

Microsoft.AZ-204.vDec-2023.by.Tracy.132q

Number: AZ-204
Passing Score: 800
Time Limit: 120
File Version: 23.0

Exam Code: AZ-204
Exam Name: Developing Solutions for Microsoft Azure

01 - Develop Azure compute solutions

Case study

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

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

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

To start the case study

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. When you are ready to answer a question, click the Question button to return to the question.

Current environment

Windows Server 2016 virtual machine

This virtual machine (VM) runs BizTalk Server 2016. The VM runs the following workflows:

Ocean Transport - This workflow gathers and validates container information including container contents and arrival notices at various shipping ports.

Inland Transport - This workflow gathers and validates trucking information including fuel usage, number of stops, and routes.

The VM supports the following REST API calls:

Container API - This API provides container information including weight, contents, and other attributes.

Location API - This API provides location information regarding shipping ports of call and trucking stops.

Shipping REST API - This API provides shipping information for use and display on the shipping website.

Shipping Data

The application uses MongoDB JSON document storage database for all container and transport information.

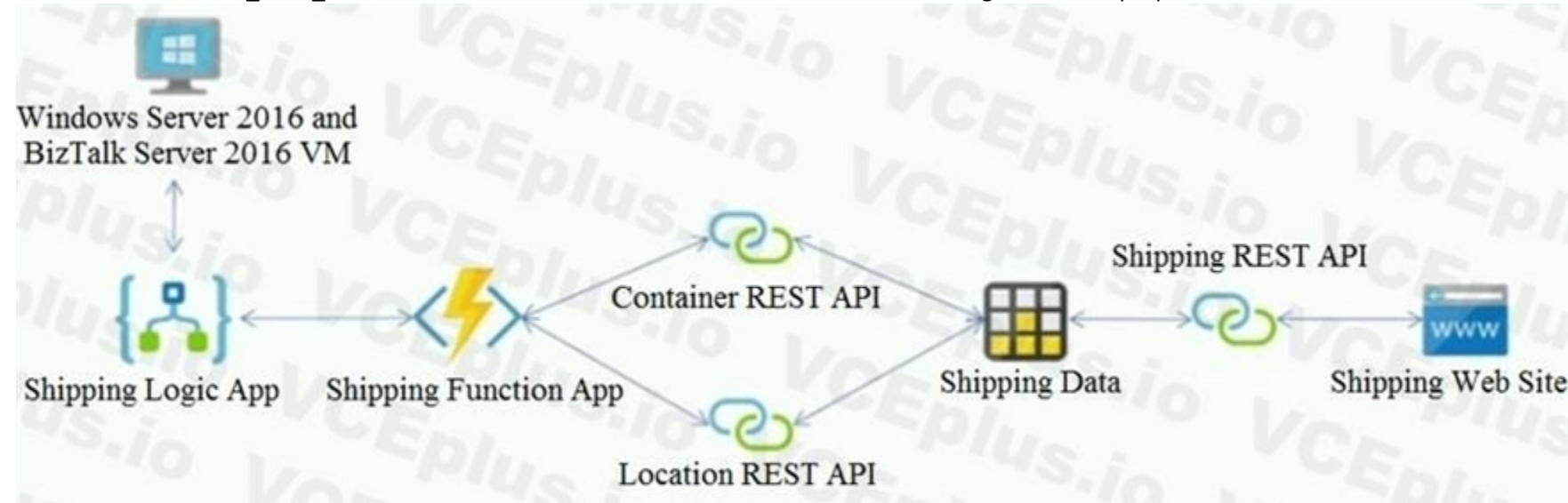
Shipping Web Site

The site displays shipping container tracking information and container contents. The site is located at <http://shipping.wideworldimporters.com/>

Proposed solution

The on-premises shipping application must be moved to Azure. The VM has been migrated to a new Standard_D16s_v3 Azure VM by using Azure Site Recovery and must remain running in Azure to complete the BizTalk component migrations.

You create a Standard_D16s_v3 Azure VM to host BizTalk Server. The Azure architecture diagram for the proposed solution is shown below:



Requirements

Shipping Logic app

The Shipping Logic app must meet the following requirements:

Support the ocean transport and inland transport workflows by using a Logic App.

Support industry-standard protocol X12 message format for various messages including vessel content details and arrival notices.

Secure resources to the corporate VNet and use dedicated storage resources with a fixed costing model.

Maintain on-premises connectivity to support legacy applications and final BizTalk migrations.

Shipping Function app

Implement secure function endpoints by using app-level security and include Azure Active Directory (Azure AD).

REST APIs

The REST API's that support the solution must meet the following requirements:

Secure resources to the corporate VNet.

Allow deployment to a testing location within Azure while not incurring additional costs.

Automatically scale to double capacity during peak shipping times while not causing application downtime.

Minimize costs when selecting an Azure payment model.

Shipping data

Data migration from on-premises to Azure must minimize costs and downtime.

Shipping website

Use Azure Content Delivery Network (CDN) and ensure maximum performance for dynamic content while minimizing latency and costs.

Issues

Windows Server 2016 VM

The VM shows high network latency, jitter, and high CPU utilization. The VM is critical and has not been backed up in the past. The VM must enable a quick restore from a 7-day snapshot to include in-place restore of disks in case of failure.

Shipping website and REST APIs

The following error message displays while you are testing the website:

Failed to load http://test-shippingapi.wideworldimporters.com/: No 'Access-Control-Allow-Origin' header is present on the requested resource. Origin 'http:// test.wideworldimporters.com/' is therefore not allowed access.

QUESTION 1

HOTSPOT

You need to configure Azure CDN for the Shipping web site.

Which configuration options 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

Option

Value

Tier

	▼
Standard	
Premium	

Profile

	▼
Akamai	
Microsoft	

Optimization

	▼
general web delivery	
large file download	
dynamic site acceleration	
video-on-demand media streaming	

Answer Area:

Answer Area

Option	Value
Tier	<div>▼</div> <div>Standard</div> <div>Premium</div>
Profile	<div>▼</div> <div>Akamai</div> <div>Microsoft</div>
Optimization	<div>▼</div> <div>general web delivery</div> <div>large file download</div> <div>dynamic site acceleration</div> <div>video-on-demand media streaming</div>

Section:

Explanation:

Scenario: Shipping website

Use Azure Content Delivery Network (CDN) and ensure maximum performance for dynamic content while minimizing latency and costs.

Tier: Standard

Profile: Akamai

Optimization: Dynamic site acceleration Dynamic site acceleration (DSA) is available for Azure CDN Standard from Akamai, Azure CDN Standard from Verizon, and Azure CDN Premium from Verizon profiles.

DSA includes various techniques that benefit the latency and performance of dynamic content. Techniques include route and network optimization, TCP optimization, and more.

You can use this optimization to accelerate a web app that includes numerous responses that aren't cacheable. Examples are search results, checkout transactions, or real-time data. You can continue to use core Azure CDN caching capabilities for static data.

Reference:

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

QUESTION 2

HOTSPOT

You need to correct the VM issues.

Which tools 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	
Issue	Tool
Backup and Restore	
	Azure Site Recovery
	Azure Backup
	Azure Data Box
	Azure Migrate
Performance	
	Azure Network Watcher
	Azure Traffic Manager
	ExpressRoute
	Accelerated Networking

Answer Area:

Answer Area	
Issue	Tool
Backup and Restore	
	Azure Site Recovery
	Azure Backup
	Azure Data Box
	Azure Migrate
Performance	
	Azure Network Watcher
	Azure Traffic Manager
	ExpressRoute
	Accelerated Networking

Section:

Explanation:

Box 1: Azure Backup The VM is critical and has not been backed up in the past. The VM must enable a quick restore from a 7-day snapshot to include in-place restore of disks in case of failure.

In-Place restore of disks in IaaS VMs is a feature of Azure Backup.

Performance: Accelerated Networking

Scenario: The VM shows high network latency, jitter, and high CPU utilization.

Box 2: Accelerated networking

The VM shows high network latency, jitter, and high CPU utilization.

Accelerated networking enables single root I/O virtualization (SR-IOV) to a VM, greatly improving its networking performance. This high-performance path bypasses the host from the datapath, reducing latency, jitter, and CPU utilization, for use with the most demanding network workloads on supported VM types.

Reference:

<https://azure.microsoft.com/en-us/blog/an-easy-way-to-bring-back-your-azure-vm-with-in-place-restore/>

02 - Develop Azure compute solutions

Case study

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

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

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

To start the case study

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. When you are ready to answer a question, click the Question button to return to the question.

Background

City Power & Light company provides electrical infrastructure monitoring solutions for homes and businesses. The company is migrating solutions to Azure.

Current environment

Architecture overview

The company has a public website located at <http://www.cpandl.com/>. The site is a single-page web application that runs in Azure App Service on Linux. The website uses files stored in Azure Storage and cached in Azure Content Delivery Network (CDN) to serve static content.

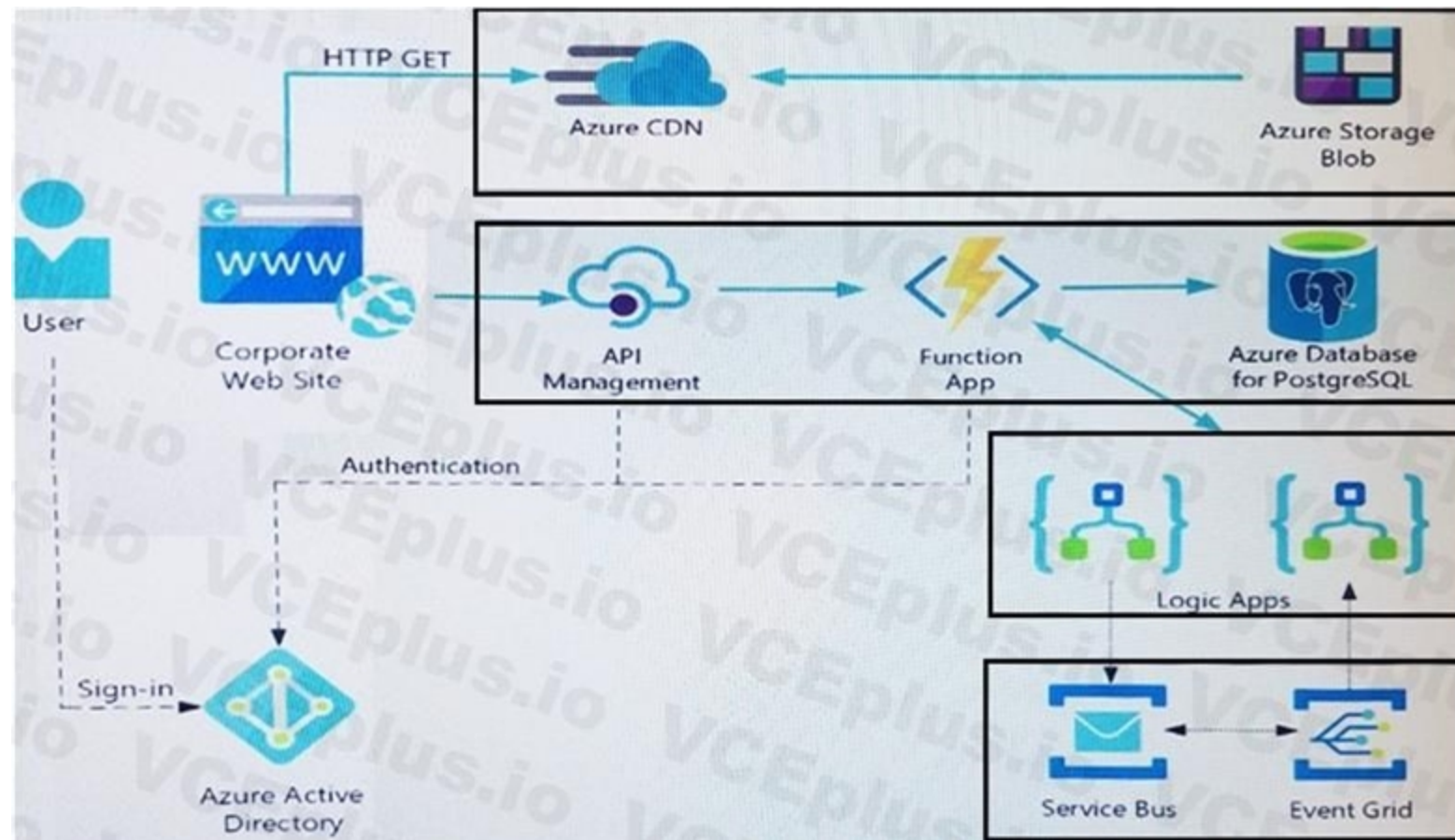
API Management and Azure Function App functions are used to process and store data in Azure Database for PostgreSQL. API Management is used to broker communications to the Azure Function app functions for Logic app integration.

