- A. Azure SQL Managed Instance Business Critical
- B. Azure SQL Database Premium
- C. Azure SQL Database Basic
- D. Azure SQL Database Hyperscale

Correct Answer: B

Azure SQL Database Premium meets the requirements and is the least expensive.

Note: There are two high availability architectural models:

- \* Standard availability model that is based on a separation of compute and storage. It relies on high availability and reliability of the remote storage tier. This architecture targets budget-oriented business applications that can tolerate some performance degradation during maintenance activities.
- \* Premium availability model that is based on a cluster of database engine processes. It relies on the fact that there is always a quorum of available database engine nodes. This architecture targets mission-critical applications with high IO performance, high transaction rate and guarantees minimal performance impact to your workload during maintenance activities.

Note: Zone-redundant configuration for the general purpose service tier is offered for both serverless and provisioned compute. This configuration utilizes Azure Availability Zones to replicate databases across multiple physical locations within an Azure region. By selecting zone-redundancy, you can make your new and existing serverless and provisioned general-purpose single databases and elastic pools resilient to a much larger set of failures, including catastrophic datacenter outages, without any changes of the application logic.

Incorrect:

Not A: Azure SQL Managed Instance Business Critical is more expensive.

Not C: Azure SQL Database Basic, and General purpose provide only locally redundant availability.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-sql/database/high-availability-sla>

## Question 56

You need to design a highly available Azure SQL database that meets the following requirements:

- ☞ Failover between replicas of the database must occur without any data loss.
- ☞ The database must remain available in the event of a zone outage.
- ☞ Costs must be minimized.

Which deployment option should you use?

- A. Azure SQL Database Serverless
- B. Azure SQL Database Business Critical
- C. Azure SQL Database Basic
- D. Azure SQL Database Standard

Correct Answer: A

A (67%)

B (33%)

Now your new and existing serverless Azure SQL Databases allow for zone redundant configuration. This feature utilizes Azure Availability Zones to replicate databases across multiple physical locations within an Azure region. By selecting zone redundancy, you can make your serverless databases resilient to a much larger set of failures, including catastrophic datacenter outages without any changes of the application logic.

The SQL Database serverless compute tier optimizes price-performance and simplifies performance management for single databases with intermittent, unpredictable usage by auto-scaling compute and billing for compute used per second.

Incorrect:

Not B: Azure SQL Database Business Critical is a more expensive solution.

Not C: Azure SQL Database Basic does not provide zone redundancy.

Not D: Azure SQL Database Standard is a more expensive solution.

Reference:

<https://azure.microsoft.com/en-us/updates/public-preview-zone-redundant-configuration-for-azure-sql-database-serverless-compute-tier/>

## Question 57

HOTSPOT -

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

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

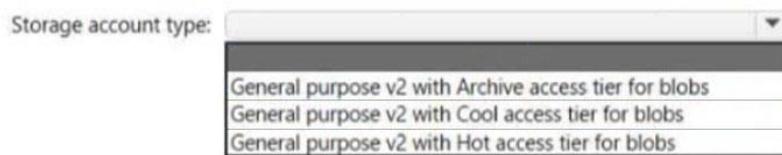
- ☞ All the data written to storage must be retained for five years.
- ☞ Once the data is written, the data can only be read. Modifications and deletion must be prevented.
- ☞ After five years, the data can be deleted, but never modified.
- ☞ Data access charges must be minimized.

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

NOTE: Each correct selection is worth one point.

Hot Area:

### Answer Area



Configuration to prevent modifications and deletions:



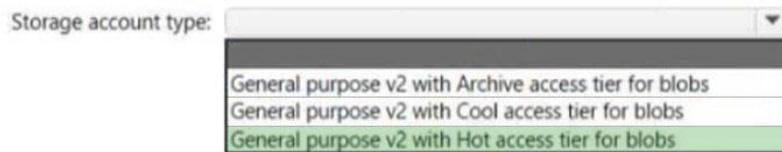
Answer:

ET User:

Box 1: General purpose v2 with Hot access tier for blobs

Box 2: Container Access policy

### Answer Area



Configuration to prevent modifications and deletions:



Box 1: General purpose v2 with Hot access tier for blobs

Note:

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

\* Data access charges must be minimized

Hot tier has higher storage costs, but lower access and transaction costs.

Incorrect:

Not Archive: Lowest storage costs, but highest access, and transaction costs.

Not Cool: Lower storage costs, but higher access and transaction costs.

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.

Reference:

<https://docs.microsoft.com/en-us/azure/storage/blobs/access-tiers-overview>

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

## Question 58 - New

HOTSPOT -

You are designing a data storage solution to support reporting.

The solution will ingest high volumes of data in the JSON format by using Azure Event Hubs. As the data arrives, Event Hubs will write the data to storage. The solution must meet the following requirements:

- Organize data in directories by date and time.
- Allow stored data to be queried directly, transformed into summarized tables, and then stored in a data warehouse.
- Ensure that the data warehouse can store 50 TB of relational data and support between 200 and 300 concurrent read operations.

Which service should you recommend for each type of data store? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

### Answer Area

Data store for the ingested data:

Azure Blob Storage  
Azure Data Lake Storage Gen2  
Azure Files  
Azure NetApp Files

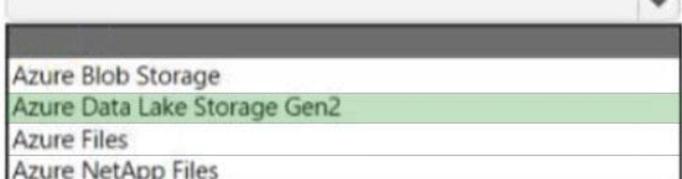
Data store for the data warehouse:

Azure Cosmos DB Cassandra API  
Azure Cosmos DB SQL API  
Azure SQL Database Hyperscale  
Azure Synapse Analytics dedicated SQL pools

Answer:

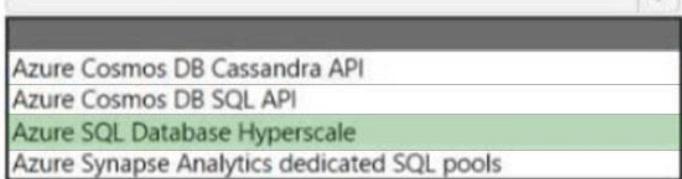
## Answer Area

Data store for the ingested data:



Azure Blob Storage  
Azure Data Lake Storage Gen2  
Azure Files  
Azure NetApp Files

Data store for the data warehouse:



Azure Cosmos DB Cassandra API  
Azure Cosmos DB SQL API  
Azure SQL Database Hyperscale  
Azure Synapse Analytics dedicated SQL pools

### Box 1: Azure Data Lake Storage Gen2

Azure Data Explorer integrates with Azure Blob Storage and Azure Data Lake Storage (Gen1 and Gen2), providing fast, cached, and indexed access to data stored in external storage. You can analyze and query data without prior ingestion into Azure Data Explorer. You can also query across ingested and uningested external data simultaneously.

Azure Data Lake Storage is optimized storage for big data analytics workloads.

Use cases: Batch, interactive, streaming analytics and machine learning data such as log files, IoT data, click streams, large datasets

### Box 2: Azure SQL Database Hyperscale

Azure SQL Database Hyperscale is optimized for OLTP and high throughput analytics workloads with storage up to 100TB.

A Hyperscale database supports up to 100 TB of data and provides high throughput and performance, as well as rapid scaling to adapt to the workload requirements. Connectivity, query processing, database engine features, etc. work like any other database in Azure SQL Database.

Hyperscale is a multi-tiered architecture with caching at multiple levels. Effective IOPS will depend on the workload.

Compare to:

General purpose: 500 IOPS per vCore with 7,000 maximum IOPS

Business critical: 5,000 IOPS with 200,000 maximum IOPS

Incorrect:

\* Azure Synapse Analytics Dedicated SQL pool.

Max database size: 240 TB -

A maximum of 128 concurrent queries will execute and remaining queries will be queued.

Reference:

<https://docs.microsoft.com/en-us/azure/data-explorer/data-lake-query-data>

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

<https://docs.microsoft.com/en-us/azure/synapse-analytics/sql-data-warehouse/sql-data-warehouse-service-capacity-limits>

## Question 59 - New

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

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

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

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

- A. RSA 3072
- B. AES 256
- C. RSA 4096
- D. RSA 2048

Correct Answer: A

**A (75%)**

**B (25%)**

From what I can find, I agree with A, RSA 3072 maximum encryption.

AES256 for built-in cert.

As per below URL, with SQL MI customer managed key

<https://learn.microsoft.com/en-us/azure/azure-sql/database/transparent-data-encryption-byok-overview?view=azuresql>

It's not RSA4096 since that's for storage encryption as per below;

<https://learn.microsoft.com/en-us/azure/storage/common/customer-managed-keys-overview>

<https://learn.microsoft.com/en-us/azure/data-factory/enable-customer-managed-key>

<https://learn.microsoft.com/en-us/azure/virtual-machines/disk-encryption>

## Question 60

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

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

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

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

NOTE: Each correct selection is worth one point.

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

Correct Answer: CD

与 Q45 的 C 选项不一样, C. Azure Cosmos DB SQL API

## Question 61

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

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

- ⇒ Provide the ability to recover in the event of a regional outage.
- ⇒ Support a recovery time objective (RTO) of 15 minutes.
- ⇒ Support a recovery point objective (RPO) of 24 hours.
- ⇒ Support automated recovery.
- ⇒ Minimize costs.

What should you include in the recommendation?

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

Correct Answer: D

Replication with Azure Site Recovery:

- ⇒ RTO is typically less than 15 minutes.
- ⇒ RPO: One hour for application consistency and five minutes for crash consistency.

Incorrect Answers:

B: Too slow.

C: Always On availability group RPO: Because replication to the secondary replica is asynchronous, there's some data loss.

Reference:

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

## Question 62

HOTSPOT -

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

### Policy 1

Associated items   Delete   Save   Discard

---

#### Backup schedule

\*Frequency   \*Time   \*Timezone

Daily   6:00 PM   (UTC) Coordinated Univers...

---

#### Instant Restore

Retain instant recovery snapshot(s) for

3 Day(s)

---

#### Retention range

Retention of daily backup point.

\*At   For

6:00 PM   90 Day(s)

---

Retention of weekly backup point.

\*On   \*At   For

Sunday   6:00 PM   26 Week(s)

---

Retention of monthly backup point.

\*On   \*Day   \*At   For

First   Sunday   6:00 PM   36 Month(s)

---

Retention of yearly backup point.

Not Configured

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

NOTE: Each correct selection is worth one point.

Hot Area:

### Answer Area

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

90 days	▼
26 weeks	▼
36 months	▼
45 months	▼

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

1 hour	▼
1 day	▼
1 week	▼
1 month	▼
1 year	▼

Answer:

### Answer Area

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

90 days	▼
26 weeks	▼
36 months	▼
45 months	▼

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

1 hour	▼
1 day	▼
1 week	▼
1 month	▼
1 year	▼

## Question 63

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.

Hot Area:

### Answer Area

Storage tier:

<input type="checkbox"/>	Hot
<input type="checkbox"/>	Premium
<input type="checkbox"/>	Transaction optimized

Redundancy:

<input type="checkbox"/>	Geo-redundant storage (GRS)
<input type="checkbox"/>	Zone-redundant storage (ZRS)
<input type="checkbox"/>	Locally-redundant storage (LRS)

Answer:

## Answer Area

Storage tier:

Hot	▼
Premium	
Transaction optimized	

Redundancy:

Geo-redundant storage (GRS)	▼
Zone-redundant storage (ZRS)	
Locally-redundant storage (LRS)	

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.

Incorrect Answers:

☞ Hot: Hot file shares offer storage optimized for general purpose file sharing scenarios such as team shares. Hot file shares are offered on the standard storage hardware backed by HDDs.

☞ Transaction optimized: Transaction optimized file shares enable transaction heavy workloads that don't need the latency offered by premium file shares.

Transaction optimized file shares are offered on the standard storage hardware backed by hard disk drives (HDDs). Transaction optimized has historically been called "standard", however this refers to the storage media type rather than the tier itself (the hot and cool are also "standard" tiers, because they are on standard storage hardware).

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 64

HOTSPOT -

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

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

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

NOTE: Each correct selection is worth one point.

Hot Area:

### **Answer Area**

Application1:	<input type="checkbox"/> BlobStorage with Standard performance, Hot access tier, and Read-access geo-redundant storage (RA-GRS) replication
	<input type="checkbox"/> BlockBlobStorage with Premium performance and Zone-redundant storage (ZRS) replication
	<input type="checkbox"/> General purpose v1 with Premium performance and Locally-redundant storage (LRS) replication
	<input type="checkbox"/> General purpose v2 with Standard performance, Hot access tier, and Locally-redundant storage (LRS) replication
Application2:	<input type="checkbox"/> BlobStorage with Standard performance, Cool access tier, and Geo-redundant storage (GRS) replication
	<input type="checkbox"/> BlockBlobStorage with Premium performance and Zone-redundant storage (ZRS) replication
	<input type="checkbox"/> General purpose v1 with Standard performance and Read-access geo-redundant storage (RA-GRS) replication
	<input type="checkbox"/> General purpose v2 with Standard performance, Cool access tier, and Read-access geo-redundant storage (RA-GRS) replication

Answer:

Box 2: From ET User, maybe GRS

## Answer Area

Application1:

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

Application2:

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

Box 1: BlobStorage with Premium Performance,..

Application1 requires high transaction rates and the lowest possible latency. We need to use Premium, not Standard.

Box 2: General purpose v2 with Standard Performance,..

General Purpose v2 provides access to the latest Azure storage features, including Cool and Archive storage, with pricing optimized for the lowest GB storage prices. These accounts provide access to Block Blobs, Page Blobs, Files, and Queues. Recommended for most scenarios using Azure Storage.

Reference:

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

## Question 65

HOTSPOT -

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

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

What storage solution should you recommend for the app? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

### Answer Area

Storage Account type:

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

Redundancy:

Zone-redundant storage (ZRS)
Locally-redundant storage (LRS)

Answer:

Pre+ZRS

### Answer Area

Storage Account type:

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

Redundancy:

Zone-redundant storage (ZRS)
Locally-redundant storage (LRS)

Box 1: Standard general-purpose v2

Standard general-purpose v2 supports immutable storage.

In general Standard general-purpose v2 is the preferred Microsoft recommendation.

Box 2: Zone-redundant storage (ZRS)

ZRS is more resilient compared to LRS.