Logic apps are used to orchestrate the data processing while Service Bus and Event Grid handle messaging and events.

The solution uses Application Insights, Azure Monitor, and Azure Key Vault.

Architecture diagram

The company has several applications and services that support their business. The company plans to implement serverless computing where possible. The overall architecture is shown below.



User authentication

The following steps detail the user authentication process:

1. The user selects Sign in in the website.
2. The browser redirects the user to the Azure Active Directory (Azure AD) sign in page.
3. The user signs in.
4. Azure AD redirects the user's session back to the web application. The URL includes an access token.
5. The web application calls an API and includes the access token in the authentication header. The application ID is sent as the audience ('aud') claim in the access token.
6. The back-end API validates the access token.

Requirements

Corporate website

Communications and content must be secured by using SSL.

Communications must use HTTPS.

Data must be replicated to a secondary region and three availability zones.

Data storage costs must be minimized.

Azure Database for PostgreSQL

The database connection string is stored in Azure Key Vault with the following attributes:

Azure Key Vault name: cpandlkeyvault

Secret name: PostgreSQLConn

Id: 80df3e46ffcd4f1cb187f79905e9a1e8

The connection information is updated frequently. The application must always use the latest information to connect to the database.

Azure Service Bus and Azure Event Grid

Azure Event Grid must use Azure Service Bus for queue-based load leveling.

Events in Azure Event Grid must be routed directly to Service Bus queues for use in buffering.

Events from Azure Service Bus and other Azure services must continue to be routed to Azure Event Grid for processing.

Security

All SSL certificates and credentials must be stored in Azure Key Vault.

File access must restrict access by IP, protocol, and Azure AD rights.

All user accounts and processes must receive only those privileges which are essential to perform their intended function.

Compliance

Auditing of the file updates and transfers must be enabled to comply with General Data Protection Regulation (GDPR). The file updates must be read-only, stored in the order in which they occurred, include only create, update, delete, and copy operations, and be retained for compliance reasons.

Issues

Corporate website

While testing the site, the following error message displays:

CryptographicException: The system cannot find the file specified.

Function app

You perform local testing for the RequestUserApproval function. The following error message displays:

'Timeout value of 00:10:00 exceeded by function: RequestUserApproval'

The same error message displays when you test the function in an Azure development environment when you run the following Kusto query:

FunctionAppLogs

| where FunctionName == "RequestUserApproval"

Logic app

You test the Logic app in a development environment. The following error message displays:

'400 Bad Request'

Troubleshooting of the error shows an HttpTrigger action to call the RequestUserApproval function.

Code

Corporate website

Security.cs:

```
SC01 public class Security
SC02 {
SC03     var bytes = System.IO.File.ReadAllBytes("~/var/ssl/private");
SC04     var cert = new System.Security.Cryptography.X509Certificate2(bytes);
SC05     var certName = cert.FriendlyName;
SC06 }
```

Function app

RequestUserApproval.cs:


```

RA01 public static class RequestUserApproval
RA02 {
RA03     [FunctionName("RequestUserApproval")]
RA04     public static async Task<IActionResult> Run(
RA05     [HttpTrigger(AuthorizationLevel.Function, "get", "post", Route = null)] HttpRequest req,
RA06     ILogger log)
RA07     {
RA08         log.LogInformation("RequestUserApproval function processed a request.");
RA09         ...
RA10         return ProcessRequest(req)
RA11         ? (ActionResult)new OkObjectResult($"User approval processed")
RA12         : new BadRequestObjectResult("Failed to process user approval");
RA13     }
RA14     private static bool ProcessRequest(HttpRequest req)
RA15     {
RA16         ...
RA17     }

```

QUESTION 1

You need to correct the RequestUserApproval Function app error.
What should you do?

- A. Update line RA13 to use the async keyword and return an HttpRequest object value.
- B. Configure the Function app to use an App Service hosting plan. Enable the Always On setting of the hosting plan.
- C. Update the function to be stateful by using Durable Functions to process the request payload.
- D. Update the functionTimeout property of the host.json project file to 15 minutes.

Correct Answer: C

Section:

Explanation:

Async operation tracking

The HTTP response mentioned previously is designed to help implement long-running HTTP async APIs with Durable Functions. This pattern is sometimes referred to as the polling consumer pattern.

Both the client and server implementations of this pattern are built into the Durable Functions HTTP APIs.

Function app

You perform local testing for the RequestUserApproval function. The following error message displays:

'Timeout value of 00:10:00 exceeded by function: RequestUserApproval'

The same error message displays when you test the function in an Azure development environment when you run the following Kusto query:

FunctionAppLogs

| where FunctionName == "RequestUserApproval"

References:

<https://docs.microsoft.com/en-us/azure/azure-functions/durable/durable-functions-http-features>

03 - Develop Azure compute solutions

Case study

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

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

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

To start the case study

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. When you are ready to answer a question, click the Question button to return to the question.

Background

You are a developer for Proseware, Inc. You are developing an application that applies a set of governance policies for Proseware's internal services, external services, and applications. The application will also provide a shared library for common functionality.

Requirements

Policy service

You develop and deploy a stateful ASP.NET Core 2.1 web application named Policy service to an Azure App Service Web App. The application reacts to events from Azure Event Grid and performs policy actions based on those events.

The application must include the Event Grid Event ID field in all Application Insights telemetry.

Policy service must use Application Insights to automatically scale with the number of policy actions that it is performing.

Policies

Log policy

All Azure App Service Web Apps must write logs to Azure Blob storage. All log files should be saved to a container named logdrop. Logs must remain in the container for 15 days.

Authentication events

Authentication events are used to monitor users signing in and signing out. All authentication events must be processed by Policy service. Sign outs must be processed as quickly as possible.

PolicyLib

You have a shared library named PolicyLib that contains functionality common to all ASP.NET Core web services and applications. The PolicyLib library must:

Exclude non-user actions from Application Insights telemetry.

Provide methods that allow a web service to scale itself.

Ensure that scaling actions do not disrupt application usage.

Other

Anomaly detection service

You have an anomaly detection service that analyzes log information for anomalies. It is implemented as an Azure Machine Learning model. The model is deployed as a web service. If an anomaly is detected, an Azure Function that emails administrators is called by using an HTTP WebHook.

Health monitoring

All web applications and services have health monitoring at the /health service endpoint.

Issues

Policy loss

When you deploy Policy service, policies may not be applied if they were in the process of being applied during the deployment.

Performance issue

When under heavy load, the anomaly detection service undergoes slowdowns and rejects connections.

Notification latency

Users report that anomaly detection emails can sometimes arrive several minutes after an anomaly is detected.

App code

EventGridController.cs

Relevant portions of the app files are shown below. Line numbers are included for reference only and include a two-character prefix that denotes the specific file to which they belong.

EventGridController.cs

```
EG01 public class EventGridController : Controller
EG02 {
EG03     public static AsyncLocal<string> EventId = new AsyncLocal<string>();
EG04     public IActionResult Process([FromBody] string eventsJson)
EG05     {
EG06         var events = JObject.Parse(eventsJson);
EG07
EG08         foreach (var @event in events)
EG09         {
EG10             EventId.Value = @event["id"].ToString();
EG11             if (@event["topic"].ToString().Contains("providers/Microsoft.Storage"))
EG12             {
EG13                 SendToAnomalyDetectionService(@event["data"]["url"].ToString());
EG14             }
EG15
EG16             {
EG17                 EnsureLogging(@event["subject"].ToString());
EG18             }
EG19         }
EG20         return null;
EG21     }
EG22     private void EnsureLogging(string resource)
EG23     {
EG24         . . .
EG25     }
EG26     private async Task SendToAnomalyDetectionService(string uri)
EG27     {
EG28         var content = GetLogData(uri);
EG29         var scoreRequest = new
EG30         {
EG31             Inputs = new Dictionary<string, List<Dictionary<string, string>>>()
EG32             {
EG33                 {
EG34                     "input1",
EG35                     new List<Dictionary<string, string>>()
EG36                     {
EG37                         new Dictionary<string, string>()
EG38                         {
EG39                             {
EG40                                 "logcontent", content
EG41                             }
EG42                         }
EG43                     }
EG44                 },
EG45             },
EG46             GlobalParameters = new Dictionary<string, string>() { }
EG47         };
EG48         var result = await (new HttpClient()).PostAsJsonAsync("...", scoreRequest);
EG49         var rawModelResult = await result.Content.ReadAsStringAsync();
EG50         var modelResult = JObject.Parse(rawModelResult);
EG51         if (modelResult["notify"].HasValues)
EG52         {
EG53             . . .
EG54         }
EG55     }
```


LoginEvent.cs

Relevant portions of the app files are shown below. Line numbers are included for reference only and include a two-character prefix that denotes the specific file to which they belong.

LoginEvent.cs

```
LE01 public class LoginEvent
LE02 {
LE03
LE04     public string subject { get; set; }
LE05     public DateTime eventTime { get; set; }
LE06     public Dictionary<string, string> data { get; set; }
LE07     public string Serialize()
LE08     {
LE09         return JsonConvert.SerializeObject(this);
LE10     }
LE11 }
```

QUESTION 1

You need to resolve a notification latency issue.

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

NOTE: Each correct selection is worth one point.

- A. Set Always On to true.
- B. Ensure that the Azure Function is using an App Service plan.
- C. Set Always On to false.
- D. Ensure that the Azure Function is set to use a consumption plan.

Correct Answer: A, B

Section:

Explanation:

Azure Functions can run on either a Consumption Plan or a dedicated App Service Plan. If you run in a dedicated mode, you need to turn on the Always On setting for your Function App to run properly. The Function runtime will go idle after a few minutes of inactivity, so only HTTP triggers will actually "wake up" your functions. This is similar to how WebJobs must have Always On enabled.

Scenario: Notification latency: Users report that anomaly detection emails can sometimes arrive several minutes after an anomaly is detected.

Anomaly detection service: You have an anomaly detection service that analyzes log information for anomalies. It is implemented as an Azure Machine Learning model. The model is deployed as a web service.

If an anomaly is detected, an Azure Function that emails administrators is called by using an HTTP WebHook.

Reference:

<https://github.com/Azure/Azure-Functions/wiki/Enable-Always-On-when-running-on-dedicated-App-Service-Plan>

01 - Develop for Azure storage

Case study

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

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

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

To start the case study

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. When you are ready to answer a question, click the Question button to return to the question.

Background

Overview

You are a developer for Contoso, Ltd. The company has a social networking website that is developed as a Single Page Application (SPA). The main web application for the social networking website loads user uploaded content from blob storage.

You are developing a solution to monitor uploaded data for inappropriate content. The following process occurs when users upload content by using the SPA:

- Messages are sent to ContentUploadService.
- Content is processed by ContentAnalysisService.
- After processing is complete, the content is posted to the social network or a rejection message is posted in its place.

The ContentAnalysisService is deployed with Azure Container Instances from a private Azure Container Registry named contosoimages.

The solution will use eight CPU cores.

Azure Active Directory

Contoso, Ltd. uses Azure Active Directory (Azure AD) for both internal and guest accounts.

Requirements

ContentAnalysisService

The company's data science group built ContentAnalysisService which accepts user generated content as a string and returns a probable value for inappropriate content. Any values over a specific threshold must be reviewed by an employee of Contoso, Ltd.

You must create an Azure Function named CheckUserContent to perform the content checks.

Costs

You must minimize costs for all Azure services.

Manual review

To review content, the user must authenticate to the website portion of the ContentAnalysisService using their Azure AD credentials. The website is built using React and all pages and API endpoints require authentication. In order to review content a user must be part of a ContentReviewer role. All completed reviews must include the reviewer's email address for auditing purposes.

High availability

All services must run in multiple regions. The failure of any service in a region must not impact overall application availability.

Monitoring

An alert must be raised if the ContentUploadService uses more than 80 percent of available CPU cores.

Security

You have the following security requirements:

Any web service accessible over the Internet must be protected from cross site scripting attacks.

All websites and services must use SSL from a valid root certificate authority.

Azure Storage access keys must only be stored in memory and must be available only to the service.

All Internal services must only be accessible from internal Virtual Networks (VNets).

All parts of the system must support inbound and outbound traffic restrictions.

All service calls must be authenticated by using Azure AD.

User agreements

When a user submits content, they must agree to a user agreement. The agreement allows employees of Contoso, Ltd. to review content, store cookies on user devices, and track user's IP addresses.

Information regarding agreements is used by multiple divisions within Contoso, Ltd.

User responses must not be lost and must be available to all parties regardless of individual service uptime. The volume of agreements is expected to be in the millions per hour.

Validation testing

When a new version of the ContentAnalysisService is available the previous seven days of content must be processed with the new version to verify that the new version does not significantly deviate from the old version.

Issues

Users of the ContentUploadService report that they occasionally see HTTP 502 responses on specific pages.

Code

ContentUploadService

```
CS01 apiVersion: '2018-10-01'
CS02 type: Microsoft.ContainerInstance/containerGroups
CS03 location: westus
CS04 name: contentUploadService
CS05 properties:
CS06   containers:
CS07   - name: service
CS08     properties:
CS09       image: contoso/contentUploadService:latest
CS10       ports:
CS11       - port: 80
CS12         protocol: TCP
CS13     resources:
CS14       requests:
CS15         cpu: 1.0
CS16         memoryInGB: 1.5
CS17
CS18 ipAddress:
CS19   ip: 10.23.121.112
CS20   ports:
CS21   - port: 80
CS22     protocol: TCP
CS23
CS24
CS25 networkProfile:
CS26
id: /subscriptions/98...19/resourceGroups/container/providers/Microsoft.Network/networkProfiles/subnet
```

```

AM01 {
AM02     "id" : "2b079f03-9b06-2d44-98bb-e9182901fcb6",
AM03     "appId" : "7118a7f0-b5c2-4c9d-833c-3d711396fe65",
AM04
AM05     "createdDateTime" : "2019-12-24T06:01:44Z",
AM06     "logoUrl" : null,
AM07     "logoutUrl" : null,
AM08     "name" : "ContentAnalysisService",
AM09
AM10
AM11     "orgRestrictions" : [],
AM12     "parentalControlSettings" : {
AM13         "countriesBlockedForMinors" : [],
AM14         "legalAgeGroupRule" : "Allow"
AM15     },
AM16     "passwordCredentials" : []
AM17 }

```

QUESTION 1

You need to configure the ContentUploadService deployment.

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

NOTE: Each correct selection is worth one point.

- A. Add the following markup to line CS23:
type: Private
- B. Add the following markup to line CS24:
osType: Windows
- C. Add the following markup to line CS24:
osType: Linux
- D. Add the following markup to line CS23:
type: Public

Correct Answer: A, C

Section:

Explanation:

Scenario: All Internal services must only be accessible from Internal Virtual Networks (VNETs)

There are three Network Location types - Private, Public and Domain

Reference: <https://devblogs.microsoft.com/powershell/setting-network-location-to-private/>

QUESTION 2

You need to store the user agreements.

Where should you store the agreement after it is completed?

- A. Azure Storage queue

- B. Azure Event Hub
- C. Azure Service Bus topic
- D. Azure Event Grid topic

Correct Answer: B

Section:

Explanation:

Azure Event Hub is used for telemetry and distributed data streaming. This service provides a single solution that enables rapid data retrieval for real-time processing as well as repeated replay of stored raw data. It can capture the streaming data into a file for processing and analysis. It has the following characteristics: low latency capable of receiving and processing millions of events per second at least once delivery
Reference: <https://docs.microsoft.com/en-us/azure/event-grid/compare-messaging-services>

QUESTION 3

HOTSPOT

You need to implement the bindings for the CheckUserContent function.
How should you complete the code segment? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

```
public static class CheckUserContent
{
    [FunctionName("CheckUserContent")]
    public static void Run(

```

▼ string content,

[QueueTrigger("userContent")]

[BlobTrigger("userContent/{name}")]

[CosmosDBTrigger("content", "userContent")]

[Table("content", "userContent", "{name}")]

▼ Stream output)

[Queue("userContent")]

[CosmosDB("content", "userContent")]

[Table("content", "userContent", "{name}")]

[Blob("userContent/{name}", FileAccess.Write)]

```
    {
        ...
    }
}
```

Answer Area:

Answer Area

```
public static class CheckUserContent
{
    [FunctionName("CheckUserContent")]
    public static void Run(
        string content,
        [QueueTrigger("userContent")]
        [BlobTrigger("userContent/{name}")]
        [CosmosDBTrigger("content", "userContent")]
        [Table("content", "userContent", "{name}")]
        Stream output)
    {
        ...
    }
}
```

Section:

Explanation:

Box 1: [BlobTrigger(..)]

Box 2: [Blob(..)]

Azure Blob storage output binding for Azure Functions. The output binding allows you to modify and delete blob storage data in an Azure Function.

The attribute's constructor takes the path to the blob and a FileAccess parameter indicating read or write, as shown in the following example:

```
[FunctionName("ResizeImage")]
public static void Run(
    [BlobTrigger("sample-images/{name}")] Stream image,
    [Blob("sample-images-md/{name}", FileAccess.Write)] Stream imageSmall)
{
    ...
}
```

Scenario: You must create an Azure Function named CheckUserContent to perform the content checks.

The company's data science group built ContentAnalysisService which accepts user generated content as a string and returns a probable value for inappropriate content. Any values over a specific threshold must be reviewed by an employee of Contoso, Ltd.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-functions/functions-bindings-storage-blob-output>

02 - Develop for Azure storage

Case study

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage

your time to ensure that you are able to complete all questions included on this exam in the time provided.

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

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

To start the case study

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. When you are ready to answer a question, click the Question button to return to the question.

Background

City Power & Light company provides electrical infrastructure monitoring solutions for homes and businesses. The company is migrating solutions to Azure.

Current environment

Architecture overview

The company has a public website located at <http://www.cpandl.com/>. The site is a single-page web application that runs in Azure App Service on Linux. The website uses files stored in Azure Storage and cached in Azure Content Delivery Network (CDN) to serve static content.

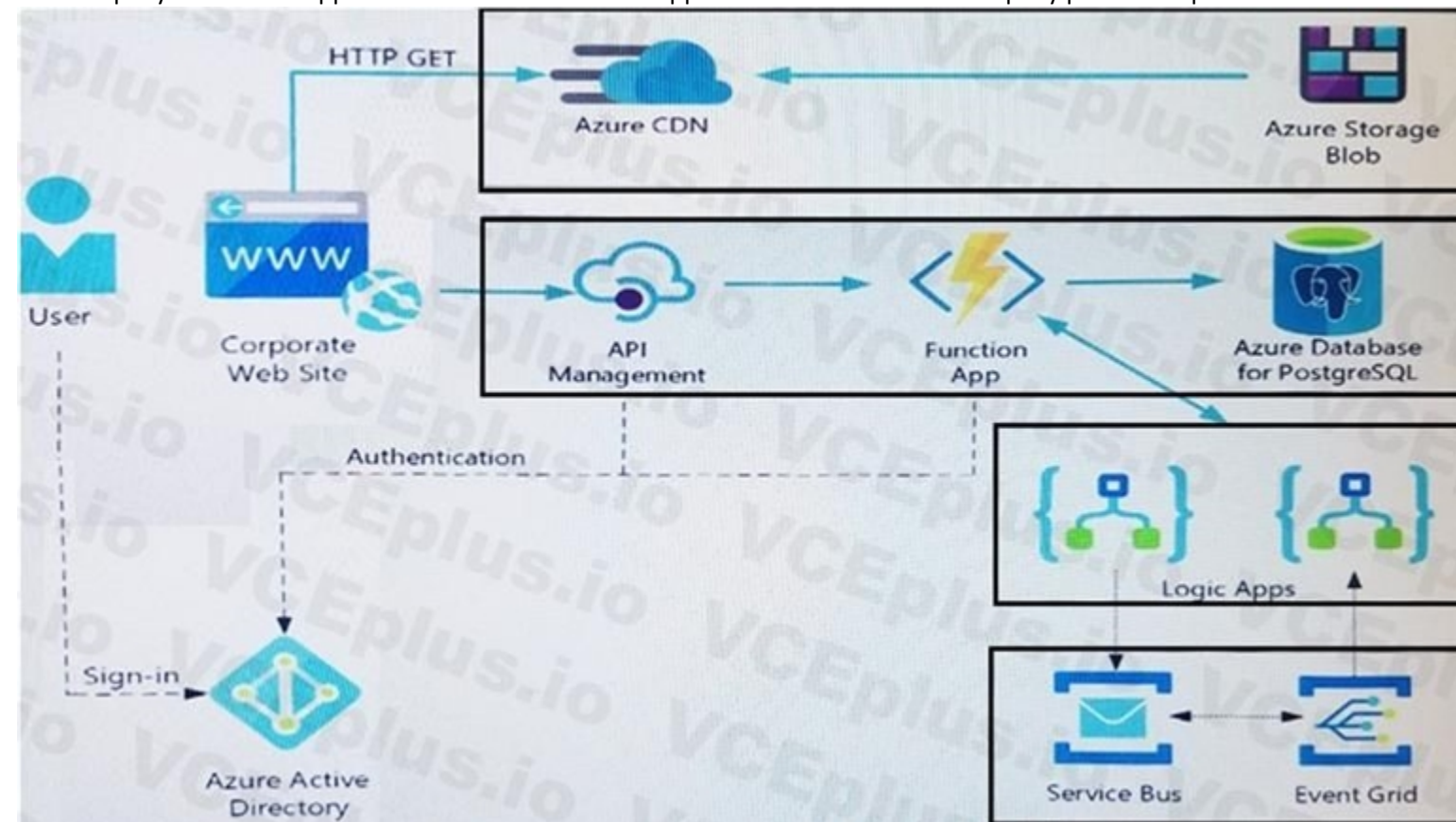
API Management and Azure Function App functions are used to process and store data in Azure Database for PostgreSQL. API Management is used to broker communications to the Azure Function app functions for Logic app integration.

Logic apps are used to orchestrate the data processing while Service Bus and Event Grid handle messaging and events.

The solution uses Application Insights, Azure Monitor, and Azure Key Vault.

Architecture diagram

The company has several applications and services that support their business. The company plans to implement serverless computing where possible. The overall architecture is shown below.



User authentication

The following steps detail the user authentication process:

The user selects Sign in in the website.

The browser redirects the user to the Azure Active Directory (Azure AD) sign in page.

The user signs in.

Azure AD redirects the user's session back to the web application. The URL includes an access token.

The web application calls an API and includes the access token in the authentication header. The application ID is sent as the audience ('aud') claim in the access token.

The back-end API validates the access token.

Requirements

Corporate website

Communications and content must be secured by using SSL.

Communications must use HTTPS.

Data must be replicated to a secondary region and three availability zones.

Data storage costs must be minimized.

Azure Database for PostgreSQL

The database connection string is stored in Azure Key Vault with the following attributes:

Azure Key Vault name: cpandlkeyvault

Secret name: PostgreSQLConn

Id: 80df3e46ffcd4f1cb187f79905e9a1e8

The connection information is updated frequently. The application must always use the latest information to connect to the database.

Azure Service Bus and Azure Event Grid

Azure Event Grid must use Azure Service Bus for queue-based load leveling.

Events in Azure Event Grid must be routed directly to Service Bus queues for use in buffering.

Events from Azure Service Bus and other Azure services must continue to be routed to Azure Event Grid for processing.

Security

All SSL certificates and credentials must be stored in Azure Key Vault.

File access must restrict access by IP, protocol, and Azure AD rights.

All user accounts and processes must receive only those privileges which are essential to perform their intended function.

Compliance

Auditing of the file updates and transfers must be enabled to comply with General Data Protection Regulation (GDPR). The file updates must be read-only, stored in the order in which they occurred, include only create, update, delete, and copy operations, and be retained for compliance reasons.

Issues

Corporate website

While testing the site, the following error message displays:

CryptographicException: The system cannot find the file specified.

Function app

You perform local testing for the RequestUserApproval function. The following error message displays:

'Timeout value of 00:10:00 exceeded by function: RequestUserApproval'

The same error message displays when you test the function in an Azure development environment when you run the following Kusto query:

FunctionAppLogs

| where FunctionName == "RequestUserApproval"

Logic app

You test the Logic app in a development environment. The following error message displays:

'400 Bad Request'

Troubleshooting of the error shows an HttpTrigger action to call the RequestUserApproval function.