Note: RA-GRS is even more resilient, but it is not an option here.

Reference:

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

## Question 66

HOTSPOT -

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

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

You need to recommend a storage solution for the app.

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

Hot Area:

### Answer Area

Azure Storage account kind:

StorageV2
BlobStorage
BlockBlobStorage

Replication:

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

Answer: 存疑

### Answer Area

Azure Storage account kind:

StorageV2
BlobStorage
BlockBlobStorage

Replication:

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

Box 1:

BlockBlobStorage -

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

Box 2:

Reference:

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

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

## Question 67

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

Correct Answer: A

Azure Front Door supports SSL.

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.

Reference:

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

## Question 68

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 point.

Hot Area:

### Answer Area

Storage Account type:	<input type="button" value="▼"/>				
<table border="1"><tr><td>Premium block blobs</td></tr><tr><td>Standard general-purpose v1</td></tr><tr><td>Standard general-purpose v2</td></tr></table>		Premium block blobs	Standard general-purpose v1	Standard general-purpose v2	
Premium block blobs					
Standard general-purpose v1					
Standard general-purpose v2					
Redundancy:	<input type="button" value="▼"/>				
<table border="1"><tr><td>Geo-redundant storage (GRS)</td></tr><tr><td>Zone-redundant storage (ZRS)</td></tr><tr><td>Locally-redundant storage (LRS)</td></tr><tr><td>Read-access geo-redundant storage (RA-GRS)</td></tr></table>		Geo-redundant storage (GRS)	Zone-redundant storage (ZRS)	Locally-redundant storage (LRS)	Read-access geo-redundant storage (RA-GRS)
Geo-redundant storage (GRS)					
Zone-redundant storage (ZRS)					
Locally-redundant storage (LRS)					
Read-access geo-redundant storage (RA-GRS)					

Answer:

### Answer Area

Storage Account type:	<input type="button" value="▼"/>				
<table border="1"><tr><td>Premium block blobs</td></tr><tr><td>Standard general-purpose v1</td></tr><tr><td>Standard general-purpose v2</td></tr></table>		Premium block blobs	Standard general-purpose v1	Standard general-purpose v2	
Premium block blobs					
Standard general-purpose v1					
Standard general-purpose v2					
Redundancy:	<input type="button" value="▼"/>				
<table border="1"><tr><td>Geo-redundant storage (GRS)</td></tr><tr><td>Zone-redundant storage (ZRS)</td></tr><tr><td>Locally-redundant storage (LRS)</td></tr><tr><td>Read-access geo-redundant storage (RA-GRS)</td></tr></table>		Geo-redundant storage (GRS)	Zone-redundant storage (ZRS)	Locally-redundant storage (LRS)	Read-access geo-redundant storage (RA-GRS)
Geo-redundant storage (GRS)					
Zone-redundant storage (ZRS)					
Locally-redundant storage (LRS)					
Read-access geo-redundant storage (RA-GRS)					

Box 1: Standard general-purpose v2

Standard general-purpose v2 meets the requirements and minimizes the costs.

Box 2: Zone-redundant storage (ZRS)

ZRS protects against a Datacenter failure, while minimizing the costs.

Reference:

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

## Question 69

HOTSPOT -

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

App1 stores database connection strings in KV1.

App1 performs the following types of requests to KV1:

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

You are evaluating the continuity of service for App1.

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

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

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

NOTE: Each correct selection is worth one point.

Hot Area:

### Answer Area

To where will KV1 fail over?

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

During the failover, which request type will be unavailable?

Get
List
Wrap
Delete
Unwrap
Backup
Decrypt
Encrypt

Answer:

## Answer Area

To where will KV1 fail over?

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

During the failover, which request type will be unavailable?

Get
List
Wrap
Delete
Unwrap
Backup
Decrypt
Encrypt

Box 1: A server in the 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.

Regions are paired for cross-region replication based on proximity and other factors.

Box 2: Delete -

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

List certificates -

Get certificates -

List secrets -

Get secrets -

List keys -

Get (properties of) keys -

Encrypt -

Decrypt -

Wrap -

Unwrap -

Verify -

Sign -

Backup -

Reference:

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

## Question 70

DRAG DROP -

Your company identifies the following business continuity and disaster recovery objectives for virtual machines that host sales, finance, and reporting applications in the company's on-premises data center:

- The sales application must be able to fail over to a second on-premises data center.
- The reporting application must be able to recover point-in-time data at a daily granularity. The RTO is eight hours.
- The finance application requires that data be retained for seven years. In the event of a disaster, the application must be able to run from Azure. The recovery time objective (RTO) is 10 minutes.

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

What should you recommend for each application? To answer, drag the appropriate services to the correct applications. Each service may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:

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

Answer:

Services	Answer Area
Azure Backup only	Sales: Azure Site Recovery only
Azure Site Recovery and Azure Backup	Finance: Azure Site Recovery and Azure Backup
Azure Site Recovery only	Reporting: Azure Backup only

Box 1: Azure Site Recovery -

Azure Site Recovery -

Coordinates virtual-machine and physical-server replication, failover, and fullback.

DR solutions have low Recovery point objectives; DR copy can be behind by a few seconds/minutes.

DR needs only operational recovery data, which can take hours to a day. Using DR data for

long-term retention is not recommended because of the fine-grained data capture. Disaster recovery solutions have smaller Recovery time objectives because they are more in sync with the source. Remote monitor the health of machines and create customizable recovery plans.

Box 2: Azure Site Recovery and Azure Backup

Backup ensures that your data is safe and recoverable while Site Recovery keeps your workloads available when/if an outage occurs.

Box 3: Azure Backup only -

Azure Backup -

Backs up data on-premises and in the cloud

Have wide variability in their acceptable Recovery point objective. VM backups usually one day while database backups as low as 15 minutes.

Backup data is typically retained for 30 days or less. From a compliance view, data may need to be saved for years. Backup data is ideal for archiving in such instances.

Because of a larger Recovery point objective, the amount of data a backup solution needs to process is usually much higher, which leads to a longer Recovery time objective.

Reference:

<https://lighthousemsp.com/whats-the-difference-between-azure-backup-and-azure-site-recovery/>

## Question 71 - New

### HOTSPOT

You have an on-premises Microsoft SQL Server database named SQL1.

You plan to migrate SQL1 to Azure.

You need to recommend a hosting solution for SQL1. The solution must meet the following requirements:

- Support the deployment of multiple secondary, read-only replicas.
- Support automatic replication between primary and secondary replicas.
- Support failover between primary and secondary replicas within a 15-minute recovery time objective (RTO).

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

Azure service or service tier:

	▼
Azure SQL Database	
Azure SQL managed Instance	
The Hyperscale service tier	

Replication mechanism:

	▼
Active geo-replication	
Auto-failover groups	
Standard geo-replication	

Answer:

ET User:

Azure service or service tier "Azure SQL Managed Instance"

Replication mechanism should be "Auto failover groups"

Azure SQL Managed Instance is a fully managed, Azure-based version of SQL Server that can be used to host your on-premises SQL Server database in the cloud. It supports the deployment of multiple secondary, read-only replicas and can automatically replicate data between primary and secondary replicas. It also supports failover between primary and secondary replicas within a 15-minute RTO, which meets the requirement for the solution to have a recovery time objective of 15 minutes.

Auto failover groups is a feature of Azure SQL Managed Instance that allows you to automatically failover between primary and secondary replicas in the event of an outage or failure. It supports the deployment of multiple secondary, read-only replicas and can

automatically replicate data between primary and secondary replicas. It also supports failover between primary and secondary replicas within a 15-minute RTO, which meets the requirement for the solution to have a recovery time objective of 15 minutes.

## Answer Area

Azure service or service tier:

Azure SQL Database
Azure SQL managed Instance
The Hyperscale service tier

Replication mechanism:

Active geo-replication
Auto-failover groups
Standard geo-replication

## Question 72 - New

HOTSPOT

You have two on-premises Microsoft SQL Server 2017 instances that host an Always On availability group named AG1. AG1 contains a single database named DB1.

You have an Azure subscription that contains a virtual machine named VM1. VM1 runs Linux and contains a SQL Server 2019 instance.

You need to migrate DB1 to VM1. The solution must minimize downtime on DB1.

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

NOTE: Each correct selection is worth one point.

Prepare for the migration by:

- Adding a secondary replica to AG1
- Creating an Always On availability group on VM1
- Upgrading the on-premises SQL Server instances

Perform the migration by using:

- A distributed availability group
- Azure Migrate
- Log shipping

Answer:

Prepare for the migration by:

- Adding a secondary replica to AG1
- Creating an Always On availability group on VM1
- Upgrading the on-premises SQL Server instances

Perform the migration by using:

- A distributed availability group
- Azure Migrate
- Log shipping

## Question 73

You have an Azure subscription that contains a Basic Azure virtual WAN named VirtualWAN1 and the virtual hubs shown in the following table.

Name	Location
Hub1	US East
Hub2	US West

You have an ExpressRoute circuit in the US East Azure 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. Enable the ExpressRoute premium add-on.
- D. Create a hub virtual network in US East.

Correct Answer: A

A basic Azure virtual WAN does not support express route. You have to upgrade to standard.

Reference:

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

## Question 74

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

Correct Answer: B

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.

Reference:

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

## Question 75

Your company has the infrastructure shown in the following table.

Location	Resource
Azure	<ul style="list-style-type: none"><li>• Azure subscription named Subscription1</li><li>• 20 Azure web apps</li></ul>
On-premises datacenter	<ul style="list-style-type: none"><li>• Active Directory domain</li><li>• Server running Azure AD Connect</li><li>• Linux computer named Server1</li></ul>

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

Server1 runs an application named App1 that uses LDAP queries to verify user identities in the on-premises Active Directory domain.

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

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

You need to recommend a solution to ensure that App1 continues to function after the migration. The solution must meet the security policy.

What should you include in the recommendation?

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

Correct Answer: D

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.

Reference:

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

## Question 76

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 Consumption plan
- B. Azure Functions in the Premium plan
- C. Azure Functions in the Consumption plan
- D. Azure Logic Apps in the integrated service environment

注意与下题的区别

Correct Answer: B

Virtual connectivity is included in the Premium plan.

Reference:

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

## Question 77

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

注意与上题的区别

Answer: D

Explanation:

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

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

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

Reference:

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

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

## Question 78

You have an on-premises network and an Azure subscription. The on-premises network has several branch offices.

A branch office in Toronto contains a virtual machine named VM1 that is configured as a file server. Users access the shared files on VM1 from all the offices.

You need to recommend a solution to ensure that the users can access the shared files as quickly as possible if the Toronto branch office is inaccessible.

What should you include in the recommendation?

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

Correct Answer: D

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.

Reference:

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

## Question 79

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. Server is prevented from accessing the internet.

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

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

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

NOTE: Each correct selection is worth one point.

Hot Area:

### Answer Area

On-premises:

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

Azure:

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

Answer:

## Answer Area

On-premises:

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

Azure:

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

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:

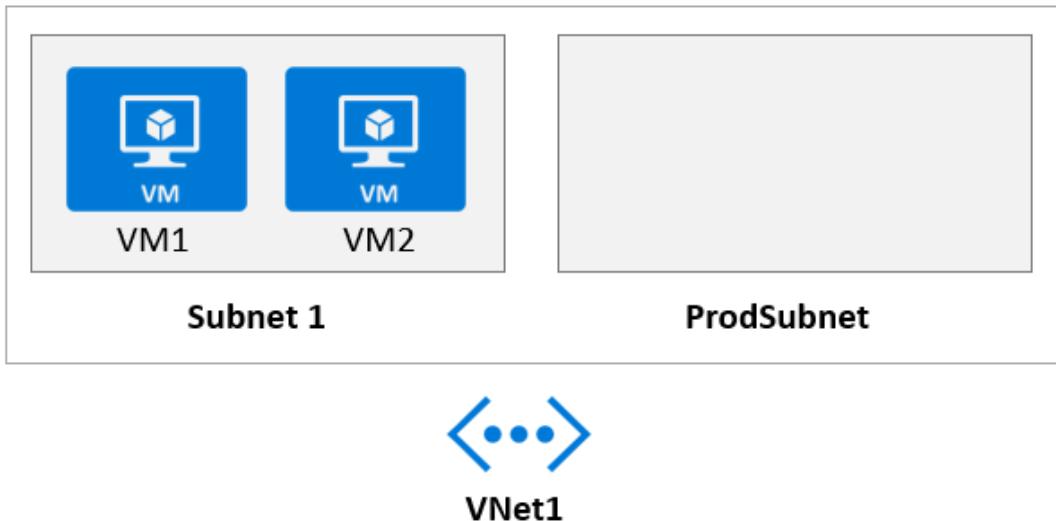
<https://docs.microsoft.com/en-us/azure/connectors/connectors-create-api-sqlazure>

## Question 80

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.



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.

Virtual network		
Location	Virtual network	Subnet
West Europe	VNet1	ProdSubnet

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

NOTE: Each correct selection is worth one point.

Hot Area:

**Answer Area**

Statements	Yes	No
The API is available to partners over the internet.	<input type="radio"/>	<input type="radio"/>
The APIM instance can access real-time data from VM1.	<input type="radio"/>	<input type="radio"/>
A VPN gateway is required for partner access.	<input type="radio"/>	<input type="radio"/>

Answer:

**Answer Area**

Statements	Yes	No
The API is available to partners over the internet.	<input checked="" type="radio"/>	<input type="radio"/>
The APIM instance can access real-time data from VM1.	<input checked="" type="radio"/>	<input type="radio"/>
A VPN gateway is required for partner access.	<input type="radio"/>	<input checked="" type="radio"/>

Reference:

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

## Question 81

DRAG DROP -

Your company has an existing web app that runs on Azure virtual machines. You need to ensure that the app is protected from SQL injection attempts and uses a layer-7 load balancer. The solution must minimize disruptions to the code of the app. What should you recommend? 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.

Services	Answer Area
Web Application Firewall (WAF)	Azure service: <input type="text" value="Service"/>
Azure Application Gateway	Feature: <input type="text" value="Service"/>

⋮

⋮

⋮

⋮

⋮

Answer:

Services	Answer Area
Web Application Firewall (WAF)	Azure service: <input type="text" value="Azure Application Gateway"/>
Azure Application Gateway	Feature: <input type="text" value="Web Application Firewall (WAF)"/>

⋮

⋮

⋮

⋮

⋮

Box 1: Azure Application Gateway

The Azure Application Gateway Web Application Firewall (WAF) provides protection for web applications. These protections are provided by the Open Web Application Security Project (OWASP) Core Rule Set (CRS).