Code

Corporate website

Security.cs:

```
SC01 public class Security
SC02 {
SC03     var bytes = System.IO.File.ReadAllBytes("~/var/ssl/private");
SC04     var cert = new System.Security.Cryptography.X509Certificate2(bytes);
SC05     var certName = cert.FriendlyName;
SC06 }
```

Function app

RequestUserApproval.cs:


```
RA01 public static class RequestUserApproval
RA02 {
RA03     [FunctionName("RequestUserApproval")]
RA04     public static async Task<IActionResult> Run(
RA05     [HttpTrigger(AuthorizationLevel.Function, "get", "post", Route = null)] HttpRequest req,
RA06     ILogger log)
RA07     {
RA08         log.LogInformation("RequestUserApproval function processed a request.");
RA09         ...
RA10         return ProcessRequest(req)
RA11             ? (ActionResult)new OkObjectResult($"User approval processed")
RA12             : new BadRequestObjectResult("Failed to process user approval");
RA13     }
RA14     private static bool ProcessRequest(HttpRequest req)
RA15     {
RA16         ...
RA17     }
```

QUESTION 1

HOTSPOT

You need to configure the Account Kind, Replication, and Storage tier options for the corporate website's Azure Storage account.

How should you complete the configuration? To answer, select the appropriate options in the dialog box in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Create storage account



Basics Advanced Tags Review + create

Azure Storage is a Microsoft-managed service providing cloud storage that is highly available, secure, durable, scalable, and redundant. Azure Storage includes Azure Blobs (objects), Azure Data Lake Storage Gen2, Azure Files, Azure Queues, and Azure Tables. The cost of your storage account depends on the usage and the options you choose below. [Learn more](#)

PROJECT DETAILS

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

* Subscription

Visual Studio Enterprise



* Resource group

(New) cplcorporatesite



[Create new](#)

INSTANCE DETAILS

The default deployment model is Resource Manager, which supports the latest Azure features. You may choose to deploy using the classic deployment model instead. [Choose classic deployment model](#)

* Storage account name ⓘ

corporatewebsitecontent



* Location

(US) East US



Performance ⓘ

☒ Standard ☐ Premium

Account kind ⓘ

StorageV2 (general purpose v2)
Storage (general purpose v1)
BlobStorage



Replication ⓘ

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



Access tier (default) ⓘ

☐ Cool ☐ Hot

Answer Area:

Create storage account



Basics [Advanced](#) [Tags](#) [Review + create](#)

Azure Storage is a Microsoft-managed service providing cloud storage that is highly available, secure, durable, scalable, and redundant. Azure Storage includes Azure Blobs (objects), Azure Data Lake Storage Gen2, Azure Files, Azure Queues, and Azure Tables. The cost of your storage account depends on the usage and the options you choose below. [Learn more](#)

PROJECT DETAILS

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

* Subscription

Visual Studio Enterprise



* Resource group

(New) cplcorporatesite



[Create new](#)

INSTANCE DETAILS

The default deployment model is Resource Manager, which supports the latest Azure features. You may choose to deploy using the classic deployment model instead. [Choose classic deployment model](#)

* Storage account name ⓘ

corporatewebsitecontent



* Location

(US) East US



Performance ⓘ

☒ Standard ☐ Premium

Account kind ⓘ

StorageV2 (general purpose v2)
Storage (general purpose v1)
BlobStorage



Replication ⓘ

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



Access tier (default) ⓘ

☒ Cool ☐ Hot

Section:**Explanation:**

Account Kind: StorageV2 (general-purpose v2)

Scenario: Azure Storage blob will be used (refer to the exhibit). Data storage costs must be minimized.

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

Incorrect Answers:

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

General-purpose v1 accounts: Legacy account type for blobs, files, queues, and tables. Use general-purpose v2 accounts instead when possible.

Replication: Geo-redundant Storage

Scenario: Data must be replicated to a secondary region and three availability zones.

Geo-redundant storage (GRS) copies your data synchronously three times within a single physical location in the primary region using LRS. It then copies your data asynchronously to a single physical location in the secondary region.

Incorrect Answers:

Geo-zone-redundant storage (GZRS), but it would be more costly.

Storage tier: Cool

Data storage costs must be minimized.

Note: Azure storage offers different access tiers, which allow you to store blob object data in the most cost-effective manner. The available access tiers include:

Hot - Optimized for storing data that is accessed frequently.

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

Reference:

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

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

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

03 - Develop for Azure storage**Case study**

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

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

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

To start the case study

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. When you are ready to answer a question, click the Question button to return to the question.

Background

You are a developer for Litware Inc., a SaaS company that provides a solution for managing employee expenses. The solution consists of an ASP.NET Core Web API project that is deployed as an Azure Web App.

Overall architecture

Employees upload receipts for the system to process. When processing is complete, the employee receives a summary report email that details the processing results. Employees then use a web application to manage their receipts and perform any additional tasks needed for reimbursement.

Receipt processing

Employees may upload receipts in two ways:

Uploading using an Azure Files mounted folder

Uploading using the web application

Data Storage

Receipt and employee information is stored in an Azure SQL database.

Documentation

Employees are provided with a getting started document when they first use the solution. The documentation includes details on supported operating systems for Azure File upload, and instructions on how to configure the mounted folder.

Solution details

Users table

Column	Description
UserId	unique identifier for and employee
ExpenseAccount	employees expense account number in the format 1234-123-1234
AllowedAmount	limit of allowed expenses before approval is needed
SupervisorId	unique identifier for employee's supervisor
SecurityPin	value used to validate user identity

Web Application

You enable MSI for the Web App and configure the Web App to use the security principal name WebAppIdentity.

Processing

Processing is performed by an Azure Function that uses version 2 of the Azure Function runtime. Once processing is completed, results are stored in Azure Blob Storage and an Azure SQL database. Then, an email summary is sent to the user with a link to the processing report. The link to the report must remain valid if the email is forwarded to another user.

Logging

Azure Application Insights is used for telemetry and logging in both the processor and the web application. The processor also has TraceWriter logging enabled. Application Insights must always contain all log messages.

Requirements

Receipt processing

Concurrent processing of a receipt must be prevented.

Disaster recovery

Regional outage must not impact application availability. All DR operations must not be dependent on application running and must ensure that data in the DR region is up to date.

Security

User's SecurityPin must be stored in such a way that access to the database does not allow the viewing of SecurityPins. The web application is the only system that should have access to SecurityPins.

All certificates and secrets used to secure data must be stored in Azure Key Vault.

You must adhere to the principle of least privilege and provide privileges which are essential to perform the intended function.

All access to Azure Storage and Azure SQL database must use the application's Managed Service Identity (MSI).

Receipt data must always be encrypted at rest.

All data must be protected in transit.

User's expense account number must be visible only to logged in users. All other views of the expense account number should include only the last segment, with the remaining parts obscured.

In the case of a security breach, access to all summary reports must be revoked without impacting other parts of the system.

Issues

Upload format issue

Employees occasionally report an issue with uploading a receipt using the web application. They report that when they upload a receipt using the Azure File Share, the receipt does not appear in their profile. When this occurs, they delete the file in the file share and use the web application, which returns a 500 Internal Server error page.

Capacity issue

During busy periods, employees report long delays between the time they upload the receipt and when it appears in the web application.

Log capacity issue

Developers report that the number of log messages in the trace output for the processor is too high, resulting in lost log messages.

Application code

Processing.cs


```

PC01 public static class Processing
PC02 {
PC03     public static class Function
PC04     {
PC05         [FunctionName("IssueWork")]
PC06         public static async Task Run([TimerTrigger("0 */5 * * * *")] TimerInfo timer, ILogger
log)
PC07         {
PC08             var container = await GetCloudBlobContainer();
PC09             foreach (var fileItem in await ListFiles())
PC10             {
PC11                 var file = new CloudFile(fileItem.StorageUri.PrimaryUri);
PC12                 var ms = new MemoryStream();
PC13                 await file.DownloadToStreamAsync(ms);
PC14                 var blob = container.GetBlockBlobReference(fileItem.Uri.ToString());
PC15                 await blob.UploadFromStreamAsync(ms);
PC16             }
PC17         }
PC18     }
PC19     private static CloudBlockBlob GetDRBlob(CloudBlockBlob sourceBlob)
PC20     {
PC21         . . .
PC22     }
PC23     private static async Task<CloudBlobContainer> GetCloudBlobContainer()
PC24     {
PC25         var cloudBlobClient = new CloudBlobClient(new Uri(". . ."), await GetCredentials());
PC26
PC27         await cloudBlobClient.GetRootContainerReference().CreateIfNotExistsAsync();
PC28         return cloudBlobClient.GetRootContainerReference();
PC29     }
PC30     private static async Task<StorageCredentials> GetCredentials()
PC31     {
PC32         . . .
PC33     }
PC34     private static async Task<List<IListFileItem>> ListFiles()
PC35     {
PC36         . . .
PC37     }
PC37     private KeyVaultClient _keyVaultClient = new KeyVaultClient(". . .");
PC38 }
PC39 }

```

```

DB01 public class Database
DB02 {
DB03     private string ConnectionString =
DB04
DB05     public async Task<object> LoadUserDetails(string userId)
DB06     {
DB07
DB08         return await policy.ExecuteAsync(async () =>
DB09         {
DB10             using (var connection = new SqlConnection(ConnectionString))
DB11             {
DB12                 await connection.OpenAsync();
DB13                 using (var command = new SqlCommand("...", connection))
DB14                 using (var reader = command.ExecuteReader())
DB15                 {
DB16                     ...
DB17                 }
DB18             }
DB19         });
DB20     }
DB21 }

```

ReceiptUploader.cs

```

RU01 public class ReceiptUploader
RU02 {
RU03     public async Task UploadFile(string file, byte[] binary)
RU04     {
RU05         var httpClient = new HttpClient();
RU06         var response = await httpClient.PutAsync("...", new ByteArrayContent(binary));
RU07         while (ShouldRetry(response))
RU08         {
RU09             response = await httpClient.PutAsync("...", new ByteArrayContent(binary));
RU10         }
RU11     }
RU12     private bool ShouldRetry(HttpResponseMessage response)
RU13     {
RU14
RU15     }
RU16 }

```

ConfigureSSE.ps1


```

CS01 $storageAccount = Get-AzureRmStorageAccount -ResourceGroupName "..." -AccountName "..."
CS02 $keyVault = Get-AzureRmKeyVault -VaultName "..."
CS03 $key = Get-AzureKeyVaultKey -VaultName $keyVault.VaultName -Name "..."
CS04 Set-AzureRmKeyVaultAccessPolicy `
CS05   -VaultName $keyVault.VaultName `
CS06   -ObjectId $storageAccount.Identity.PrincipalId `
CS07
CS08
CS09 Set-AzureRmStorageAccount `
CS10   -ResourceGroupName $storageAccount.ResourceGroupName `
CS11   -AccountName $storageAccount.StorageAccountName `
CS12   -EnableEncryptionService File `
CS13   -KeyvaultEncryption `
CS14   -KeyName $key.Name
CS15   -KeyVersion $key.Version `
CS16   -KeyVaultUri $keyVault.VaultUri

```

QUESTION 1

DRAG DROP

You need to add code at line PC32 in Processing.cs to implement the GetCredentials method in the Processing class.

How should you complete the code? To answer, drag the appropriate code segments to the correct locations. Each code segment 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:

Code segments

MSITokenProvider("...", null)

tp.GetAccessTokenAsync("...")

AzureServiceTokenProvider()

StringTokenProvider("storage", "msi")

tp.GetAuthenticationHeaderAsync(CancellationTokens.None)

Answer Area

```

var tp = new code segment
var t = new TokenCredential(await code segment );
return new StorageCredentials(t);

```

Correct Answer:

Code segments

MSITokenProvider("...", null)

StringTokenProvider("storage", "msi")

tp.GetAuthenticationHeaderAsync(CancellationToken.None)

Answer Area

var tp = new AzureServiceTokenProvider()

var t = new TokenCredential(await tp.GetAccessTokenAsync("..."))

return new StorageCredentials(t);

Section:

Explanation:

Box 1: AzureServiceTokenProvider()

Box 2: tp.GetAccessTokenAsync("...")

Acquiring an access token is then quite easy. Example code:

```
private async Task<string> GetAccessTokenAsync()
```

```
{
```

```
var tokenProvider = new AzureServiceTokenProvider();
```

```
return await tokenProvider.GetAccessTokenAsync("https://storage.azure.com/");
```

```
}
```

Reference:

<https://joonasw.net/view/azure-ad-authentication-with-azure-storage-and-managed-service-identity>

QUESTION 2

DRAG DROP

You need to ensure disaster recovery requirements are met.