Box 2: Web Application Firewall (WAF)

Reference: <https://docs.microsoft.com/en-us/azure/web-application-firewall/ag/application-gateway-customize-waf-rules-portal>

## Question 82

You are designing a microservices architecture that will be hosted in an Azure Kubernetes Service (AKS) cluster. Apps that will consume the microservices will be hosted on Azure virtual machines. The virtual machines and the AKS cluster will reside on the same virtual network.

You need to design a solution to expose the microservices to the consumer apps. The solution must meet the following requirements:

- Ingress access to the microservices must be restricted to a single private IP address and protected by using mutual TLS authentication.
- The number of incoming microservice calls must be rate-limited.
- Costs must be minimized.

What should you include in the solution?

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

Correct Answer: D

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 83

You have a .NET web service named Service1 that performs the following tasks:

- ☞ Reads and writes temporary files to the local file system.
- ☞ Writes to the Application event log.

You need to recommend a solution to host Service1 in Azure. The solution must meet the following requirements:

- ☞ Minimize maintenance overhead.
- ☞ Minimize costs.

What should you include in the recommendation?

- A. an 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

Azure Web App meets the requirements and is less expensive compared to VM scale sets.

Reference:

<https://docs.microsoft.com/es-es/azure/app-service/troubleshoot-diagnostic-logs>

## Question 84

You have the Azure resources shown in the following table.

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

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

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

- A. 0
- B. 1
- C. 2
- D. 3

Correct Answer: D

题库答案给的 B

Firewall policies work across regions and subscriptions.

Place all your global configurations in the parent policy.

The parent policy is required to be in the same region as the child policy.

Each of the three regions must have a new parent policy.

Reference:

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

## Question 85

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	400 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% percent 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 and ensure that the database is only available on the first day of each month.

Which service tier should you use?

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

Correct Answer: A

Note: App1 and the data are used on the first day of the month only. See Serverless compute tier below.

The vCore based purchasing model.

The term vCore refers to the Virtual Core. In this purchasing model of Azure SQL Database, you can choose from the provisioned compute tier and serverless compute tier.

- \* Provisioned compute tier: You choose the exact compute resources for the workload.
- \* Serverless compute tier: Azure automatically pauses and resumes the database based on workload activity in the serverless tier. During the pause period, Azure does not charge you for the compute resources.

Reference:

<https://www.sqlshack.com/dtu-and-vcore-based-models-for-azure-sql-databases/>

## Question 86

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

You plan to move all the virtual machines to Azure.

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

What should you use to make the recommendation?

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

Suggested Answer: C

Azure Migrate provides a centralized hub to assess and migrate on-premises servers, infrastructure, applications, and data to Azure. It provides the following:

Unified migration platform: A single portal to start, run, and track your migration to Azure.

Range of tools: A range of tools for assessment and migration.

Reference:

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

## Question 87

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

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

What should you include in the recommendation?

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

Answer: B

You can dynamically provision Azure HPC clusters with Azure CycleCloud.

Azure CycleCloud is the simplest way to manage HPC workloads.

Note: Azure CycleCloud is an enterprise-friendly tool for orchestrating and managing High Performance Computing (HPC) environments on Azure. With

CycleCloud, users can provision infrastructure for HPC systems, deploy familiar HPC schedulers, and automatically scale the infrastructure to run jobs efficiently at any scale.

Through CycleCloud, users can create different types of file systems and mount them to the compute cluster nodes to support HPC workloads.

Reference:

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

## Question 89

HOTSPOT -

You are designing an Azure App Service web app.

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

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

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

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

NOTE: Each correct selection is worth one point.

Hot Area:

### Answer Area

Request routing method:

A Traffic Manager profile
Azure Application Gateway
Azure Load Balancer

Request routing configuration:

Cookie-based session affinity
Performance traffic routing
Priority traffic routing
Weighted traffic routing

Answer:

## Answer Area

Request routing method:

A Traffic Manager profile
Azure Application Gateway
Azure Load Balancer

Request routing configuration:

Cookie-based session affinity
Performance traffic routing
Priority traffic routing
Weighted traffic routing

Box 1: A Traffic Manager profile

To support load balancing across the regions we need a Traffic Manager.

Box 2: Priority traffic routing -

Priority traffic-routing method.

Often an organization wants to provide reliability for their services. To do so, they deploy one or more backup services in case their primary goes down. The 'Priority' traffic-routing method allows Azure customers to easily implement this failover pattern.

Reference:

<https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/app-service-web-app/multi-region>

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

## Question 90

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 ExpressRoute Global Reach circuits to both regions.

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

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

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

NOTE: Each correct selection is worth one point.

Hot Area:

### Answer Area

Routing from the virtual networks to the on-premises locations must be configured by using:

Azure default routes
Border Gateway Protocol (BGP)
User-defined routes

The automatic routing configuration following a failover must be handled by using:

Border Gateway Protocol (BGP)
Hot Standby Routing Protocol (HSRP)
Virtual Router Redundancy Protocol (VRRP)

Answer:

### Answer Area

Routing from the virtual networks to the on-premises locations must be configured by using:

Azure default routes
Border Gateway Protocol (BGP)
User-defined routes

The automatic routing configuration following a failover must be handled by using:

Border Gateway Protocol (BGP)
Hot Standby Routing Protocol (HSRP)
Virtual Router Redundancy Protocol (VRRP)

Box 1: Border Gateway Protocol (BGP)

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.

Box 2: Border Gateway Protocol (BGP)

Incorrect:

Microsoft does not support HSRP or VRRP for high availability configurations.

Reference:

<https://docs.microsoft.com/ja-jp/azure/expressroute/designing-for-disaster-recovery-with-expressroute-privatepeering>

<https://docs.microsoft.com/en-us/azure/expressroute/expressroute-routing>

## Question 91

HOTSPOT -

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

You plan to provision an Azure Storage account to host the files.

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

- ☞ Supports video files of up to 7 TB
- ☞ Provides the highest availability possible
- ☞ Ensures that storage is optimized for the large video files
- ☞ Ensures that files from the on-premises network are uploaded by using ExpressRoute

How should you configure the storage account? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

### Answer Area

Storage account type:	<ul style="list-style-type: none"><li>Premium files shares</li><li>Premium page blobs</li><li>Standard general-purpose v2</li></ul>
Data redundancy:	<ul style="list-style-type: none"><li>Zone-redundant storage (ZRS)</li><li>Locally-redundant storage (LRS)</li><li>Geo-redundant storage (GRS)</li></ul>
Networking:	<ul style="list-style-type: none"><li>Azure Route Server</li><li>A private endpoint</li><li>A service endpoint</li></ul>

Answer:

Box 1 should be v2

## Answer Area

Storage account type:	<table border="1"><tr><td>Premium files shares</td></tr><tr><td>Premium page blobs</td></tr><tr><td>Standard general-purpose v2</td></tr></table>	Premium files shares	Premium page blobs	Standard general-purpose v2
Premium files shares				
Premium page blobs				
Standard general-purpose v2				
Data redundancy:	<table border="1"><tr><td>Zone-redundant storage (ZRS)</td></tr><tr><td>Locally-redundant storage (LRS)</td></tr><tr><td>Geo-redundant storage (GRS)</td></tr></table>	Zone-redundant storage (ZRS)	Locally-redundant storage (LRS)	Geo-redundant storage (GRS)
Zone-redundant storage (ZRS)				
Locally-redundant storage (LRS)				
Geo-redundant storage (GRS)				
Networking:	<table border="1"><tr><td>Azure Route Server</td></tr><tr><td>A private endpoint</td></tr><tr><td>A service endpoint</td></tr></table>	Azure Route Server	A private endpoint	A service endpoint
Azure Route Server				
A private endpoint				
A service endpoint				

Box 1: Premium page blobs -

The maximum size for a page blob is 8 TiB.

Incorrect:

Not Premium file shares:

Max file size for Standard and Premium file shares are 4 TB.

Box 2: Geo-redundant storage (GRS)

GRS provides additional redundancy for data storage compared to LRS or ZRS.

Box 3: A private endpoint -

Azure Private Link allows you to securely link Azure PaaS services to your virtual network using private endpoints. For many services, you just set up an endpoint per resource. This means you can connect your on-premises or multi-cloud servers with Azure Arc and send all traffic over an Azure ExpressRoute or site-to-site

VPN connection instead of using public networks.

Reference:

<https://docs.microsoft.com/en-us/rest/api/storageservices/understanding-block-blobs--append-blobs--and-page-blobs>

<https://docs.microsoft.com/en-us/azure/storage/files/storage-files-scale-targets>

<https://docs.microsoft.com/en-us/azure/azure-arc/servers/private-link-security>

## Question 92

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.
- ☞ Prevent write operations.

You need to recommend which HTTP methods and authorization level to configure.

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

NOTE: Each correct selection is worth one point.

Hot Area

### Answer Area

HTTP methods:

API methods
GET only
GET and POST only
GET, POST, and OPTIONS only

Authorization level:

Function
Anonymous
Admin

Answer:

### Answer Area

HTTP methods:

API methods
GET only
GET and POST only
GET, POST, and OPTIONS only

Authorization level:

Function
Anonymous
Admin

Box 1: GET only, Get for read-only-

Box 2: Anonymous, Anonymous for public operations.

## Question 93

You have an Azure subscription.

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

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

What should you include in the recommendation?

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

Suggested Answer: B

Azure Policies allows you to specify allowed locations, and allowed VM SKUs.

Reference:

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

## Question 94

DRAG DROP -

You have an on-premises network that uses an IP address space of 172.16.0.0/16.

You plan to deploy 30 virtual machines to a new Azure subscription.

You identify the following technical requirements:

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

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

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

NOTE: Each correct selection is worth one point.

Select and Place:

Network Addresses	Answer Area
172.16.0.0/16	Subnet1: <input type="text"/>
172.16.1.0/27	Gateway subnet: <input type="text"/>
192.168.0.0/24	
192.168.1.0/27	

Answer:

Network Addresses	Answer Area
172.16.0.0/16	Subnet1: <input type="text"/>
172.16.1.0/27	Gateway subnet: <input type="text"/>
192.168.0.0/24	
192.168.1.0/27	

## Question 95

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

Answer: C

You can copy and transform data in Azure Data Lake Storage Gen2 using Azure Data Factory or Azure Synapse Analytics.

Reference:

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

## Question 96

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

Answer: C

Deployments can scale across AKS with no delay as cluster autoscaler deploys new nodes in your AKS cluster.

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

- \* The cluster autoscaler watches for pods that can't be scheduled on nodes because of resource constraints. The cluster then automatically increases the number of nodes.
- \* The horizontal pod autoscaler uses the Metrics Server in a Kubernetes cluster to monitor the resource demand of pods. If an application needs more resources, the number of pods is automatically increased to meet the demand.

Incorrect:

Not D: If your application needs to rapidly scale, the horizontal pod autoscaler may schedule more pods than can be provided by the existing compute resources in the node pool. If configured, this scenario would then trigger the cluster autoscaler to deploy additional nodes in the node pool, but it may take a few minutes for those nodes to successfully provision and allow the Kubernetes scheduler to run pods on them.

Reference:

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

## Question 97

HOTSPOT -

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

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

You add a new data factory.

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

NOTE: Each correct selection is worth one point.

Hot Area:

### Answer Area

From Server1:

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

From the data factory:

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

Answer:

### Answer Area

From Server1:

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

From the data factory:

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

Box 1: Install a self-hosted integration runtime.

If your data store is located inside an on-premises network, an Azure virtual network, or Amazon Virtual Private Cloud, you need to configure a self-hosted integration runtime to connect to it.

The Integration Runtime to be used to connect to the data store. You can use Azure Integration Runtime or Self-hosted Integration Runtime (if your data store is located in private network). If not specified, it uses the default Azure Integration Runtime.

Box 2: Create a pipeline.

You perform the Copy activity with a pipeline.

Reference:

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

## Question 98

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

Answer: C

To rapidly scale application workloads in an AKS cluster, you can use virtual nodes. With virtual nodes, you have quick provisioning of pods, and only pay per second for their execution time. You don't need to wait for Kubernetes cluster autoscaler to deploy VM compute nodes to run the additional pods. Virtual nodes are only supported with Linux pods and nodes.

Reference:

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

## Question 99

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

Name	Type	Purpose
App1	App Service web app	Processes customer orders
Function1	Function	Checks product availability at vendor 1
Function2	Function	Checks product availability at vendor 2
storage1	Storage account	Stores order processing logs

The order processing system will have the following transaction flow:

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

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

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

Answer: B



Azure Data Factory is the platform 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.

Data Factory contains a series of interconnected systems that provide a complete end-to-end platform for data engineers.

Reference:

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

## Question 100

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 create Azure-SQL Server Integration Services (SSIS) packages. The solution must ensure that the packages can target the SQL Database instances as their destinations.

What should you include in the recommendation?

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

Answer: B

Migrate on-premises SSIS workloads to SSIS using ADF (Azure Data Factory).

When you migrate your database workloads from SQL Server on premises to Azure database services, namely Azure SQL Database or Azure SQL Managed

Instance, your ETL workloads on SQL Server Integration Services (SSIS) as one of the primary value-added services will need to be migrated as well.

Azure-SSIS Integration Runtime (IR) in Azure Data Factory (ADF) supports running SSIS packages. Once Azure-SSIS IR is provisioned, you can then use familiar tools, such as SQL Server Data Tools (SSDT)/SQL Server Management Studio (SSMS), and command-line utilities, such as dtinstall/dtutil/dtexec, to deploy and run your packages in Azure.

Reference:

<https://docs.microsoft.com/en-us/azure/data-factory/scenario-ssis-migration-overview>

## Question 101

You have an Azure virtual machine named VM1 that runs Windows Server 2019 and contains 500 GB of data files.

You are designing a solution that will use Azure Data Factory to transform the data files, and then load the files to Azure Data Lake Storage.

What should you deploy on VM1 to support the design?

- A. the On-premises data gateway
- B. the Azure Pipelines agent
- C. the self-hosted integration runtime
- D. the Azure File Sync agent

Answer: C

The integration runtime (IR) is the compute infrastructure that Azure Data Factory and Synapse pipelines use to provide data-integration capabilities across different network environments.

A self-hosted integration runtime can run copy activities between a cloud data store and a data store in a private network. It also can dispatch transform activities against compute resources in an on-premises network or an Azure virtual network. The installation of a self-hosted integration runtime needs an on-premises machine or a virtual machine inside a private network.

Reference:

<https://docs.microsoft.com/en-us/azure/data-factory/create-self-hosted-integration-runtime>

## Question 102

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

Answer: CE

## Question 103

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

Suggested Answer: D

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.

Incorrect:

Not A: An ARM template is a document that doesn't exist natively in Azure - each is stored either locally or in source control or in Templates (preview). The template gets used for deployments of one or more Azure resources, but once those resources deploy there's no active connection or relationship to the template.

Not C: Blueprints are a declarative way to orchestrate the deployment of various resource templates and other artifacts such as:

Role Assignments -

Policy Assignments -

Azure Resource Manager templates (ARM templates)

Resource Groups -

Reference:

<https://docs.microsoft.com/en-us/azure/governance/blueprints/overview#how-its-different-from-resource-manager-templates>

## Question 104

HOTSPOT -

You have the resources shown in the following table.

Name	Type	Resource group
VM1	Azure virtual machine	RG1
VM2	On-premises virtual machine	<b>Not applicable</b>

You create a new resource group in Azure named RG2.

You need to move the virtual machines to RG2.

What should you use to move each virtual machine? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

## Answer Area

VM1

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

VM2

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

Answer:

此题有争议，部分 ET User 认为两个都是 ARM

## Answer Area

VM1

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

VM2

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

Box 1: Azure Resource Mover -

To move Azure VMs to another region, Microsoft now recommends using Azure Resource Mover.

Incorrect:

Not Azure Migrate: We are not migrating, only moving a VM between resource groups.

Box 2: Azure Migrate -

Azure Migrate provides a centralized hub to assess and migrate on-premises servers, infrastructure, applications, and data to Azure.

Azure migrate includes Azure Migrate Server Migration: Migrate VMware VMs, Hyper-V VMs, physical servers, other virtualized servers, and public cloud VMs to Azure.

Incorrect:

Not Arc: Azure Migrate is adequate. No need to use Azure Arc.

Not Data Migration Assistant: Data Migration Assistant is a stand-alone tool to assess SQL Servers.

It is used to assess SQL Server databases for migration to Azure SQL Database, Azure SQL Managed Instance, or Azure VMs running SQL Server.

Not Lighthouse: Azure Lighthouse enables multi-tenant management with scalability, higher automation, and enhanced governance across resources.

With Azure Lighthouse, service providers can deliver managed services using comprehensive and robust tooling built into the Azure platform. Customers maintain control over who has access to their tenant, which resources they can access, and what actions can be taken.

Reference:

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

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

<https://docs.microsoft.com/en-us/azure/site-recovery/azure-to-azure-tutorial-migrate>

## Question 105

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 Traffic Manager
- C. Azure Application Gateway
- D. Azure Load Balancer

Answer: A

Azure Front Door works across regions and support URL routing (HTTP(S)).

Note: HTTP(S) load-balancing services are Layer 7 load balancers that only accept HTTP(S) traffic. They are intended for web applications or other HTTP(S) endpoints. They include features such as SSL offload, web application firewall, path-based load balancing, and session affinity.

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

Incorrect:

Application Gateway and Azure Load Balancer only work within one single region.

Reference:

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

## Question 106

HOTSPOT -

You have the Azure resources shown in the following table.

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

You need to design a solution that provides on-premises network connectivity to SQLDB1 through PE1.

How should you configure name resolution? To answer select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

### Answer Area

Azure configuration

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

On-premises DNS configuration

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

Answer:

Box1, ET User think it should be 2

### Answer Area

Azure configuration

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

On-premises DNS configuration

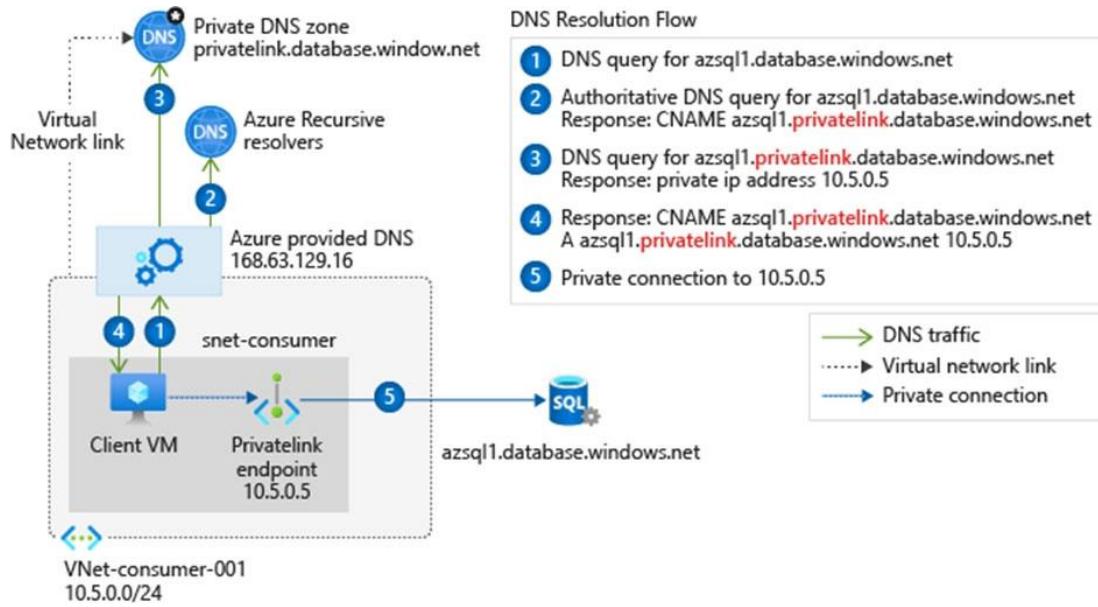
- Forward contoso.com to VM1
- Forward contoso.com to the public DNS zone
- Forward contoso.com to the Azure-provisioned DNS at 168.63.129.16

Box 1:In VNET1, configure a custom DNS server set to the Azure provided DNS at 168.63.129.16

Virtual network workloads without custom DNS server.

This configuration is appropriate for virtual network workloads without a custom DNS server. In this scenario, the client queries for the private endpoint IP address to the Azure-provided DNS service 168.63.129.16. Azure DNS will be responsible for DNS resolution of the private DNS zones.

The following screenshot illustrates the DNS resolution sequence from virtual network workloads using the private DNS zone:



Box 2: Forward contoso.com to VM1

Forward to the DNS server VM1.

Note: You can use the following options to configure your DNS settings for private endpoints:

- \* Use the host file (only recommended for testing). You can use the host file on a virtual machine to override the DNS.
- \* Use a private DNS zone. You can use private DNS zones to override the DNS resolution for a private endpoint. A private DNS zone can be linked to your virtual network to resolve specific domains.
- \* Use your DNS forwarder (optional). You can use your DNS forwarder to override the DNS resolution for a private link resource. Create a DNS forwarding rule to use a private DNS zone on your DNS server hosted in a virtual network.

Reference:

<https://docs.microsoft.com/en-us/azure/private-link/private-endpoint-dns>

## Question 107

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

The solution must meet the following requirements:

- ☞ Deploy the solution on-premises and to Azure.
- ☞ Support low-latency and hyper-scale operations.
- ☞ Allow independent upgrades to each microservice.
- ☞ Set policies for performing automatic repairs to the microservices.

You need to recommend a technology.

What should you recommend?

- A. Azure Container Instance
- B. Azure Logic App
- C. Azure Service Fabric
- D. Azure virtual machine scale set

Answer: C

Azure Service Fabric enables you to create Service Fabric clusters on premises or in other clouds.

Azure Service Fabric is low-latency and scales up to thousands of machines.

Reference:

<https://azure.microsoft.com/en-us/services/service-fabric/>

## Question 108

You are developing a sales application that will contain several Azure cloud services and 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 XML messages.

What should you include in the recommendation?

- A. Azure Notification Hubs
- B. Azure Data Lake
- C. Azure Service Bus
- D. Azure Blob Storage

Answer: C

Asynchronous messaging options.

There are different types of messages and the entities that participate in a messaging infrastructure. Based on the requirements of each message type, Microsoft recommends Azure messaging services. The options include Azure Service Bus, Event Grid, and Event Hubs.

Azure Service Bus queues are well suited for transferring commands from producers to consumers.

Data is transferred between different applications and services using messages. A message is a container decorated with metadata, and contains data. The data can be any kind of information, including structured data encoded with the common formats such as the following ones: JSON, XML, Apache Avro, Plain Text.

Reference:

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

## Question 109 – New

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

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

You need to recommend a solution to continually copy the performance data to the Azure SQL database.

What should you include in the recommendation?

- A. Azure Data Factory
- B. Data Migration Assistant (DMA)
- C. Azure Data Box
- D. Azure Database Migration Service

Answer: A

## Question 110 - New

You need to recommend a storage solution for the records of a mission critical application. The solution must provide a Service Level Agreement (SLA) for the latency of write operations and the throughput.

What should you include in the recommendation?

- A. Azure Data Lake Storage Gen2
- B. Azure Blob Storage
- C. Azure SQL
- D. Azure Cosmos DB

Answer: D

Azure Cosmos DB is Microsoft's fast NoSQL database with open APIs for any scale. It offers turnkey global distribution across any number of Azure regions by transparently scaling and replicating your data wherever your users are. The service offers comprehensive 99.99% SLAs which covers the guarantees for throughput, consistency, availability and latency for the Azure Cosmos DB Database Accounts scoped to a single Azure region configured with any of the five

Consistency Levels or Database Accounts spanning multiple Azure regions, configured with any of the four relaxed Consistency Levels. Azure Cosmos DB allows configuring multiple Azure regions as writable endpoints for a Database Account. In this configuration, Azure Cosmos DB offers 99.999% SLA for both read and write availability.

Reference:

[https://azure.microsoft.com/en-us/support/legal/sla/cosmos-db/v1\\_3/](https://azure.microsoft.com/en-us/support/legal/sla/cosmos-db/v1_3/)

## Question 111 - New

You are planning a storage solution. The solution must meet the following requirements:

- ⇒ Support at least 500 requests per second.
- ⇒ Support a large image, video, and audio streams.

Which type of Azure Storage account should you provision?

- A. standard general-purpose v2
- B. premium block blobs
- C. premium page blobs
- D. premium file shares

ET User: A

A (81%) B (19%)

Answer: B

Use Azure Blobs if you want your application to support streaming and random access scenarios.

It's ideal for applications that require high transaction rates or consistent low-latency storage.

Incorrect:

Not A: Standard storage accounts has a default maximum request rate per storage account 20,000 requests per second<sup>1</sup>, but is not optimized for video and audio streams.

Not C: Page blobs is best suited for random reads and random writes.

Not D: FileStorage storage accounts (premium) has a maximum concurrent request rate of 100,000 IOPS.

Maximum file size is 4 TB, but is not optimized for video and audio streams.

Reference:

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

<https://docs.microsoft.com/en-us/azure/storage/files/storage-files-scale-targets>

## Question 112 - New

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

- ☞ Ensures that applications can access the data by using a REST connection
- ☞ Hosts 20 independent tables of varying sizes and usage patterns
- ☞ Automatically replicates the data to a second Azure region
- ☞ Minimizes costs

What should you recommend?

- A. an Azure SQL Database elastic pool that uses active geo-replication
- B. tables in an Azure Storage account that use geo-redundant storage (GRS)
- C. tables in an Azure Storage account that use read-access geo-redundant storage (RA-GRS)
- D. an Azure SQL database that uses active geo-replication

Answer: B

The Table service offers structured storage in the form of tables. The Table service API is a REST API for working with tables and the data that they contain.

Geo-redundant storage (GRS) has a lower cost than read-access geo-redundant storage (RA-GRS).

Reference:

<https://docs.microsoft.com/en-us/rest/api/storageservices/table-service-rest-api>

<https://docs.microsoft.com/en-us/azure/storage/common/geo-redundant-design>

## Question 113 - New

HOTSPOT -

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

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

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

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

NOTE: Each correct selection is worth one point.

Hot Area:

### Answer Area

The access tokens will be generated by:

Azure AD  
A web app  
A web API

Authorization decisions will be performed by:

Azure AD  
A web app  
A web API

Answer:

### Answer Area

The access tokens will be generated by:

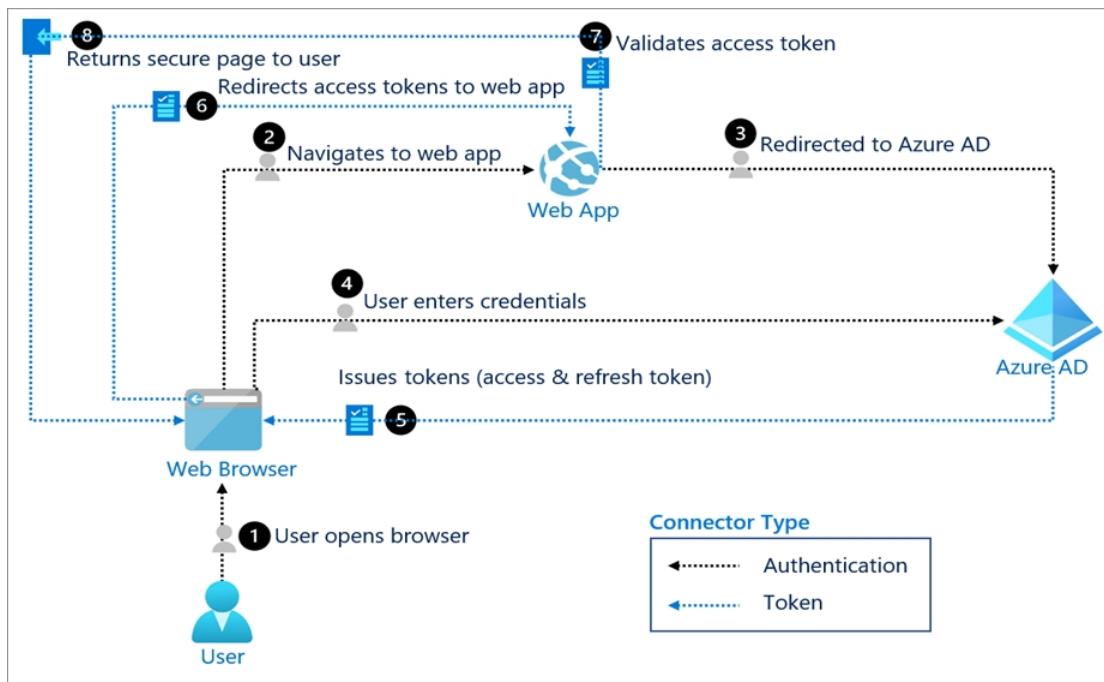
Azure AD  
A web app  
A web API

Authorization decisions will be performed by:

Azure AD  
A web app  
A web API

#### Box 1: Azure AD -

The Azure AD server issues tokens (access & refresh token). See step 5 below in graphic.  
OAuth 2.0 authentication with Azure Active Directory.  
The OAuth 2.0 is the industry protocol for authorization. It allows a user to grant limited access to its protected resources. Designed to work specifically with Hypertext Transfer Protocol (HTTP), OAuth separates the role of the client from the resource owner. The client requests access to the resources controlled by the resource owner and hosted by the resource server (here the Azure AD server). The resource server issues access tokens with the approval of the resource owner. The client uses the access tokens to access the protected resources hosted by the resource server.