What code should you add at line PC16?

To answer, drag the appropriate code fragments to the correct locations. Each code fragment 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:

Values

true

SingleTransferContext

ShouldTransferCallbackAsync

false

DirectoryTransferContext

ShouldOverwriteCallbackAsync

Answer Area

```
var copyOptions = new CopyOptions { };  
var context = new Value = (source, destination) => Task.FromResult(true);  
context. Value = (source, destination) => Task.FromResult(true);  
await TransferManager.CopyAsync(blob, GetDRBlob(blob), isServiceCopy: Value  
, context: context, options:copyOptions);
```

Correct Answer:

Values

true

SingleTransferContext

ShouldOverwriteCallbackAsync

Answer Area

```
var copyOptions = new CopyOptions { };  
var context = new DirectoryTransferContext = (source, destination) => Task.FromResult(true);  
context. ShouldTransferCallbackAsync = (source, destination) => Task.FromResult(true);  
await TransferManager.CopyAsync(blob, GetDRBlob(blob), isServiceCopy: false  
, context: context, options:copyOptions);
```

Section:**Explanation:**

Scenario: Disaster recovery. Regional outage must not impact application availability. All DR operations must not be dependent on application running and must ensure that data in the DR region is up to date.

Box 1: DirectoryTransferContext

We transfer all files in the directory.

Note: The TransferContext object comes in two forms: SingleTransferContext and DirectoryTransferContext. The former is for transferring a single file and the latter is for transferring a directory of files.

Box 2: ShouldTransferCallbackAsync

The DirectoryTransferContext.ShouldTransferCallbackAsync delegate callback is invoked to tell whether a transfer should be done.

Box 3: False

If you want to use the retry policy in Copy, and want the copy can be resume if break in the middle, you can use SyncCopy (isServiceCopy = false).

Note that if you choose to use service side copy ('isServiceCopy' set to true), Azure (currently) doesn't provide SLA for that. Setting 'isServiceCopy' to false will download the source blob locally.

Reference:

<https://docs.microsoft.com/en-us/azure/storage/common/storage-use-data-movement-library>

<https://docs.microsoft.com/en-us/dotnet/api/microsoft.windowsazure.storage.datamovement.directorytransfercontext.shouldtransfercallbackasync?view=azure-dotnet>

04 - Develop for Azure storage

Case study

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

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

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

To start the case study

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. When you are ready to answer a question, click the Question button to return to the question.

LabelMaker app

Coho Winery produces, bottles, and distributes a variety of wines globally. You are a developer implementing highly scalable and resilient applications to support online order processing by using Azure solutions.

Coho Winery has a LabelMaker application that prints labels for wine bottles. The application sends data to several printers. The application consists of five modules that run independently on virtual machines (VMs). Coho

Winery plans to move the application to Azure and continue to support label creation.

External partners send data to the LabelMaker application to include artwork and text for custom label designs.

Requirements. Data

You identify the following requirements for data management and manipulation:

Order data is stored as nonrelational JSON and must be queried using SQL.

Changes to the Order data must reflect immediately across all partitions. All reads to the Order data must fetch the most recent writes.

Requirements. Security

You have the following security requirements:

Users of Coho Winery applications must be able to provide access to documents, resources, and applications to external partners.

External partners must use their own credentials and authenticate with their organization's identity management solution.

External partner logins must be audited monthly for application use by a user account administrator to maintain company compliance.

Storage of e-commerce application settings must be maintained in Azure Key Vault.

E-commerce application sign-ins must be secured by using Azure App Service authentication and Azure Active Directory (AAD).

Conditional access policies must be applied at the application level to protect company content.

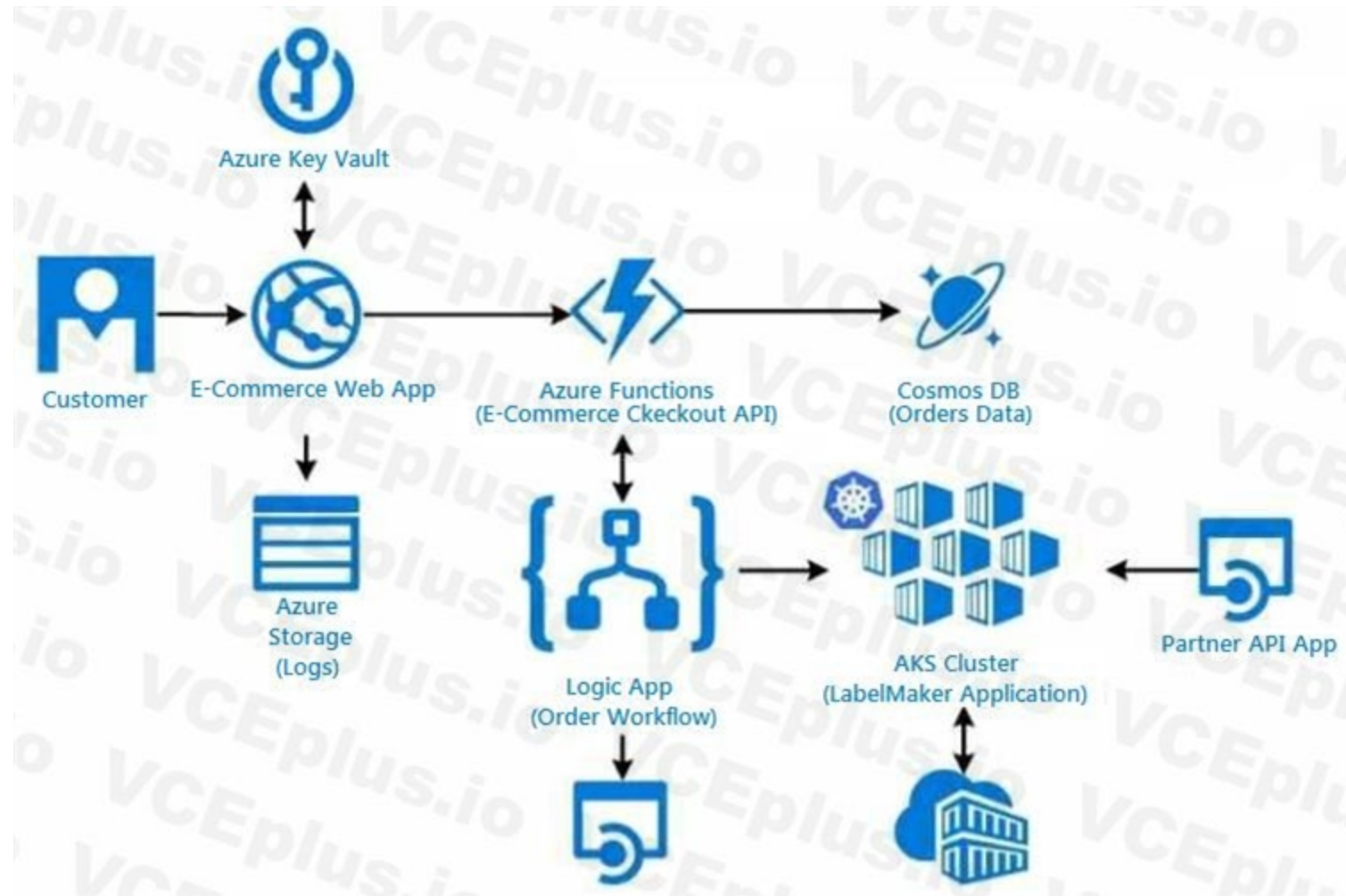
The LabelMaker application must be secured by using an AAD account that has full access to all namespaces of the Azure Kubernetes Service (AKS) cluster.

Requirements. LabelMaker app

Azure Monitor Container Health must be used to monitor the performance of workloads that are deployed to Kubernetes environments and hosted on Azure Kubernetes Service (AKS).

You must use Azure Container Registry to publish images that support the AKS deployment.

Architecture



Issues

Calls to the Printer API App fail periodically due to printer communication timeouts.

Printer communication timeouts occur after 10 seconds. The label printer must only receive up to 5 attempts within one minute.

The order workflow fails to run upon initial deployment to Azure.

Order.json

Relevant portions of the app files are shown below. Line numbers are included for reference only.

This JSON file contains a representation of the data for an order that includes a single item.

Order.json


```

01 {
02   "id" : 1,
03   "customers" : [
04     {
05       "familyName" : "Doe",
06       "givenName" : "John",
07       "customerid" : 5
08     }
09   ],
10   "line_items" : [
11     {
12       "fulfillable_quantity" : 1,
13       "id" : 6,
14       "price" : "199.99",
15       "product_id" : 7513594,
16       "quantity": 1,
17       "requires_shipping" : true ,
18       "sku" : "SFC-342-N" ,
19       "title": "Surface Go" ,
20       "vendor" : "Microsoft" ,
21       "name" : "Surface Go - 8GB" ,
22       "taxable" : true ,
23       "tax_lines" : [
24         {
25           "title" : "State Tax" ,
26           "price" : "3.98" ,
27           "rate" : 0.06
28         }
29       ],
30       "total_discount" : "5.00" ,
31       "discount_allocations" : [
32         {
33           "amount" : "5.00" ,
34           "discount_application_index" : 2
35         }
36       ]
37     }
38   ],
39   "address" : {
40     "state" : "NY" ,
41     "state": "Manhattan" ,
42     "city" : "NY"
43   }
44 }

```

QUESTION 1

HOTSPOT

You need to configure Azure Cosmos DB.

Which settings 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

Setting	Value
Consistency Level	<div><div></div><div>Strong</div><div>Bounded-staleness</div><div>Session</div><div>Eventual</div></div>
API	<div><div></div><div>SQL</div><div>MongoDB</div><div>Graph</div><div>Table</div></div>

Answer Area:

Answer Area

Setting	Value
Consistency Level	<div>▼ Strong Bounded-staleness Session Eventual</div>
API	<div>▼ SQL MongoDB Graph Table</div>

Section:

Explanation:

Box 1: Strong

When the consistency level is set to strong, the staleness window is equivalent to zero, and the clients are guaranteed to read the latest committed value of the write operation.

Scenario: Changes to the Order data must reflect immediately across all partitions. All reads to the Order data must fetch the most recent writes.

Note: You can choose from five well-defined models on the consistency spectrum. From strongest to weakest, the models are: Strong, Bounded staleness, Session, Consistent prefix, Eventual

Box 2: SQL

Scenario: You identify the following requirements for data management and manipulation:

Order data is stored as nonrelational JSON and must be queried using Structured Query Language (SQL).

QUESTION 2

HOTSPOT

You need to retrieve all order line items from Order.json and sort the data alphabetically by the city.

How should you complete the code? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

SELECT li.id AS lineitemid, li.price

FROM

Orders o
LineItems li

JOIN

li
o

IN

o.line_items
li.line_items
o.address

ORDER BY

o.address.city
li.address.city
o.city
li.city

ASC

Answer Area:

Answer Area

SELECT li.id AS lineitemid, li.price

FROM

Orders o
LinItems li

JOIN

li
o

IN

o.line_items
li.line_items
o.address

ORDER BY

o.address.city
li.address.city
o.city
li.city

ASC

Section:

Explanation:

Box 1: orders o

Scenario: Order data is stored as nonrelational JSON and must be queried using SQL.

Box 2:li

Box 3: o.line_items

Box 4: o.city

The city field is in Order, not in the 2s.

03 - Implement Azure security

Case study

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

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

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

To start the case study

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. When you are ready to answer a question, click the Question button to return to the question.

Background

City Power & Light company provides electrical infrastructure monitoring solutions for homes and businesses. The company is migrating solutions to Azure.

Current environment

Architecture overview

The company has a public website located at <http://www.cpandl.com/>. The site is a single-page web application that runs in Azure App Service on Linux. The website uses files stored in Azure Storage and cached in Azure Content Delivery

Network (CDN) to serve static content.

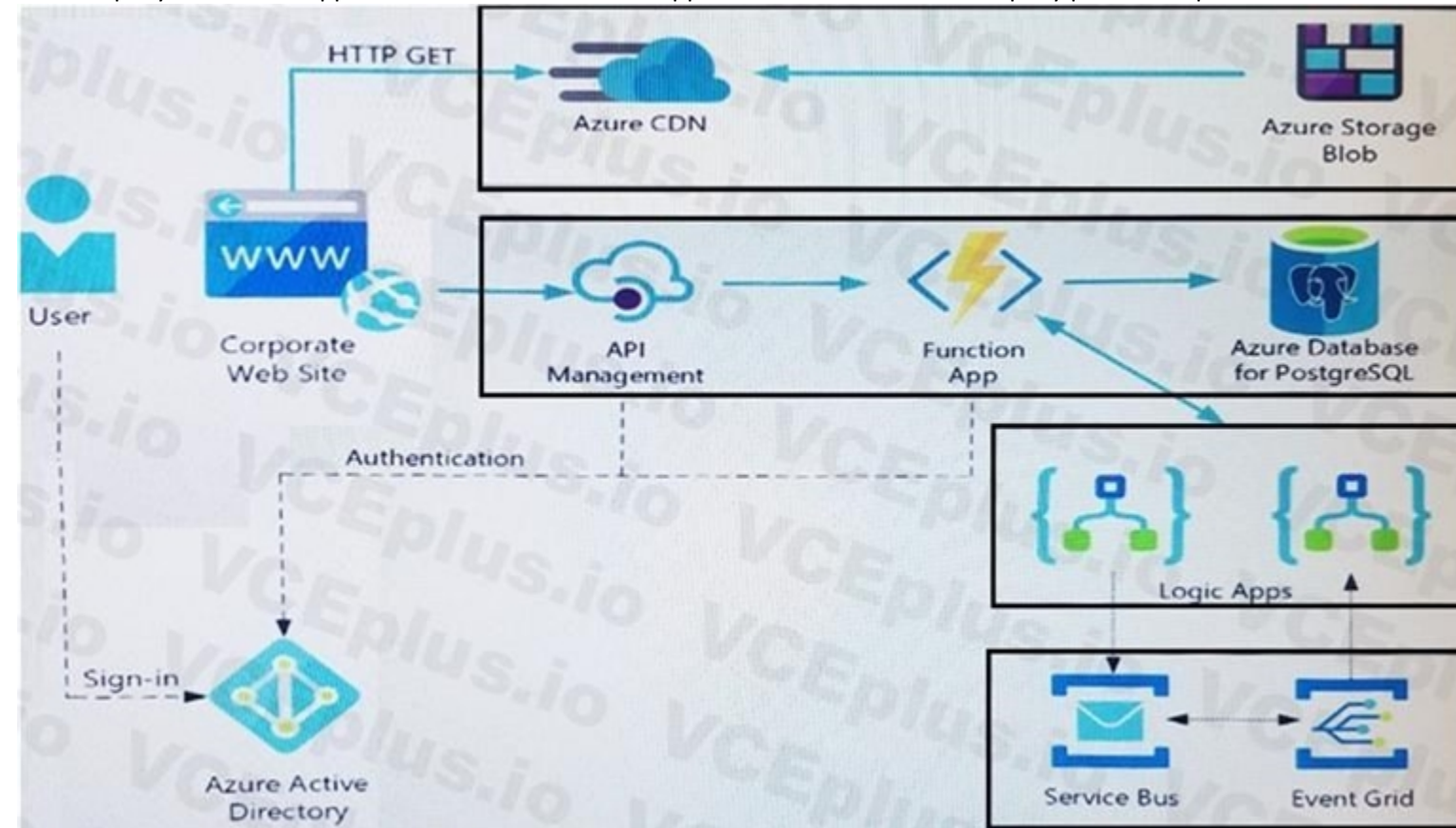
API Management and Azure Function App functions are used to process and store data in Azure Database for PostgreSQL. API Management is used to broker communications to the Azure Function app functions for Logic app integration.

Logic apps are used to orchestrate the data processing while Service Bus and Event Grid handle messaging and events.

The solution uses Application Insights, Azure Monitor, and Azure Key Vault.

Architecture diagram

The company has several applications and services that support their business. The company plans to implement serverless computing where possible. The overall architecture is shown below.



User authentication

The following steps detail the user authentication process:

The user selects Sign in in the website.

The browser redirects the user to the Azure Active Directory (Azure AD) sign in page.

The user signs in.

Azure AD redirects the user's session back to the web application. The URL includes an access token.

The web application calls an API and includes the access token in the authentication header. The application ID is sent as the audience ('aud') claim in the access token.

The back-end API validates the access token.

Requirements

Corporate website

Communications and content must be secured by using SSL.

Communications must use HTTPS.

Data must be replicated to a secondary region and three availability zones.

Data storage costs must be minimized.

Azure Database for PostgreSQL

The database connection string is stored in Azure Key Vault with the following attributes:

Azure Key Vault name: cpandlkeyvault

Secret name: PostgreSQLConn

Id: 80df3e46ffcd4f1cb187f79905e9a1e8

The connection information is updated frequently. The application must always use the latest information to connect to the database.

Azure Service Bus and Azure Event Grid

Azure Event Grid must use Azure Service Bus for queue-based load leveling.

Events in Azure Event Grid must be routed directly to Service Bus queues for use in buffering.

Events from Azure Service Bus and other Azure services must continue to be routed to Azure Event Grid for processing.

Security

All SSL certificates and credentials must be stored in Azure Key Vault.

File access must restrict access by IP, protocol, and Azure AD rights.

All user accounts and processes must receive only those privileges which are essential to perform their intended function.

Compliance

Auditing of the file updates and transfers must be enabled to comply with General Data Protection Regulation (GDPR). The file updates must be read-only, stored in the order in which they occurred, include only create, update, delete, and copy operations, and be retained for compliance reasons.

Issues

Corporate website

While testing the site, the following error message displays:

CryptographicException: The system cannot find the file specified.

Function app

You perform local testing for the RequestUserApproval function. The following error message displays:

'Timeout value of 00:10:00 exceeded by function: RequestUserApproval'

The same error message displays when you test the function in an Azure development environment when you run the following Kusto query:

FunctionAppLogs

| where FunctionName == "RequestUserApproval"

Logic app

You test the Logic app in a development environment. The following error message displays:

'400 Bad Request'

Troubleshooting of the error shows an HttpTrigger action to call the RequestUserApproval function.

Code

Corporate website

Security.cs:

```
SC01 public class Security
SC02 {
SC03     var bytes = System.IO.File.ReadAllBytes("~/var/ssl/private");
SC04     var cert = new System.Security.Cryptography.X509Certificate2(bytes);
SC05     var certName = cert.FriendlyName;
SC06 }
```

Function app

RequestUserApproval.cs:


```
RA01 public static class RequestUserApproval
RA02 {
RA03     [FunctionName("RequestUserApproval")]
RA04     public static async Task<IActionResult> Run(
RA05     [HttpTrigger(AuthorizationLevel.Function, "get", "post", Route = null)] HttpRequest req,
RA06     ILogger log)
RA07     {
RA08         log.LogInformation("RequestUserApproval function processed a request.");
RA09         ...
RA10         return ProcessRequest(req)
RA11             ? (ActionResult)new OkObjectResult($"User approval processed")
RA12             : new BadRequestObjectResult("Failed to process user approval");
RA13     }
RA14     private static bool ProcessRequest(HttpRequest req)
RA15     {
RA16         ...
RA17     }
```

QUESTION 1

HOTSPOT

You need to retrieve the database connection string.

Which values 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

REST API Endpoint:

https://	<div><div></div><div>▼</div></div>	.vault.azure.net/secrets/	<div><div></div><div>▼</div></div>	/						
<table><tr><td>cpandlkeyvault</td><td>cpandlkeyvault</td></tr><tr><td>PostgreSQLConn</td><td>PostgreSQLConn</td></tr><tr><td>80df3e46ffcd4f1cb187f79905e9a1e8</td><td>80df3e46ffcd4f1cb187f79905e9a1e8</td></tr></table>					cpandlkeyvault	cpandlkeyvault	PostgreSQLConn	PostgreSQLConn	80df3e46ffcd4f1cb187f79905e9a1e8	80df3e46ffcd4f1cb187f79905e9a1e8
cpandlkeyvault	cpandlkeyvault									
PostgreSQLConn	PostgreSQLConn									
80df3e46ffcd4f1cb187f79905e9a1e8	80df3e46ffcd4f1cb187f79905e9a1e8									

Variable type to access Azure Key Vault secret values:

<div><div></div><div>▼</div></div>
Environment
Session
ViewState
Querystring

Answer Area:

Answer Area

REST API Endpoint:

https://	<div><div></div><div>▼</div></div>	.vault.azure.net/secrets/	<div><div></div><div>▼</div></div>	/						
<table><tr><td>cpandlkeyvault</td><td>cpandlkeyvault</td></tr><tr><td>PostgreSQLConn</td><td>PostgreSQLConn</td></tr><tr><td>80df3e46ffcd4f1cb187f79905e9a1e8</td><td>80df3e46ffcd4f1cb187f79905e9a1e8</td></tr></table>					cpandlkeyvault	cpandlkeyvault	PostgreSQLConn	PostgreSQLConn	80df3e46ffcd4f1cb187f79905e9a1e8	80df3e46ffcd4f1cb187f79905e9a1e8
cpandlkeyvault	cpandlkeyvault									
PostgreSQLConn	PostgreSQLConn									
80df3e46ffcd4f1cb187f79905e9a1e8	80df3e46ffcd4f1cb187f79905e9a1e8									

Variable type to access Azure Key Vault secret values:

<div><div></div><div>▼</div></div>
Environment
Session
ViewState
Querystring

Section:

Explanation:

Azure database connection string retrieve REST API vault.azure.net/secrets/

Box 1: cpandlkeyvault

We specify the key vault, cpandlkeyvault.

Scenario: The database connection string is stored in Azure Key Vault with the following attributes:

Azure Key Vault name: cpandlkeyvault

Secret name: PostgreSQLConn

Id: 80df3e46ffcd4f1cb187f79905e9a1e8

Box 2: PostgreSQLConn

We specify the secret, PostgreSQLConn

Example, sample request:

<https://myvault.vault.azure.net//secrets/mysecretname/4387e9f3d6e14c459867679a90fd0f79?api-version=7.1>

Box 3: Querystring

Reference:

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

QUESTION 2

DRAG DROP

You need to correct the corporate website error.

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

Select and Place:

Actions

Upload the certificate to Azure Key Vault.

Update line SC05 of Security.cs to include error handling and then redeploy the code.

Update line SC03 of Security.cs to include a using statement and then re-deploy the code.

Add the certificate thumbprint to the WEBSITE_LOAD_CERTIFICATES app setting.

Upload the certificate to source control.

Import the certificate to Azure App Service.

Generate a certificate.

Answer Area

>

<

↑

↓

Correct Answer:

Actions	Answer Area
	Generate a certificate.
	Upload the certificate to Azure Key Vault.
Update line SC03 of Security.cs to include a using statement and then re-deploy the code.	Import the certificate to Azure App Service.
Add the certificate thumbprint to the WEBSITE_LOAD_CERTIFICATES app setting.	Update line SC05 of Security.cs to include error handling and then redeploy the code.
Upload the certificate to source control.	

Section:

Explanation:

Scenario: Corporate website

While testing the site, the following error message displays:

CryptographicException: The system cannot find the file specified.

Step 1: Generate a certificate

Step 2: Upload the certificate to Azure Key Vault

Scenario: All SSL certificates and credentials must be stored in Azure Key Vault.

Step 3: Import the certificate to Azure App Service

Step 4: Update line SC05 of Security.cs to include error handling and then redeploy the code

Reference:

<https://docs.microsoft.com/en-us/azure/app-service/configure-ssl-certificate>

QUESTION 3

HOTSPOT

You need to configure API Management for authentication.

Which policy values 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

Setting	Value
Policy	<div><div></div><div>Check HTTP header</div><div>Restrict caller IPs</div><div>Limit call rate by key</div><div>Validate JWT</div></div>
Policy section	<div><div></div><div>Inbound</div><div>Outbound</div></div>

Answer Area:

Answer Area

Setting	Value
Policy	<div><div></div><div>Check HTTP header</div><div>Restrict caller IPs</div><div>Limit call rate by key</div><div>Validate JWT</div></div>
Policy section	<div><div></div><div>Inbound</div><div>Outbound</div></div>

Section:

Explanation:

Box 1: Validate JWT

The validate-jwt policy enforces existence and validity of a JWT extracted from either a specified HTTP Header or a specified query parameter.