#### Box 2: A web API -

Delegated access is used.

The bearer token sent to the web API contains the user identity.

The web API makes authorization decisions based on the user identity.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/auth-oauth2>

<https://docs.microsoft.com/lb-lu/azure/architecture/multitenant-identity/web-api>

## Question 114

HOTSPOT -

You plan to create an Azure environment that will contain a root management group and 10 child management groups. Each child management group will contain five Azure subscriptions. You plan to have between 10 and 30 resource groups in each subscription. You need to design an Azure governance solution. The solution must meet the following requirements:

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

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

NOTE: Each correct selection is worth one point.

Hot Area:

### Answer Area

Level at which to define the blueprints:

The child management groups
The root management group
The subscriptions

Level at which to create the blueprint assignments:

The child management groups
The root management group
The subscriptions

Answer:

### Answer Area

Level at which to define the blueprints:

The child management groups
The root management group
The subscriptions

Level at which to create the blueprint assignments:

The child management groups
The root management group
The subscriptions

Box 1. The root management group

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

The root management group is built into the hierarchy to have all management groups and subscriptions fold up to it. This root management group allows for global policies and Azure role assignments to be applied at the directory level.

Box 2. The root management group

Reference:

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

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

## Question 115

DRAG DROP -

You are designing a virtual machine that will run Microsoft SQL Server and contain two data disks. The first data disk will store log files, and the second data disk will store data. Both disks are P40 managed disks.

You need to recommend a host caching method for each disk. The method must provide the best overall performance for the virtual machine while preserving the integrity of the SQL data and logs.

Which host caching method should you recommend for each disk? To answer, drag the appropriate methods to the correct disks. Each method 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.

Methods	Answer Area
<input type="button" value="None"/>	Log: <input type="text"/>
<input type="button" value="ReadOnly"/>	Data: <input type="text"/>
<input type="button" value="ReadWrite"/>	

Answer:

Methods	Answer Area
<input type="button" value="None"/>	Log: <input type="text" value="None"/>
<input type="button" value="ReadOnly"/>	Data: <input type="text" value="ReadOnly"/>
<input type="button" value="ReadWrite"/>	

Box 1: None - No data disk caching for the Log files.

Box 2: ReadOnly - Guidelines to optimize performance for your SQL Server on Azure Virtual Machines (VMs) include:

Set host caching to read-only for data file disks.

Set host caching to none for log file disks.

Reference: <https://docs.microsoft.com/en-us/azure/azure-sql/virtual-machines/windows/performance-guidelines-best-practices-storage>

## Question 116

You are designing a solution that calculates 3D geometry from height-map data.

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

- ☞ Performs calculations in Azure.
- ☞ Ensures that each node can communicate data to every other node.
- ☞ Maximizes the number of nodes to calculate multiple scenes as fast as possible.
- ☞ Minimizes the amount of effort to implement the solution.

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

NOTE: Each correct selection is worth one point.

- A. Enable parallel file systems on Azure.
- B. Create a render farm that uses virtual machines.
- C. Create a render farm that uses virtual machine scale sets.
- D. Create a render farm that uses Azure Batch.
- E. Enable parallel task execution on compute nodes.

Answer: DE

Multi-instance tasks allow you to run an Azure Batch task on multiple compute nodes simultaneously. These tasks enable high performance computing scenarios like Message Passing Interface (MPI) applications in Batch.

You configure compute nodes for parallel task execution at the pool level.

Azure Batch allows you to set task slots per node up to (4x) the number of node cores.

Reference:

<https://docs.microsoft.com/en-us/azure/batch/batch-mpi>

<https://docs.microsoft.com/en-us/azure/batch/batch-parallel-node-tasks#enable-parallel-task-execution>

## Question 117 - New

You have an on-premises application that consumes data from multiple databases. The application code references database tables by using a combination of the server, database, and table name.

You need to migrate the application data to Azure.

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

NOTE: Each correct selection is worth one point.

- A. SQL Server Stretch Database
- B. SQL Server on an Azure virtual machine
- C. Azure SQL Database
- D. Azure SQL Managed Instance

Answer: BD

Cross-database queries are supported by SQL Server, for example on an Azure virtual machine, and also supported by an Azure SQL Managed Instance.

Reference:

<https://techcommunity.microsoft.com/t5/azure-database-support-blog/cross-database-queries-between-azure-sql-database-and-managed/ba-p/2706670>

## Question 118

HOTSPOT -

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

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

- ☞ Supports user-initiated backups
- ☞ Supports multiple automatically replicated instances across Azure regions
- ☞ Minimizes administrative effort to implement and maintain business continuity

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

NOTE: Each correct selection is worth one point.

Hot Area:

### Answer Area

Deployment solution:

Azure SQL Managed Instance
SQL Server on Azure Virtual Machines
An Azure SQL Database single database

Resiliency solution:

Auto-failover group
Active geo-replication
Zone-redundant deployment

Answer:

ET User: Azure SQL Managed instances & Auto Failover Group

## Answer Area

Deployment solution:

Azure SQL Managed Instance
SQL Server on Azure Virtual Machines
An Azure SQL Database single database

Resiliency solution:

Auto-failover group
Active geo-replication
Zone-redundant deployment

Box 1: an Azure SQL database -

Incorrect answers:

User imitated backups are not supported by Azure SQL Managed instance.

Box 2: Active geo-replication -

Active geo-replication required to multiple automatically replicated instances across Azure regions.

You can manage Azure SQL Database security for geo-restore. SQL database cannot be used for geo-restore.

Incorrect:

Not SQL Server: Active geo-replication requires Azure SQL database.

Reference:

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

## Question 119

You need to design a highly available Azure SQL database that meets the following requirements:

- ☞ Failover between replicas of the database must occur without any data loss.
- ☞ The database must remain available in the event of a zone outage.
- ☞ Costs must be minimized.

Which deployment option should you use?

- A. Azure SQL Managed Instance Business Critical
- B. Azure SQL Managed Instance General Purpose
- C. Azure SQL Database Business Critical
- D. Azure SQL Database Serverless

Answer: D

Azure SQL Database Serverless meets the requirements and is less expensive than Azure SQL Database Business Critical.

Note: General Purpose service tier zone redundant availability.

Zone-redundant configuration for the general purpose service tier is offered for both serverless and provisioned compute.

This configuration utilizes Azure Availability Zones  $\geq$  2 to replicate databases across multiple physical locations within an Azure region. $\geq$  3 By selecting zone-redundancy, you can make your new and existing serverless and provisioned general-purpose single databases and elastic pools resilient to a much larger set of failures, including catastrophic datacenter outages, without any changes of the application logic.

Incorrect:

Not A, not B: Zone-redundant configuration is not available in SQL Managed Instance.

Not C: Azure SQL Database Business Critical is more expensive than Azure SQL Database Serverless.

Note: Premium and Business Critical service tiers use the Premium availability model, which integrates compute resources (sqlservr.exe process) and storage (locally attached SSD) on a single node. High availability is achieved by replicating both compute and storage to additional nodes creating a three to four-node cluster.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-sql/database/high-availability-sla>

## Question 120 - New

You have an Azure web app that uses an Azure key vault named KeyVault1 in the West US Azure region.

You are designing a disaster recovery plan for KeyVault1.

You plan to back up the keys in KeyVault1.

You need to identify to where you can restore the backup.

What should you identify?

- A. any region worldwide
- B. the same region only
- C. KeyVault1 only
- D. the same geography only

Answer: D

Using the backup and restore commands has two limitations:

- \* You can't back up a key vault in one geography and restore it into another geography.
- \* The backup command backs up all versions of each secret.

Incorrect:

Not A: Azure Key Vault does not allow you to move a key vault from one region to another.

You can, however, create a key vault in the new region, manually copy each individual key, secret, or certificate from your existing key vault to the new key vault, and then remove the original key vault.

Reference:

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

## Question 121 – New

You have an on-premises line-of-business (LOB) application that uses a Microsoft SQL Server instance as the backend.

You plan to migrate the on-premises SQL Server instance to Azure virtual machines.

You need to recommend a highly available SQL Server deployment that meets the following requirements:

- ☞ Minimizes costs
- ☞ Minimizes failover time if a single server fails

What should you include in the recommendation?

- A. an Always On availability group that has premium storage disks and a virtual network name (VNN)
- B. an Always On Failover Cluster Instance that has a virtual network name (VNN) and a standard file share
- C. an Always On availability group that has premium storage disks and a distributed network name (DNN)
- D. an Always On Failover Cluster Instance that has a virtual network name (VNN) and a premium file share

Answer: C

C (61%)

B (39%)

Always On availability groups on Azure Virtual Machines are similar to Always On availability groups on-premises, and rely on the underlying Windows Server Failover Cluster.

If you deploy your SQL Server VMs to a single subnet, you can configure a virtual network name (VNN) and an Azure Load Balancer, or a distributed network name (DNN) to route traffic to your availability group listener.

There are some behavior differences between the functionality of the VNN listener and DNN listener that are important to note:

- \* Failover time: Failover time is faster when using a DNN listener since there is no need to wait for the network load balancer to detect the failure event and change its routing.

- \* Etc.

Incorrect:

Not B, not D: Migrate to an Always On availability group, not an Always on Failover cluster Instance.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-sql/virtual-machines/windows/availability-group-overview>

## Question 122 - New

You plan to move a web app named App1 from an on-premises datacenter 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 datacenter becomes unavailable.
- ☞ Costs must be minimized.

What should you include in the recommendation?

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

Answer: C

Need to use a virtual machine as Azure App service does not allow COM components.

Need two availability zones to protect against an Azure datacenter failure.

Incorrect:

Not A, Not D: Cannot use a web app.

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.

Reference:

<https://docs.microsoft.com/en-us/dotnet/azure/migration/app-service#com-and-com-components>

## Question 123

You plan to deploy an application named App1 that will run in containers on Azure Kubernetes Service (AKS) clusters. The AKS clusters will be distributed across four Azure regions.

You need to recommend a storage solution to ensure that updated container images are replicated automatically to all the Azure regions hosting the AKS clusters.

Which storage solution should you recommend?

- A. geo-redundant storage (GRS) accounts
- B. Premium SKU Azure Container Registry
- C. Azure Content Delivery Network (CDN)
- D. Azure Cache for Redis

Answer: B

Enable geo-replication for container images.

Best practice: Store your container images in Azure Container Registry and geo-replicate the registry to each AKS region.

To deploy and run your applications in AKS, you need a way to store and pull the container images. Container Registry integrates with AKS, so it can securely store your container images or Helm charts. Container Registry supports multimaster geo-replication to automatically replicate your images to Azure regions around the world.

Geo-replication is a feature of Premium SKU container registries.

Note:

When you use Container Registry geo-replication to pull images from the same region, the results are:

Faster: You pull images from high-speed, low-latency network connections within the same Azure region.

More reliable: If a region is unavailable, your AKS cluster pulls the images from an available container registry.

Cheaper: There's no network egress charge between datacenters.

Reference:

<https://docs.microsoft.com/en-us/azure/aks/operator-best-practices-multi-region>

## Question 124 - New

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

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

You need to recommend a solution to provide specific Azure AD user accounts with read access to the Cosmos DB databases.

What should you include in the recommendation?

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

Answer: D

The Access control (IAM) pane in the Azure portal is used to configure role-based access control on Azure Cosmos resources. The roles are applied to users, groups, service principals, and managed identities in Active Directory. You can use built-in roles or custom roles for individuals and groups. The following screenshot shows Active Directory integration (RBAC) using access control (IAM) in the Azure portal:

The screenshot shows the 'Access control (IAM)' pane in the Azure portal. The left sidebar has a red box around the 'Access control (IAM)' tab. The main area has tabs for 'Check access', 'Role assignments' (which is selected), 'Deny assignments', and 'Roles'. It says 'Manage access to Azure resources for users, groups, service principals and managed identities at this scope by creating role assignments.' Below are filters for Name, Type (All), Role (6 selected), and Scope (All scopes). A table lists 3 items (2 Users, 1 Groups):

NAME	TYPE	ROLE	SCOPE
ivashni@contoso.com	User	DocumentDB Account Contributor	Assigned
miowx@contoso.com	User	Reader	Assigned
Subscription admins	Group	Owner	Inherited (Subscription)

Note: To use the Azure Cosmos DB RBAC in your application, you have to update the way you initialize the Azure Cosmos DB SDK. Instead of passing your account's primary key, you have to pass an instance of a TokenCredential class. This instance provides the Azure Cosmos DB SDK with the context required to fetch an Azure AD (AAD) token on behalf of the identity you wish to use.

Reference:

<https://docs.microsoft.com/en-us/azure/cosmos-db/role-based-access-control>

<https://docs.microsoft.com/en-us/azure/cosmos-db/how-to-setup-rbac>

## Question 125

You need to recommend an Azure Storage solution that meets the following requirements:

- ☞ The storage must support 1 PB of data.
- ☞ The data must be stored in blob storage.
- ☞ The storage must support three levels of subfolders.
- ☞ The storage must support access control lists (ACLs).

What should you include in the recommendation?

- A. a premium storage account that is configured for block blobs
- B. a general purpose v2 storage account that has hierarchical namespace enabled
- C. a premium storage account that is configured for page blobs
- D. a premium storage account that is configured for file shares and supports large file shares

Answer: B

Default limits for Azure general-purpose v2 (GPv2), general-purpose v1 (GPv1), and Blob storage accounts include:

\* Default maximum storage account capacity: 5 PiB

Blob storage supports Azure Data Lake Storage Gen2, Microsoft's enterprise big data analytics solution for the cloud. Azure Data Lake Storage Gen2 offers a hierarchical file system as well as the advantages of Blob storage.

Blob storage supports Azure Data Lake Storage Gen2, Microsoft's enterprise big data analytics solution for the cloud. Azure Data Lake Storage Gen2 offers a hierarchical file system as well as the advantages of Blob storage

Incorrect:

Not D: In a Premium FileStorage account, storage size is limited to 100 TB.

Reference:

<https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blobs-introduction>

<https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/azure-subscription-service-limits#storage-limits>

## Question 126

HOTSPOT -

You manage a database environment for a Microsoft Volume Licensing customer named Contoso, Ltd. Contoso uses License Mobility through Software Assurance.

You need to deploy 50 databases. The solution must meet the following requirements:

- ☞ Support automatic scaling.
- ☞ Minimize Microsoft SQL Server licensing costs.

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

NOTE: Each correct selection is worth one point.

Hot Area:

### Answer Area

Purchase model:

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

Deployment option:

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

Answer:

### Answer Area

Purchase model:

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

Deployment option:

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

Box 1: vCore -

You can only apply the Azure Hybrid licensing model when you choose a vCore-based purchasing model and the provisioned compute tier for your Azure SQL Database. Azure Hybrid Benefit isn't available for service tiers under the DTU-based purchasing model or for the serverless compute tier.

Box 2: An Azure SQL Database elastic pool

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 SQL Database enable software as a service (SaaS) developers to optimize the price performance for a group of databases within a prescribed budget while delivering performance elasticity for each database.

Reference:

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

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

## Question 127 - New

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

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

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

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

NOTE: Each correct selection is worth one point.

- A. Azure Data Box Gateway
- B. Azure Import/Export service
- C. Azure Data Lake Storage
- D. Azure Data Box Edge
- E. Azure Data Factory

ET User Selected Answer: CE

The correct answer should be C and E

ADF moves data from on-prem Oracle to Data Lake storage, which makes data ready for DataBrick

<https://docs.microsoft.com/en-us/azure/data-factory/load-azure-data-lake-storage-gen2>

DataBricks "ETL" data to Synapse:

<https://docs.microsoft.com/en-us/azure/databricks/scenarios/databricks-extract-load-sql-data-warehouse>

Answer: BE

Data Factory is a data integration service that provides a low-code or no-code approach to construct extract, transform, and load (ETL) processes within a visual environment or by writing your own code.

Exporting data, either to another data technology or to another Dataverse environment, can use any of the same technologies for importing data, such as dataflows, Data Factory, Power Query, and Power Automate.

Reference:

<https://docs.microsoft.com/en-us/power-apps/maker/data-platform/import-export-data>

## Question 128 - New

HOTSPOT -

You are designing a cost-optimized solution that uses Azure Batch to run two types of jobs on Linux nodes. The first job type will consist of short-running tasks for a development environment. The second job type will consist of long-running Message Passing Interface (MPI) applications for a production environment that requires timely job completion.

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

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

NOTE: Each correct selection is worth one point.

Hot Area:

### Answer Area

First job:

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

Second job:

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

Answer:

### Answer Area

First job:

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

Second job:

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

Box 1: User subscription and low-priority virtual machines

The first job type will consist of short-running tasks for a development environment. Among the many ways to purchase and consume Azure resources are Azure low priority VMs and Spot VMs. These virtual machines are compute instances allocated from spare capacity, offered at a highly discounted rate compared to "on demand" VMs. This means they can be a great option for cost savings for the right workloads

Box 2: Batch service and dedicate virtual machines

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

Azure Batch Service is a cloud based job scheduling and compute management platform that enables running large-scale parallel and high performance computing applications efficiently in the cloud. Azure Batch Service provides job scheduling and automatically scaling and managing virtual machines running those jobs.

Reference:

<https://www.parkmycloud.com/blog/azure-low-priority-vms>

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

## Question 129

You are developing a sales application that will contain several Azure cloud services and 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 XML messages.

What should you include in the recommendation?

- A. Azure Notification Hubs
- B. Azure Service Fabric
- C. Azure Queue Storage
- D. Azure Data Lake

Answer: C

Queue Storage delivers asynchronous messaging between application components, whether they are running in the cloud, on the desktop, on an on-premises server, or on a mobile device.

The maximum message size supported by Azure Storage Queues is 64KB while Azure Service Bus Queues support messages up to 256KB. This becomes an important factor especially when the message format is padded (such as XML).

Reference:

<https://docs.microsoft.com/en-us/azure/storage/queues/storage-dotnet-how-to-use-queues>  
<https://blog.kloud.com.au/2016/03/01/cloud-cushioning-using-azure-queues/>

## Question 130

You are developing a sales application that will contain several Azure cloud services and 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 XML messages.

What should you include in the recommendation?

- A. Azure Service Fabric
- B. Azure Data Lake
- C. Azure Service Bus
- D. Azure Traffic Manager

Answer: C

Explanation:

Asynchronous messaging options in Azure include Azure Service Bus, Event Grid, and Event Hubs.

Reference:

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

## Question 131

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>

## Question 132

You are developing a sales application that will contain several Azure cloud services and 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 XML messages.

What should you include in the recommendation?

- A. Azure Notification Hubs
- B. Azure Service Fabric
- C. Azure Queue Storage
- D. Azure Application Gateway

Answer: C

Queue storage is often used to create a backlog of work to process asynchronously. A queue message must be in a format compatible with an XML request using UTF-8 encoding.

Reference:

<https://docs.microsoft.com/en-us/azure/storage/queues/storage-tutorial-queues>

## Question 133 - New

Your company has offices in North America and Europe.

You plan to migrate to Azure.

You need to recommend a networking solution for the new Azure infrastructure. The solution must meet the following requirements:

- The Point-to-Site (P2S) VPN connections of mobile users must connect automatically to the closest Azure region.
- The offices in each region must connect to their local Azure region by using an ExpressRoute circuit.
- Transitive routing between virtual networks and on-premises networks must be supported.
- The network traffic between virtual networks must be filtered by using FQDNs.

What should you include in the recommendation?

- A. Azure Virtual WAN with a secured virtual hub
- B. virtual network peering and application security groups
- C. virtual network gateways and network security groups (NSGs)
- D. Azure Route Server and Azure Network Function Manager

**Suggested Answer: C** 

*Community vote distribution*

A (67%) B (25%) 8%

Answer: A

According to <https://learn.microsoft.com/en-us/azure/architecture/networking/hub-spoke-vwan-architecture#architecture>, which shako shared, I think the answer needs to be A. This supports requirement 1 & 2 (P2S/ExpressRoute) per "Standard Virtual WAN supports any-to-any connectivity (Site-to-Site VPN, VNet, ExpressRoute, Point-to-site endpoints) in a single hub as well as across hubs." Requirement 2 "Virtual network peering is a nontransitive relationship between two virtual networks. While using Azure Virtual WAN, virtual network peering is managed by Microsoft. Each connection added to a hub will also configure virtual network peering. With the help Virtual WAN, all spokes will have a transitive relationship." Finally, requirement 4, "A virtual hub can be created as a secured virtual hub or converted to a secure one anytime after creation. For additional information, see Secure your virtual hub using Azure Firewall Manager." Azure Firewall Manager will allow the FQDN filtering.

## Question 134

You are designing an Azure resource deployment that will use Azure Resource Manager templates. The deployment will use Azure Key Vault to store secrets.

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

- Prevent the IT staff that will perform the deployment from retrieving the secrets directly from Key Vault.
- Use the principle of least privilege.

Which two actions should you recommend? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Create a Key Vault access policy that allows all get key permissions, get secret permissions, and get certificate permissions.
- B. From Access policies in Key Vault, enable access to the Azure Resource Manager for template deployment.
- C. Create a Key Vault access policy that allows all list key permissions, list secret permissions, and list certificate permissions.
- D. Assign the IT staff a custom role that includes the Microsoft.KeyVault/Vaults/Deploy/Action permission.
- E. Assign the Key Vault Contributor role to the IT staff.

Answer: BD

Explanation:

B: To access a key vault during template deployment, set enabledForTemplateDeployment on the key vault to true.

D: The user who deploys the template must have the Microsoft.KeyVault/vaults/deploy/action permission for the scope of the resource group and key vault.

Incorrect Answers:

E: To grant access to a user to manage key vaults, you assign a predefined key vault Contributor role to the user at a specific scope.

If a user has Contributor permissions to a key vault management plane, the user can grant themselves access to the data plane by setting a Key Vault access policy. You should tightly control who has Contributor role access to your key vaults. Ensure that only authorized persons can access and manage your key vaults, keys, secrets, and certificates.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-resource-manager/templates/key-vault-parameter> <https://docs.microsoft.com/en-us/azure/key-vault/general/overview-security>

## Question 135

### QUESTION 61

You have an Azure subscription that contains resources in three Azure regions.

You need to implement Azure Key Vault to meet the following requirements:

- In the event of a regional outage, all keys must be readable.
- All the resources in the subscription must be able to access Key Vault.
- The number of Key Vault resources to be deployed and managed must be minimized.

How many instances of Key Vault should you implement?

- A. 1
- B. 2
- C. 3
- D. 6

Answer: A

争议: A or C

Explanation:

The contents of your key vault are replicated within the region and to a secondary region at least 150 miles away but within the same geography. This maintains high durability of your keys and secrets. See the Azure paired regions document for details on specific region pairs.

Example: Secrets that must be shared by your application in both Europe West and Europe North. Minimize these as much as you can. Put these in a key vault in either of the two regions. Use the same URI from both regions. Microsoft will fail over the Key Vault service internally.

Reference:

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

## Question 136

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

You plan to provide users with access to shared files by using Azure Storage. The users will be provided with different levels of access to various Azure file shares based on their user account or their group membership.

You need to recommend which additional Azure services must be used to support the planned deployment.

What should you include in the recommendation?

- A. an Azure AD enterprise application
- B. Azure Information Protection
- C. an Azure AD Domain Services (Azure AD DS) instance
- D. an Azure Front Door instance

Answer: C

Explanation:

Azure Filessupports identity-based authentication over Server Message Block (SMB) throughtwo types of Domain Services: on-premises Active Directory Domain Services (AD DS) and Azure Active Directory Domain Services (Azure AD DS).

Reference:

<https://docs.microsoft.com/en-us/azure/storage/files/storage-files-identity-auth-active-directory-domain-service-enable>

## Question 137

You are developing a web application that provides streaming video to users. You configure the application to use continuous integration and deployment.

The app must be highly available and provide a continuous streaming experience for users.

You need to recommend a solution that allows the application to store data in a geographical location that is closest to the user.

What should you recommend?

- A. Azure Content Delivery Network (CDN)
- B. Azure Redis Cache
- C. Azure App Service Web Apps
- D. Azure App Service Isolated

Answer: A

Explanation:

Azure Content Delivery Network (CDN) is a global CDN solution for delivering high-bandwidth content. It can be hosted in Azure or any other location. With Azure CDN, you can cache static objects loaded from Azure Blob storage, a web application, or any publicly accessible web server, by using the closest point of presence (POP) server. Azure CDN can also accelerate dynamic content, which cannot be cached, by leveraging various network and routing optimizations.

Reference:

<https://docs.microsoft.com/en-in/azure/cdn/>

## Question 138

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

## Question 139

You have an Azure SQL database named DB1.

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

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

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

NOTE: Each correct selection is worth one point.

Hot Area:

### Answer Area

Helpdesk requirements:

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

Credit Rating requirement:

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

Answer:

## Answer Area

Helpdesk requirements:

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

Credit Rating requirement:

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

Box 1: Dynamic data masking -

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

Box 2: Always encrypted -

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

Reference:

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

## Question 140

You have an Azure Data Lake Storage account that contains 1,000 10-MB CSV files and an Azure Synapse Analytics dedicated SQL pool named sql1. You need to load the files to sql1. The solution must meet the following requirements:

- Maximize data load performance.
- Eliminate the need to define external tables before the data loads.

What should you use?

- A. the copy statement
- B. PolyBase
- C. BCP
- D. the sqlBulkcopy object

Answer: B

## Question 141

You plan to deploy an Azure Databricks Data Science & Engineering workspace and ingest data into the workspace.

Where should you persist the ingested data?

- A. Azure Files
- B. Azure Data Lake
- C. Azure SQL Database
- D. Azure Cosmos DB

Answer: B

Explanation:

The Azure Databricks Data Science & Engineering data lands in a data lake for long term persisted storage, in Azure Blob Storage or Azure Data Lake Storage.

Reference:

<https://docs.microsoft.com/en-us/azure/databricks/scenarios/what-is-azure-databricks-ws>

## Question 142

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

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

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

What should you include the recommendation?

- A. an NGINX ingress controller
- B. Application Gateway Ingress Controller (AGIC)
- C. an HTTP application routing ingress controller
- D. the Kubernetes load balancer service

Answer: B

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

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

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

Reference:

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

## Question 143

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

Which storage solution should you recommend for archiving?

- A. Ingest the log files into an Azure Log Analytics workspace
- B. Use an Azure Blob storage account and a time-based retention policy
- C. Use an Azure Blob storage account configured to use the Archive access tier
- D. Use an Azure file share that has access control enabled

Answer: B

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

Immutable storage supports:

Time-based retention policy support: Users can set policies to store data for a specified interval. When a time-based retention policy is set, blobs can be created and read, but not modified or deleted. After the retention period has expired, blobs can be deleted but not overwritten.

Reference:

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

## Question 144

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

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

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

What should you include in the recommendation?

- A. Microsoft Intune
- B. a Windows Virtual Desktop automation task
- C. Azure Automation
- D. Azure Service Health

Answer: C

Reference:

<https://www.ciraltos.com/automatically-start-and-stop-wvd-vms-with-azure-automation/>

<https://wvdlogix.net/windows-virtual-desktop-host-pool-automation-2>

<https://getnerd.io/academy/how-to-optimize-windows-virtual-desktop-wvd-azure-costs-with-event-based-autoscaling-and-azure-vm-scale-sets/>

## Question 145

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

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

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

What should you include in the recommendation?

- A. an Azure Cosmos DB database
- B. a Microsoft SQL Server Always On availability group on Azure virtual machines
- C. an Azure SQL database in an elastic pool
- D. Azure Table storage that uses geo-redundant storage (GRS) replication

Answer: A

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

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

Incorrect Answers:

D: Not able to do local writes.

Reference:

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

## Question 146

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

Where should you store the backups?