Scenario: User authentication (see step 5 below)

The following steps detail the user authentication process:

1. The user selects Sign in in the website.
2. The browser redirects the user to the Azure Active Directory (Azure AD) sign in page.
3. The user signs in.
4. Azure AD redirects the user's session back to the web application. The URL includes an access token.
5. The web application calls an API and includes the access token in the authentication header. The application ID is sent as the audience ('aud') claim in the access token.
6. The back-end API validates the access token.

Incorrect Answers:

Limit call rate by key - Prevents API usage spikes by limiting call rate, on a per key basis.

Restrict caller IPs - Filters (allows/denies) calls from specific IP addresses and/or address ranges.

Check HTTP header - Enforces existence and/or value of a HTTP Header.

Box 2: Outbound

Reference:

<https://docs.microsoft.com/en-us/azure/api-management/api-management-access-restriction-policies>

QUESTION 4

You need to authenticate the user to the corporate website as indicated by the architectural diagram.

Which two values should you use? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. ID token signature
- B. ID token claims
- C. HTTP response code
- D. Azure AD endpoint URI
- E. Azure AD tenant ID

Correct Answer: A, D

Section:

Explanation:

A: Claims in access tokens

JWTs (JSON Web Tokens) are split into three pieces:

Header - Provides information about how to validate the token including information about the type of token and how it was signed.

Payload - Contains all of the important data about the user or app that is attempting to call your service.

Signature - Is the raw material used to validate the token.

E: Your client can get an access token from either the v1.0 endpoint or the v2.0 endpoint using a variety of protocols.

Scenario: User authentication (see step 5 below)

The following steps detail the user authentication process:

1. The user selects Sign in in the website.
2. The browser redirects the user to the Azure Active Directory (Azure AD) sign in page.
3. The user signs in.
4. Azure AD redirects the user's session back to the web application. The URL includes an access token.
5. The web application calls an API and includes the access token in the authentication header. The application ID is sent as the audience ('aud') claim in the access token.
6. The back-end API validates the access token.

Reference:

<https://docs.microsoft.com/en-us/azure/api-management/api-management-access-restriction-policies>

QUESTION 5

HOTSPOT

You need to correct the Azure Logic app error message.

Which configuration values 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

Setting	Value
authentication level	<div>anonymous</div> <div>function</div> <div>admin</div>
managed identity	<div>system-assigned</div> <div>user-assigned</div>

Answer Area:

Answer Area

Setting	Value
authentication level	<div>anonymous</div> <div>function</div> <div>admin</div>
managed identity	<div>system-assigned</div> <div>user-assigned</div>

Section:

Explanation:

Scenario: You test the Logic app in a development environment. The following error message displays:
'400 Bad Request'

Troubleshooting of the error shows an HttpTrigger action to call the RequestUserApproval function.

Note: If the inbound call's request body doesn't match your schema, the trigger returns an HTTP 400 Bad Request error.

Box 1: function

If you have an Azure function where you want to use the system-assigned identity, first enable authentication for Azure functions.

Box 2: system-assigned

Your logic app or individual connections can use either the system-assigned identity or a single user-assigned identity, which you can share across a group of logic apps, but not both.

Reference:

QUESTION 6

HOTSPOT

You need to configure Azure Service Bus to Event Grid integration.
Which Azure Service Bus settings 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

Setting	Value
Tier	<div>Basic</div> <div>Standard</div> <div>Premium</div>
RBAC role	<div>Owner</div> <div>Contributor</div> <div>Azure Service Bus Data Owner</div> <div>Azure Service Bus Data Receiver</div>

Answer Area:

Answer Area

Setting	Value
Tier	<div>Basic</div> <div>Standard</div> <div>Premium</div>
RBAC role	<div>Owner</div> <div>Contributor</div> <div>Azure Service Bus Data Owner</div> <div>Azure Service Bus Data Receiver</div>

Section:

Explanation:

Box 1: Premium

Service Bus can now emit events to Event Grid when there are messages in a queue or a subscription when no receivers are present. You can create Event Grid subscriptions to your Service Bus namespaces, listen to these events, and then react to the events by starting a receiver. With this feature, you can use Service Bus in reactive programming models.

To enable the feature, you need the following items:

A Service Bus Premium namespace with at least one Service Bus queue or a Service Bus topic with at least one subscription.

Contributor access to the Service Bus namespace.

Box 2: Contributor

Reference:

<https://docs.microsoft.com/en-us/azure/service-bus-messaging/service-bus-to-event-grid-integration-concept>

04 - Implement Azure security

Case study

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

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

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

To start the case study

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. When you are ready to answer a question, click the Question button to return to the question.

Background

You are a developer for Litware Inc., a SaaS company that provides a solution for managing employee expenses. The solution consists of an ASP.NET Core Web API project that is deployed as an Azure Web App.

Overall architecture

Employees upload receipts for the system to process. When processing is complete, the employee receives a summary report email that details the processing results. Employees then use a web application to manage their receipts and perform any additional tasks needed for reimbursement.

Receipt processing

Employees may upload receipts in two ways:

Uploading using an Azure Files mounted folder

Uploading using the web application

Data Storage

Receipt and employee information is stored in an Azure SQL database.

Documentation

Employees are provided with a getting started document when they first use the solution. The documentation includes details on supported operating systems for Azure File upload, and instructions on how to configure the mounted folder.

Solution details

Users table

Column	Description
UserId	unique identifier for and employee
ExpenseAccount	employees expense account number in the format 1234-123-1234
AllowedAmount	limit of allowed expenses before approval is needed
SupervisorId	unique identifier for employee's supervisor
SecurityPin	value used to validate user identity

Web Application

You enable MSI for the Web App and configure the Web App to use the security principal name WebAppIdentity.

Processing

Processing is performed by an Azure Function that uses version 2 of the Azure Function runtime. Once processing is completed, results are stored in Azure Blob Storage and an Azure SQL database. Then, an email summary is sent to the user with a link to the processing report. The link to the report must remain valid if the email is forwarded to another user.

Logging

Azure Application Insights is used for telemetry and logging in both the processor and the web application. The processor also has TraceWriter logging enabled. Application Insights must always contain all log messages.

Requirements

Receipt processing

Concurrent processing of a receipt must be prevented.

Disaster recovery

Regional outage must not impact application availability. All DR operations must not be dependent on application running and must ensure that data in the DR region is up to date.

Security

User's SecurityPin must be stored in such a way that access to the database does not allow the viewing of SecurityPins. The web application is the only system that should have access to SecurityPins.

All certificates and secrets used to secure data must be stored in Azure Key Vault.

You must adhere to the principle of least privilege and provide privileges which are essential to perform the intended function.

All access to Azure Storage and Azure SQL database must use the application's Managed Service Identity (MSI).

Receipt data must always be encrypted at rest.

All data must be protected in transit.

User's expense account number must be visible only to logged in users. All other views of the expense account number should include only the last segment, with the remaining parts obscured.

In the case of a security breach, access to all summary reports must be revoked without impacting other parts of the system.

Issues

Upload format issue

Employees occasionally report an issue with uploading a receipt using the web application. They report that when they upload a receipt using the Azure File Share, the receipt does not appear in their profile. When this occurs, they delete the file in the file share and use the web application, which returns a 500 Internal Server error page.

Capacity issue

During busy periods, employees report long delays between the time they upload the receipt and when it appears in the web application.

Log capacity issue

Developers report that the number of log messages in the trace output for the processor is too high, resulting in lost log messages.

Application code

Processing.cs

```

PC01 public static class Processing
PC02 {
PC03     public static class Function
PC04     {
PC05         [FunctionName("IssueWork")]
PC06         public static async Task Run([TimerTrigger("0 */5 * * * *")] TimerInfo timer, ILogger
log)
PC07         {
PC08             var container = await GetCloudBlobContainer();
PC09             foreach (var fileItem in await ListFiles())
PC10             {
PC11                 var file = new CloudFile(fileItem.StorageUri.PrimaryUri);
PC12                 var ms = new MemoryStream();
PC13                 await file.DownloadToStreamAsync(ms);
PC14                 var blob = container.GetBlockBlobReference(fileItem.Uri.ToString());
PC15                 await blob.UploadFromStreamAsync(ms);
PC16             }
PC17         }
PC18     }
PC19     private static CloudBlockBlob GetDRBlob(CloudBlockBlob sourceBlob)
PC20     {
PC21         . . .
PC22     }
PC23     private static async Task<CloudBlobContainer> GetCloudBlobContainer()
PC24     {
PC25         var cloudBlobClient = new CloudBlobClient(new Uri(". . ."), await GetCredentials());
PC26
PC27         await cloudBlobClient.GetRootContainerReference().CreateIfNotExistsAsync();
PC28         return cloudBlobClient.GetRootContainerReference();
PC29     }
PC30     private static async Task<StorageCredentials> GetCredentials()
PC31     {
PC32         . . .
PC33     }
PC34     private static async Task<List<IListFileItem>> ListFiles()
PC35     {
PC36         . . .
PC37     }
PC37     private KeyVaultClient _keyVaultClient = new KeyVaultClient(". . .");
PC38 }
PC39 }

```

Database.cs


```

DB01 public class Database
DB02 {
DB03     private string ConnectionString =
DB04
DB05     public async Task<object> LoadUserDetails(string userId)
DB06     {
DB07
DB08         return await policy.ExecuteAsync(async () =>
DB09         {
DB10             using (var connection = new SqlConnection(ConnectionString))
DB11             {
DB12                 await connection.OpenAsync();
DB13                 using (var command = new SqlCommand("...", connection))
DB14                 using (var reader = command.ExecuteReader())
DB15                 {
DB16                     ...
DB17                 }
DB18             }
DB19         });
DB20     }
DB21 }

```

ReceiptUploader.cs

```

RU01 public class ReceiptUploader
RU02 {
RU03     public async Task UploadFile(string file, byte[] binary)
RU04     {
RU05         var httpClient = new HttpClient();
RU06         var response = await httpClient.PutAsync("...", new ByteArrayContent(binary));
RU07         while (ShouldRetry(response))
RU08         {
RU09             response = await httpClient.PutAsync("...", new ByteArrayContent(binary));
RU10         }
RU11     }
RU12     private bool ShouldRetry(HttpResponseMessage response)
RU13     {
RU14
RU15     }
RU16 }

```

ConfigureSSE.ps1


```
CS01 $storageAccount = Get-AzureRmStorageAccount -ResourceGroupName "... " -AccountName "... "
CS02 $keyVault = Get-AzureRmKeyVault -VaultName "... "
CS03 $key = Get-AzureKeyVaultKey -VaultName $keyVault.VaultName -Name "... "
CS04 Set-AzureRmKeyVaultAccessPolicy `
CS05   -VaultName $keyVault.VaultName `
CS06   -ObjectId $storageAccount.Identity.PrincipalId `
CS07
CS08
CS09 Set-AzureRmStorageAccount `
CS10   -ResourceGroupName $storageAccount.ResourceGroupName `
CS11   -AccountName $storageAccount.StorageAccountName `
CS12   -EnableEncryptionService File `
CS13   -KeyvaultEncryption `
CS14   -KeyName $key.Name
CS15   -KeyVersion $key.Version `
CS16   -KeyVaultUri $keyVault.VaultUri
```

QUESTION 1

HOTSPOT

You need to add code at line PC26 of Processing.cs to ensure that security policies are met.

How should you complete the code that you will add at line PC26? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

```
var resolver = new KeyVaultKeyResolver(_keyVaultClient);  
var keyBundle = await _keyVaultClient.GetKeyAsync("...", "...");
```

```
var key = keyBundle.Key;  
var key = keyBundle.KeyIdentifier.Identifier;  
var key = await resolver.ResolveKeyAsync("encrypt", null);  
var key = await resolver.ResolveKeyAsync(keyBundle.KeyIdentifier.Identifier, CancellationToken.None);
```

```
var x = keyBundle.Managed;  
var x = AuthenticationScheme.SharedKey;  
var x = new BlobEncryptionPolicy(key, resolver);  
var x = new DeleteRetentionPolicy {Enabled = key.Kid != null};
```

```
cloudBlobClient.AuthenticationScheme = x;  
cloudBlobClient.DefaultRequestOptions.RequireEncryption = x;  
cloudBlobClient.DefaultRequestOptions.EncryptionPolicy = x;  
cloudBlobClient.SetServiceProperties(new ServiceProperties(deleteRetentionPolicy:x));
```

Answer Area:

Answer Area

```
var resolver = new KeyVaultKeyResolver(_keyVaultClient);  
var keyBundle = await _keyVaultClient.GetKeyAsync("...", "...");
```

```
var key = keyBundle.Key;  
var key = keyBundle.KeyIdentifier.Identifier;  
var key = await resolver.ResolveKeyAsync("encrypt", null);  
var key = await resolver.ResolveKeyAsync(keyBundle.KeyIdentifier.Identifier, CancellationToken.None);
```

```
var x = keyBundle.Managed;  
var x = AuthenticationScheme.SharedKey;  
var x = new BlobEncryptionPolicy(key, resolver);  
var x = new DeleteRetentionPolicy {Enabled = key.Kid != null};
```

```
cloudBlobClient.AuthenticationScheme = x;  
cloudBlobClient.DefaultRequestOptions.RequireEncryption = x;  
cloudBlobClient.DefaultRequestOptions.EncryptionPolicy = x;  
cloudBlobClient.SetServiceProperties(new ServiceProperties(deleteRetentionPolicy:x));
```

Section:

Explanation:

Box 1: var key = await Resolver.ResolveKeyAsyn(keyBundle,KeyIdentifier.CancellationToken.None);

Box 2: var x = new BlobEncryptionPolicy(key,resolver);

Example:

// We begin with cloudKey1, and a resolver capable of resolving and caching Key Vault secrets.