- A. Azure Blob storage that uses the Archive tier
- B. Azure SQL Database
- C. Azure Blob storage that uses the Cool tier
- D. a Recovery Services vault

Answer: A

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

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

Incorrect Answers:

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

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

Reference:

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

## Question 147

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

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

- A. Azure Resource Manager templates remain connected to the deployed resources.
- B. Only Azure Resource Manager templates can contain policy definitions.
- C. Azure Blueprints remain connected to the deployed resources.
- D. Only Azure Blueprints can contain policy definitions.

Answer: C

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.

Incorrect:

Not A: Nearly everything that you want to include for deployment in Azure Blueprints can be accomplished with a Resource Manager template. However, a Resource Manager template is a document that doesn't exist natively in Azure – each is stored either locally or in source control. The template gets used for deployments of one or more Azure resources, but once those resources deploy there's no active connection or relationship to the template.

Reference:

<https://docs.microsoft.com/en-us/answers/questions/26851/how-is-azure-blueprints-different-from-resource-m.html>

## Question 148

You have an Azure subscription that contains an Azure SQL database.

You are evaluating whether to use Azure reservations on the Azure SQL database.

Which tool should you use to estimate the potential savings?

- A. The Purchase reservations blade in the Azure portal
- B. The Advisor blade in the Azure portal
- C. The SQL database blade in the Azure portal

Answer: A

Buy reserved capacity -

1. Sign in to the Azure portal.
2. Select All services > Reservations.
3. Select Add and then in the Purchase Reservations pane, select SQL Database to purchase a new reservation for SQL Database.
4. Fill in the required fields. Existing databases in SQL Database and SQL Managed Instance that match the attributes you select qualify to get the reserved capacity discount. The actual number of databases or managed instances that get the discount depends on the scope and quantity selected.

The screenshot shows a modal dialog titled "Select the product you want to purchase". At the top, there are filter options: "Scope" set to "Single resource group", "Subscription" set to "Finance App - Test", and "Resource Group" set to "cloud-shell-storage-westus". Below these are filters for "Region" (West US 2), "Term" (One Year), and "Add Filter". The main table lists various Azure Database products:

PERFORMANCE TIER	REGION	TERM	DEPLOYMENT TYPE
SQL Database Managed Instance Business Critical - Compute Gen4	West US 2	One Year	SQL Database Managed Instance
SQL Database Managed Instance Business Critical - Compute Gen5	West US 2	One Year	SQL Database Managed Instance
SQL Database Managed Instance General Purpose - Compute Gen4	West US 2	One Year	SQL Database Managed Instance
SQL Database Managed Instance General Purpose - Compute Gen5	West US 2	One Year	SQL Database Managed Instance
SQL Database Single/Elastic Pool Business Critical - Compute Gen4	West US 2	One Year	SQL Database Single/Elastic Pool
SQL Database Single/Elastic Pool Business Critical - Compute Gen5	West US 2	One Year	SQL Database Single/Elastic Pool
SQL Database Single/Elastic Pool General Purpose - Compute Gen4	West US 2	One Year	SQL Database Single/Elastic Pool
SQL Database Single/Elastic Pool General Purpose - Compute Gen5	West US 2	One Year	SQL Database Single/Elastic Pool

At the bottom left are "Select" and "Cancel" buttons. On the right, it says "Price per unit: <UnitPrice>" and "34% Estimated savings" (with "Estimated savings" highlighted by a red box).

5. Review the cost of the capacity reservation in the Costs section.

6. Select Purchase.

7. Select View this Reservation to see the status of your purchase.

Reference:

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

## Question 149

You have an Azure subscription that contains an Azure SQL database.

You plan to use Azure reservations on the Azure SQL database.

To which resource type will the reservation discount be applied?

- A. vCore compute
- B. DTU compute
- C. Storage
- D. License

Answer: A

Quantity: The amount of compute resources being purchased within the capacity reservation.

The quantity is a number of vCores in the selected Azure region and

Performance tier that are being reserved and will get the billing discount. For example, if you run or plan to run multiple databases with the total compute capacity of Gen5 16 vCores in the East US region, then you would specify the quantity as 16 to maximize the benefit for all the databases.

Reference:

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

## Question 150

You are designing an Azure Cosmos DB solution that will host multiple writable replicas in multiple Azure regions.

You need to recommend the strongest database consistency level for the design. The solution must meet the following requirements:

- ☞ Provide a latency-based Service Level Agreement (SLA) for writes.
- ☞ Support multiple regions.

Which consistency level should you recommend?

- A. bounded staleness
- B. strong
- C. session
- D. consistent prefix

Answer: A

Each level provides availability and performance tradeoffs. The following image shows the different consistency levels as a spectrum.



Note: The service offers comprehensive 99.99% SLAs which covers the guarantees for throughput, consistency, availability and latency for the Azure Cosmos DB Database Accounts scoped to a single Azure region configured with any of the five Consistency Levels or Database Accounts spanning multiple Azure regions, configured with any of the four relaxed Consistency Levels.

Incorrect Answers:

B: Strong consistency for accounts with regions spanning more than 5000 miles (8000 kilometers) is blocked by default due to high write latency. To enable this capability please contact support.

Reference:

[https://azure.microsoft.com/en-us/support/legal/sla/cosmos-db/v1\\_3/](https://azure.microsoft.com/en-us/support/legal/sla/cosmos-db/v1_3/)

<https://docs.microsoft.com/en-us/azure/cosmos-db/consistency-levels#consistency-levels-and-latency>

## Question 151

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

ET User: C

The cosmos DB table api is compatible with Azure Table Storage api, just need to change few lines of code.

and the Azure table storage api has uncertain latency and 20000 operation per second limitation.

ET: D

## Question 152

You plan to archive 10 TB of on-premises data files to Azure.

You need to recommend a data archival solution. The solution must minimize the cost of storing the data files.

Which Azure Storage account type should you include in the recommendation?

- A. Standard StorageV2 (general purpose v2)
- B. Standard Storage (general purpose v1)
- C. Premium StorageV2 (general purpose v2)
- D. Premium Storage (general purpose v1)

Answer: A

Standard StorageV2 supports the Archive access tier, which would be the cheapest solution.

Incorrect Answers:

C, D: Each Premium storage account offers 35 TB of disk and 10 TB of snapshot capacity

Reference:

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

## Question 153

You have an Azure subscription.

You need to deploy 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 Kubelet
- B. cluster autoscaler
- C. horizontal pod autoscaler
- D. AKS virtual nodes

Answer: D

Explanation:

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

## Question 154

You need to recommend a solution to deploy containers that run an application. The application has two tiers. Each tier is implemented as a separate Docker Linux-based image. The solution must meet the following requirements:

- ☞ The front-end tier must be accessible by using a public IP address on port 80.
- ☞ The backend tier must be accessible by using port 8080 from the front-end tier only.
- ☞ Both containers must be able to access the same Azure file share.
- ☞ If a container fails, the application must restart automatically.
- ☞ Costs must be minimized.

What should you recommend using to host the application?

- A. Azure Kubernetes Service (AKS)
- B. Azure Service Fabric
- C. Azure Container instances
- D. Azure Container registries

Answer: C

Azure Container Instances enables a layered approach to orchestration, providing all of the scheduling and management capabilities required to run a single container, while allowing orchestrator platforms to manage multi-container tasks on top of it.

Because the underlying infrastructure for container instances is managed by Azure, an orchestrator platform does not need to concern itself with finding an appropriate host machine on which to run a single container.

Azure Container Instances can schedule both Windows and Linux containers with the same API.

Orchestration of container instances exclusively

Because they start quickly and bill by the second, an environment based exclusively on Azure Container Instances offers the fastest way to get started and to deal with highly variable workloads.

Reference:

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

<https://docs.microsoft.com/en-us/azure/container-instances/container-instances-orchestrator-relationship>

## Question 155

our company plans to publish APIs for its services by using Azure API Management. You discover that service responses include the AspNet-Version header. You need to recommend a solution to remove AspNet-Version from the response of the published APIs.

What should you include in the recommendation?

- A. a new product
- B. a modification to the URL scheme
- C. a new policy
- D. a new revision

Answer: C

Set a new transformation policy to transform an API to strip response headers.

Reference:

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

## Question 156

You are designing an Azure solution.

The network traffic for the solution must be securely distributed by providing the following features:

- ☞ HTTPS protocol
- ☞ Round robin routing
- ☞ SSL offloading

You need to recommend a load balancing option.

What should you recommend?

- A. Azure Load Balancer
- B. Azure Internal Load Balancer (ILB)
- C. Azure Traffic Manager
- D. Azure Application Gateway

Answer: D

If you are looking for Transport Layer Security (TLS) protocol termination ("SSL offload") or per-HTTP/HTTPS request, application-layer processing, review Application Gateway.

Application Gateway is a layer 7 load balancer, which means it works only with web traffic (HTTP, HTTPS, WebSocket, and HTTP/2). It supports capabilities such as SSL termination, cookie-based session affinity, and round robin for load-balancing traffic. Load Balancer load-balances traffic at layer 4 (TCP or UDP).

Reference:

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

## Question 157

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

Contoso establishes a partnership with another company named Fabrikam, Inc.

Fabrikam does not have an existing Azure Active Directory (Azure AD) tenant and uses third-party OAuth 2.0 identity management to authenticate its users.

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

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

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

What should you include in the solution?

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

Answer: C

API Management helps organizations publish APIs to external, partner, and internal developers to unlock the potential of their data and services. You can secure API Management using the OAuth 2.0 client credentials flow.

Incorrect Answers:

A: Azure Active Directory B2B uses guest users.

B: Azure Front Door is an Application Delivery Network (ADN) as a service, offering various layer 7 load-balancing capabilities for your applications. Azure Front Door supports HTTP, HTTPS and HTTP/2. Applications can be authorized through OAuth 2.0.

D: Application Proxy is a feature of Azure AD that enables users to access on-premises web applications from a remote client. Application Proxy includes both the Application Proxy service which runs in the cloud, and the Application Proxy connector which runs on an on-premises server. Application Proxy works with:

- ☞ Web applications that use Integrated Windows Authentication for authentication
- ☞ Web applications that use form-based or header-based access

Reference:

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

## Question 158

The developers at your company are building a containerized Python Django app. You need to recommend platform to host the app. The solution must meet the following requirements:

- Support autoscaling.
- Support continuous deployment from an Azure Container Registry.
- Provide built-in functionality to authenticate app users by using Azure Active Directory (Azure AD).

Which platform should you include in the recommendation?

- A. Azure Container instances
- B. an Azure App Service instance that uses containers
- C. Azure Kubernetes Service (AKS)

ET User: B

Answer: C

To keep up with application demands in Azure Kubernetes Service (AKS), you may need to adjust the number of nodes that run your workloads. The cluster autoscaler component can watch for pods in your cluster that can't be scheduled because of resource constraints.

When issues are detected, the number of nodes in a node pool is increased to meet the application demand.

Azure Container Registry is a private registry for hosting container images. It integrates well with orchestrators like Azure Container Service, including Docker Swarm, DC/OS, and the new Azure Kubernetes service. Moreover, ACR provides capabilities such as Azure Active Directory-based authentication, webhook support, and delete operations.

Reference:

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

<https://medium.com/velotio-perspectives/continuous-deployment-with-azure-kubernetes-service-azure-container-registry-jenkins-ca337940151b>

## Question 159

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

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

Answer: BC

**BC (54%)**

**CD (46%)**

B: Forced tunneling lets you redirect or "force" all Internet-bound traffic back to your on-premises location via a Site-to-Site VPN tunnel for inspection and auditing. This is a critical security requirement for most enterprise IT policies. Without forced tunneling, Internet-bound traffic from your VMs in Azure always traverses from Azure network infrastructure directly out to the Internet, without the option to allow you to inspect or audit the traffic. Forced tunneling in Azure is configured via virtual network user-defined routes. C: ExpressRoute lets you extend your on-premises networks into the Microsoft cloud over a private connection facilitated by a connectivity provider. With ExpressRoute, you can establish connections to Microsoft cloud services, such as Microsoft Azure, Office 365, and Dynamics 365. Connectivity can be from an any-to-any (IP VPN) network, a point-to-point Ethernet network, or a virtual cross-connection through a connectivity provider at a co- location facility. ExpressRoute connections do not go over the public Internet. This allows ExpressRoute connections to offer more reliability, faster speeds, lower latencies, and higher security than typical connections over the Internet.

Reference:

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

## Question 160

You are designing a message application that will run on an on-premises Ubuntu virtual machine. The application will use Azure Storage queues.

You need to recommend a processing solution for the application to interact with the storage queues. The solution must meet the following requirements:

- ☞ Create and delete queues daily.
- ☞ Be scheduled by using a CRON job.
- ☞ Upload messages every five minutes.

What should developers use to interact with the queues?

- A. Azure CLI
- B. AzCopy
- C. Azure Data Factory
- D. .NET Core

Answer: D

Incorrect Answers:

A: It is not possible to have Linux running in Windows Azure

B: AzCopy is a command-line utility that you can use to copy blobs or files to or from a storage account.

Reference:

<https://docs.microsoft.com/en-us/azure/storage/queues/storage-tutorial-queues>

## Question 161

You plan to store data in Azure Blob storage for many years. The stored data will be accessed rarely.

You need to ensure that the data in Blob storage is always available for immediate access.

The solution must minimize storage costs.

Which storage tier should you use?

- A. Cool
- B. Archive
- C. Hot

Answer: A

Data in the cool access tier can tolerate slightly lower availability, but still requires high durability, retrieval latency, and throughput characteristics similar to hot data. For cool data, a slightly lower availability service-level agreement (SLA) and higher access costs compared to hot data are acceptable trade-offs for lower storage costs.

Incorrect Answers:

B: Archive storage stores data offline and offers the lowest storage costs but also the highest data rehydrate and access costs.

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

Reference:

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

## Question 162

You use Azure virtual machines to run a custom application that uses an Azure SQL Database instance on the back end.

The IT department at your company recently enabled forced tunneling.

Since the configuration change, developers have noticed degraded performance when they access the database from the Azure virtual machine.

You need to recommend a solution to minimize latency when accessing the database. The solution must minimize costs.

What should you include in the recommendation?

- A. Virtual Network (VNET) service endpoints
- B. Azure virtual machines that run Microsoft SQL Server servers
- C. Azure SQL Database Managed Instance
- D. Always On availability groups

Answer: A

## Question 163

Your network contains an on-premises Active Directory forest.

You discover that when users change jobs within your company, the membership of the user groups are not being updated. As a result, the users can access resources that are no longer relevant to their job.

You plan to integrate Active Directory and Azure Active Directory (Azure AD) by using Azure AD Connect.

You need to recommend a solution to ensure that group owners are emailed monthly about the group memberships they manage.

What should you include in the recommendation?

- A. Azure AD Identity Protection
- B. Azure AD access reviews
- C. Tenant Restrictions
- D. conditional access policies

Answer: B

Reference:

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

## Question 164

You deploy two instances of an Azure web app. One instance is in the East US Azure region and the other instance is in the West US Azure region. The web app uses Azure Blob storage to deliver large files to end users.

You need to recommend a solution for delivering the files to the users. The solution must meet the following requirements:

- ☞ Ensure that the users receive files from the same region as the web app that they access.
- ☞ Ensure that the files only need to be uploaded once.
- ☞ Minimize costs.

What should you include in the recommendation?

- A. Distributed File System (DFS)
- B. read-access geo-redundant storage (RA-GRS)
- C. Azure File Sync
- D. geo-redundant storage (GRS)

**Suggested Answer: B** 

*Community vote distribution*

B (60%)

D (30%)

10%

## Question 165

Hotspot Question

You have an Azure subscription that is linked to an Azure Active Directory Premium Plan 2 tenant.

The tenant has multi-factor authentication (MFA) enabled for all users.

You have the named locations shown in the following table.

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

You have the users shown in the following table.

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

You plan to deploy the Conditional Access policies shown in the following table.

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

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
To ensure that the conditions in CA1 can be evaluated, you must enforce an Azure Active Directory (Azure AD) Identity Protection user risk policy .	<input type="radio"/>	<input type="radio"/>
To ensure that the conditions in CA2 can be evaluated, you must enforce an Azure Active Directory (Azure AD) Identity Protection sign-in risk policy.	<input type="radio"/>	<input type="radio"/>
To ensure that the conditions in CA3 can be evaluated, you must deploy Microsoft Endpoint Manager.	<input type="radio"/>	<input checked="" type="radio"/>

Answer:

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

## Question 166

Hotspot Question

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

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

- A virtual machine is unavailable.
- Connection attempts exceed 50,000 per minute.

Which signal should you include in the solution for each condition? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

An unavailable virtual machine:

Byte Count
Data Path Availability
Health Probe Status
Packet Count
SYN Count

More than 50,000 connection attempts per minute:

Byte Count
Data Path Availability
Health Probe Status
Packet Count
SYN Count

Answer:

An unavailable virtual machine:

Byte Count
Data Path Availability
Health Probe Status
Packet Count
SYN Count

More than 50,000 connection attempts per minute:

Byte Count
Data Path Availability
Health Probe Status
Packet Count
SYN Count

Explanation:

Box 1: Data path availability

Standard Load Balancer continuously exercises the data path from within a region to the load

balancer front end, all the way to the SDN stack that supports your VM. As long as healthy instances remain, the measurement follows the same path as your application's load-balanced traffic. The data path that your customers use is also validated. The measurement is invisible to your application and does not interfere with other operations.

Note: Load balancer distributes inbound flows that arrive at the load balancer's front end to backend pool instances. These flows are according to configured load-balancing rules and health probes. The backend pool instances can be Azure Virtual Machines or instances in a virtual machine scale set.

Box 2: SYN count

SYN (synchronize) count: Standard Load Balancer does not terminate Transmission Control Protocol (TCP) connections or interact with TCP or UDP packet flows. Flows and their handshakes are always between the source and the VM instance. To better troubleshoot your TCP protocol scenarios, you can make use of SYN packets counters to understand how many TCP connection attempts are made. The metric reports the number of TCP SYN packets that were received.

Reference:

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

## Question 167

### Hotspot Question

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

You need to design a solution to monitor the VMs.

Which Azure monitoring services should you use? To answer, select the appropriate Azure monitoring services in the answer area.

NOTE: Each correct selection is worth one point.

Scenario	Azure Monitoring Service
Analyze Network Security Group (NSG) flow logs for VMs attempting internet access.	<ul style="list-style-type: none"><li>Azure Network Watcher</li><li>Azure ExpressRoute Monitor</li><li>Azure Service Endpoint Monitor</li><li>Azure DNS Analytics</li></ul>
Visualize the VMs with their different processes and dependencies on other computers and external processes.	<ul style="list-style-type: none"><li>Azure Service Map</li><li>Azure Activity Log</li><li>Azure Service Health</li><li>Azure Advisor</li></ul>

Answer:

Scenario	Azure Monitoring Service
Analyze Network Security Group (NSG) flow logs for VMs attempting internet access.	<ul style="list-style-type: none"><li>Azure Network Watcher</li><li>Azure ExpressRoute Monitor</li><li>Azure Service Endpoint Monitor</li><li>Azure DNS Analytics</li></ul>
Visualize the VMs with their different processes and dependencies on other computers and external processes.	<ul style="list-style-type: none"><li>Azure Service Map</li><li>Azure Activity Log</li><li>Azure Service Health</li><li>Azure Advisor</li></ul>

Explanation:

Box 1: Azure Network Watcher

Traffic Analytics is a cloud-based solution that provides visibility into user and application activity in cloud networks. Traffic analytics analyzes Network Watcher network security group (NSG) flow logs to provide insights into traffic flow in your Azure cloud. With traffic analytics, you can: Identify security threats to, and secure your network, with information such as open-ports, applications attempting internet access, and virtual machines (VM) connecting to rogue networks.

Visualize network activity across your Azure subscriptions and identify hot spots.

Understand

traffic flow patterns across Azure regions and the internet to optimize your network

deployment for performance and capacity.

Pinpoint network misconfigurations leading to failed connections in your network.

#### Box 2: Azure Service Map

Service Map automatically discovers application components on Windows and Linux systems and maps the communication between services. With Service Map, you can view your servers in the way that you think of them: as interconnected systems that deliver critical services. Service Map shows connections between servers, processes, inbound and outbound connection latency, and ports across any TCP-connected architecture, with no configuration required other than the installation of an agent.

Reference:

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

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

## Question 168

Hotspot Question

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

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

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

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

- Access to at least one database server must be maintained in the event of a regional outage.
- The virtual machines must not connect to the internet directly.

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

NOTE: Each correct selection is worth one point.

Global load balancing service:

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

Availability Zone load balancing service:

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

Answer:

Global load balancing service:

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

Availability Zone load balancing service:

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

Explanation:

Box 1: Azure Traffic Manager

Traffic Manager is a DNS-based traffic load balancer that enables you to distribute traffic optimally to services across global Azure regions, while providing high availability and responsiveness. Because Traffic Manager is a DNS-based load-balancing service, it load balances only at the domain level. For that reason, it can't fail over as quickly as Front Door, because of common challenges around DNS caching and systems not honoring DNS TTLs.

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

Reference:

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

## Question 169

Hotspot Question

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.

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

- Add
- Backup
- Create
- List
- Unwrap Key

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

- Create
- Import
- List
- Wrap Key

Answer:

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

Add
Backup
Create
List
Unwrap Key

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

Create
Import
List
Wrap Key

Explanation:

Box 1: List

Get: Gets the specified Azure key vault.

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

Box 2: Create

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

Reference:

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

## Question 170

Hotspot Question

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

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

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

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

NOTE: Each correct selection is worth one point.

### Answer Area

Send Azure AD logs to:

- An Azure event hub
- An Azure Log Analytics workspace
- An Azure Storage account

Signal type to use for triggering the alerts:

- Activity log
- Log
- Metric

Answer:

### Answer Area

Send Azure AD logs to:

- An Azure event hub
- An Azure Log Analytics workspace
- An Azure Storage account

Signal type to use for triggering the alerts:

- Activity log
- Log
- Metric

Box 1: An Azure Log Analytics workspace

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

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

Box 2: Log -

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

Reference:

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

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

## Question 171

HOTSPOT -

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

**Add OAuth2 service** X

API Management service

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

**Id \*** i  
 ✓

**Description**  
Authorization server description

**Client registration page URL\***  
 ✓

**Authorization grant types**

Authorization code  
 Implicit  
 Resource owner password  
 Client credentials

**Authorization endpoint URL\***

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

NOTE: Each correct selection is worth one point.

Hot Area:

#### Answer Area

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

Background services
Headless device authentication
Web applications

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

Client credentials
Resource owner password
Support state parameter

Answer:

Some ET user think box 2 should be C

#### Answer Area

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

Background services
Headless device authentication
Web applications

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

Client credentials
Resource owner password
Support state parameter

Box 1: Web applications -

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

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

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

Incorrect Answers:

Not Headless device authentication:

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

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

Box 2: Client Credentials -

How to include additional client data

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

POST /c2id/clients HTTP/1.1 -

Host: demo.c2id.com -

Content-Type: application/json -

Authorization: Bearer ztucZS1ZyFKgh0tUEruUtiSTXhnexmd6

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

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

Incorrect Answers:

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

Reference:

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

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

## Question 172

HOTSPOT -

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

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

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

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

NOTE: Each correct selection is worth one point.

Hot Area:

### **Answer Area**

To protect against brute force attacks:

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

To block legacy authentication attempts:

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

Answer:

1. Smart Lockout

Smart lockout is always on, for all Azure AD customers, with these default settings that offer the right mix of security and usability. Customization of the smart lockout settings, with values specific to your organization, requires Azure AD Premium P1 or higher licenses for your users.

2. Security Default

Security defaults:

Available versions of Azure AD Multi-Factor Authentication

Azure AD Multi-Factor Authentication can be used, and licensed, in a few different ways depending on your organization's needs. All tenants are entitled to basic multifactor authentication features via Security Defaults.

## Answer Area

To protect against brute force attacks:

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

To block legacy authentication attempts:

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

Box 1: Smart lockout -

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

Box 2: Conditional access policies

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

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

Reference:

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

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

## Question 173

Hotspot Question

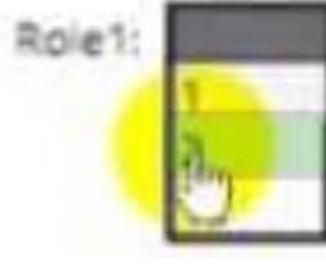
You need to implement the Azure RBAC role assignment. The solution must meet the authentication and authorization requirements.

How many assignment should you configure for the Network Contributor role for Role1? To answer, select appropriate in the answer area.

NOTE: Each correct selection is worth one point.



Answer:



## Question 174

HOTSPOT -

Your company deploys an Azure App Service Web App.

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

You need to improve the performance of the application.

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

NOTE: Each correct selection is worth one point.

Hot Area:

### Answer Area

Store content close to end users.

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

Store content close to the application.

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

Answer:

## Answer Area

Store content close to end users.

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

Store content close to the application.

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

### Box 1: Content Delivery Network -

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

Azure Content Delivery Network (CDN) offers developers a global solution for rapidly delivering high-bandwidth content to users by caching their content at strategically placed physical nodes across the world. Azure CDN can also accelerate dynamic content, which cannot be cached, by leveraging various network optimizations using CDN POPs. For example, route optimization to bypass Border Gateway Protocol (BGP).

### Box 2: Azure Redis Cache -

Azure Cache for Redis is based on the popular software Redis. It is typically used as a cache to improve the performance and scalability of systems that rely heavily on backend data-stores. Performance is improved by temporarily copying frequently accessed data to fast storage located close to the application. With

Azure Cache for Redis, this fast storage is located in-memory with Azure Cache for Redis instead of being loaded from disk by a database.

Reference:

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

## Question 175

DRAG DROP -

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

- Two virtual machines that will run Microsoft SQL Server 2016, will be deployed to different data centers in the same Azure region, and will be part of an Always On availability group
- SQL Server data that will be backed up by using the Automated Backup feature of the SQL Server IaaS Agent Extension (SQLIaaSExtension)

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

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

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

NOTE: Each correct selection is worth one point.

Select and Place:

Storage types	Answer Area
A geo-redundant storage (GRS) account	Operating system: <input type="text"/>
A locally-redundant storage (LRS) account	Databases and logs: <input type="text"/>
A premium managed disk	Backups: <input type="text"/>
A standard managed disk	

Answer:

**Storage types**

- A geo-redundant storage (GRS) account
- A locally-redundant storage (LRS) account
- A premium managed disk
- A standard managed disk

**Answer Area**

- Operating system: A premium managed disk
- Databases and logs: A premium managed disk
- Backups: A locally-redundant storage (LRS) account

## Question 176

HOTSPOT -

You have five .NET Core applications that run on 10 Azure virtual machines in the same subscription.

You need to recommend a solution to ensure that the applications can authenticate by using the same Azure Active Directory (Azure AD) identity. The solution must meet the following requirements:

- Ensure that the applications can authenticate only when running on the 10 virtual machines.
- Minimize administrative effort.

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

Hot Area:

### Answer Area

To provision the Azure AD identity:

Create a system-assigned Managed Identities for Azure resources
Create a user-assigned Managed Identities for Azure resources
Register each application in Azure AD

To authenticate, request a token by using:

An Azure AD v1.0 endpoint
An Azure AD v2.0 endpoint
An Azure Instance Metadata Service identity OAuth2 endpoint

Answer:

From ET User, box 1 should be user-assigned mi

## Answer Area

To provision the Azure AD identity:

- Create a system-assigned Managed Identities for Azure resources
- Create a user-assigned Managed Identities for Azure resources
- Register each application in Azure AD

To authenticate, request a token by using:

- An Azure AD v1.0 endpoint
- An Azure AD v2.0 endpoint
- An Azure Instance Metadata Service identity OAuth2 endpoint

## Question 177

HOTSPOT -

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

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

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

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

NOTE: Each correct selection is worth one point.

Hot Area:

### Answer Area

Virtual machine size:

Compute optimized Standard_F8s
General purpose Standard_B8ms
High performance compute Standard_H16r
Memory optimized Standard_E16s_v3

Feature:

Receive side scaling (RSS)
Remote Direct Memory Access (RDMA)
Single root I/O virtualization (SR-IOV)
Virtual Machine Multi-Queue (VMMQ)

Answer:

From ET Users' Answers are:

1. Compute Optimized Standard F8s
2. Single Root I/O Virtualization (SR-IOV)

## Answer Area

Virtual machine size:

Compute optimized Standard_F8s
General purpose Standard_B8ms
High performance compute Standard_H16r
Memory optimized Standard_E16s_v3

Feature:

Receive side scaling (RSS)
Remote Direct Memory Access (RDMA)
Single root I/O virtualization (SR-IOV)
Virtual Machine Multi-Queue (VMMQ)