BlobEncryptionPolicy encryptionPolicy = new BlobEncryptionPolicy(cloudKey1, cachingResolver); client.DefaultRequestOptions.EncryptionPolicy = encryptionPolicy;

Box 3: cloudblobClient. DefaultRequestOptions.EncryptionPolicy = x;

Reference:

<https://github.com/Azure/azure-storage-net/blob/master/Samples/GettingStarted/EncryptionSamples/KeyRotation/Program.cs>

QUESTION 2

You need to ensure the security policies are met.

What code do you add at line CS07 of ConfigureSSE.ps1?

- A. -PermissionsToKeys create, encrypt, decrypt
- B. -PermissionsToCertificates create, encrypt, decrypt
- C. -PermissionsToCertificates wrapkey, unwrapkey, get
- D. -PermissionsToKeys wrapkey, unwrapkey, get

Correct Answer: B

Section:

Explanation:

Scenario: All certificates and secrets used to secure data must be stored in Azure Key Vault.

You must adhere to the principle of least privilege and provide privileges which are essential to perform the intended function.

The Set-AzureRmKeyVaultAccessPolicy parameter -PermissionsToKeys specifies an array of key operation permissions to grant to a user or service principal. The acceptable values for this parameter: decrypt, encrypt, unwrapKey, wrapKey, verify, sign, get, list, update, create, import, delete, backup, restore, recover, purge

Incorrect Answers:

A, C: The Set-AzureRmKeyVaultAccessPolicy parameter -PermissionsToCertificates specifies an array of certificate permissions to grant to a user or service principal. The acceptable values for this parameter: get, list, delete, create, import, update, managecontacts, getissuers, listissuers, setissuers, deleteissuers, manageissuers, recover, purge, backup, restore

Reference:

<https://docs.microsoft.com/en-us/powershell/module/azurerm.keyvault/set-azurermkeyvaultaccesspolicy>

05 - Implement Azure security

QUESTION 1

Your company is developing an Azure API.

You need to implement authentication for the Azure API. You have the following requirements:

All API calls must be secure.

Callers to the API must not send credentials to the API.

Which authentication mechanism should you use?

- A. Basic
- B. Anonymous
- C. Managed identity
- D. Client certificate

Correct Answer: C

Section:

Explanation:

Use the authentication-managed-identity policy to authenticate with a backend service using the managed identity of the API Management service. This policy essentially uses the managed identity to obtain an access token from Azure Active Directory for accessing the specified resource. After successfully obtaining the token, the policy will set the value of the token in the Authorization header using the Bearer scheme.

Reference: <https://docs.microsoft.com/bs-cyrl-ba/azure/api-management/api-management-authentication-policies>

QUESTION 2

You are a developer for a SaaS company that offers many web services.

All web services for the company must meet the following requirements:

Use API Management to access the services

Use OpenID Connect for authentication

Prevent anonymous usage

A recent security audit found that several web services can be called without any authentication.

Which API Management policy should you implement?

- A. jsonp
- B. authentication-certificate
- C. check-header
- D. validate-jwt

Correct Answer: D

Section:**Explanation:**

Add the validate-jwt policy to validate the OAuth token for every incoming request.

Incorrect Answers:

A: The jsonp policy adds JSON with padding (JSONP) support to an operation or an API to allow cross-domain calls from JavaScript browser-based clients. JSONP is a method used in JavaScript programs to request data from a server in a different domain. JSONP bypasses the limitation enforced by most web browsers where access to web pages must be in the same domain.

JSONP - Adds JSON with padding (JSONP) support to an operation or an API to allow cross-domain calls from JavaScript browser-based clients.

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

QUESTION 3

You have a new Azure subscription. You are developing an internal website for employees to view sensitive data. The website uses Azure Active Directory (Azure AD) for authentication.

You need to implement multifactor authentication for the website.

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

NOTE: Each correct selection is worth one point.

- A. Configure the website to use Azure AD B2C.
- B. In Azure AD, create a new conditional access policy.
- C. Upgrade to Azure AD Premium.
- D. In Azure AD, enable application proxy.
- E. In Azure AD conditional access, enable the baseline policy.

Correct Answer: B, C

Section:**Explanation:**

B: MFA Enabled by conditional access policy. It is the most flexible means to enable two-step verification for your users. Enabling using conditional access policy only works for Azure MFA in the cloud and is a premium feature of Azure AD.

C: Multi-Factor Authentication comes as part of the following offerings:

Azure Active Directory Premium licenses - Full featured use of Azure Multi-Factor Authentication Service (Cloud) or Azure Multi-Factor Authentication Server (On-premises).

Multi-Factor Authentication for Office 365

Azure Active Directory Global Administrators

Reference:

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

QUESTION 4

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 develop Azure solutions.

You must grant a virtual machine (VM) access to specific resource groups in Azure Resource Manager.

You need to obtain an Azure Resource Manager access token.

Solution: Use an X.509 certificate to authenticate the VM with Azure Resource Manager.

Does the solution meet the goal?

- A. Yes
- B. No

Correct Answer: B

Section:**Explanation:**

Instead run the Invoke-RestMethod cmdlet to make a request to the local managed identity for Azure resources endpoint.

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

QUESTION 5

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

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

You develop Azure solutions.

You must grant a virtual machine (VM) access to specific resource groups in Azure Resource Manager.

You need to obtain an Azure Resource Manager access token.

Solution: Use the Reader role-based access control (RBAC) role to authenticate the VM with Azure Resource Manager.

Does the solution meet the goal?

A. Yes

B. No

Correct Answer: B

Section:

Explanation:

Instead run the Invoke-RestMethod cmdlet to make a request to the local managed identity for Azure resources endpoint.

Reference:

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

QUESTION 6

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

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

You develop Azure solutions.

You must grant a virtual machine (VM) access to specific resource groups in Azure Resource Manager.

You need to obtain an Azure Resource Manager access token.

Solution: Run the Invoke-RestMethod cmdlet to make a request to the local managed identity for Azure resources endpoint.

Does the solution meet the goal?

A. Yes

B. No

Correct Answer: A

Section:

Explanation:

Get an access token using the VM's system-assigned managed identity and use it to call Azure Resource Manager

You will need to use PowerShell in this portion.

1. In the portal, navigate to Virtual Machines and go to your Windows virtual machine and in the Overview, click Connect.

2. Enter in your Username and Password for which you added when you created the Windows VM.

3. Now that you have created a Remote Desktop Connection with the virtual machine, open PowerShell in the remote session.

4. Using the Invoke-WebRequest cmdlet, make a request to the local managed identity for Azure resources endpoint to get an access token for Azure Resource Manager.

Example:

```
$response = Invoke-WebRequest -Uri 'http://169.254.169.254/metadata/identity/oauth2/token?api-version=2018-02-01&resource=https://management.azure.com/' -Method GET -Headers @{Metadata="true"}
```

Reference:

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

QUESTION 7

DRAG DROP

Contoso, Ltd. provides an API to customers by using Azure API Management (APIM). The API authorizes users with a JWT token.

You must implement response caching for the APIM gateway. The caching mechanism must detect the user ID of the client that accesses data for a given location and cache the response for that user ID.

You need to add the following policies to the policies file:

a set-variable policy to store the detected user identity

a cache-lookup-value policy

a cache-store-value policy

a find-and-replace policy to update the response body with the user profile information

To which policy section should you add the policies? To answer, drag the appropriate sections to the correct policies. Each section 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:

Answer Area

Policy section	Policy	Policy section
	Set-variable	
Inbound	Cache-lookup-value	
Outbound	Cache-store-value	
	Find-and-replace	

Correct Answer:

Answer Area

Policy section

Policy

Policy section

Set-variable

Inbound

Inbound

Cache-lookup-value

Inbound

Outbound

Cache-store-value

Outbound

Find-and-replace

Section:

Explanation:

Box 1: Inbound.

A set-variable policy to store the detected user identity.

Example:

```
<policies>
```

```
<inbound>
```

```
<!-- How you determine user identity is application dependent -->
```

```
<set-variable
```

```
name="enduserid"
```

```
value="@context.Request.Headers.GetValueOrDefault("Authorization","").Split(' ')[1].AsJwt()?.Subject)" />
```

Box 2: Inbound

A cache-lookup-value policy

Example:

```
<inbound>
```

```
<base />
```

```
<cache-lookup vary-by-developer="true | false" vary-by-developer-groups="true | false" downstream-caching-type="none | private | public" must-revalidate="true | false">
```

```
<vary-by-query-parameter>parameter name</vary-by-query-parameter> <!-- optional, can repeated several times -->
```

```
</cache-lookup>
```

```
</inbound>
```

Box 3: Outbound

A cache-store-value policy.

Example:

```
<outbound>
```

```
<base />
```

```
<cache-store duration="3600" />
```

```
</outbound>
```

Box 4: Outbound

A find-and-replace policy to update the response body with the user profile information.

Example:

```
<outbound>
```

```
<!-- Update response body with user profile-->
```



```
<find-and-replace
from="$userprofile$"
to="@((string)context.Variables["userprofile"])" />
<base />
</outbound>
Reference:
https://docs.microsoft.com/en-us/azure/api-management/api-management-caching-policies
https://docs.microsoft.com/en-us/azure/api-management/api-management-sample-cache-by-key
```

QUESTION 8

DRAG DROP

You develop a web application.
You need to register the application with an active Azure Active Directory (Azure AD) tenant.
Which three actions should you perform in sequence? To answer, move all actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place:

Actions

Select **Manifest** from the middle-tier service registration.

In Enterprise Applications, select **New application**.

Add a Cryptographic key.

Create a new application and provide the name, account type, and redirect URI.

Select the Azure AD instance.

Use an access token to access the secure resource.

In App Registrations, select **New registration**.

Answer Area

⬅

➡

⬆

⬆

Correct Answer:

Actions

Select **Manifest** from the middle-tier service registration.

In Enterprise Applications, select **New application**.

Add a Cryptographic key.

Use an access token to access the secure resource.

Answer Area

Select the Azure AD instance.

In App Registrations, select **New registration**.

Create a new application and provide the name, account type, and redirect URI.

⬅

➡

⬆

⬇

Section:

Explanation:

Register a new application using the Azure portal

1. Sign in to the Azure portal using either a work or school account or a personal Microsoft account.
2. If your account gives you access to more than one tenant, select your account in the upper right corner. Set your portal session to the Azure AD tenant that you want.
3. Search for and select Azure Active Directory. Under Manage, select App registrations.
4. Select New registration. (Step 1)
5. In Register an application, enter a meaningful application name to display to users.
6. Specify who can use the application. Select the Azure AD instance. (Step 2)
7. Under Redirect URI (optional), select the type of app you're building: Web or Public client (mobile & desktop). Then enter the redirect URI, or reply URL, for your application. (Step 3)
8. When finished, select Register.

QUESTION 9

DRAG DROP

You are developing an application. You have an Azure user account that has access to two subscriptions.

You need to retrieve a storage account key secret from Azure Key Vault.

In which order should you arrange the PowerShell commands to develop the solution? To answer, move all commands from the list of commands to the answer area and arrange them in the correct order.

Select and Place:

Powershell commands

Answer Area

```
$secretvalue = ConvertTo-SecureString  
$storAcctkey -AsPlainText  
-Force  
Set-AzKeyVaultSecret -VaultName  
$vaultName -Name $secretName  
-SecretValue $secretvalue
```

```
Get-AzStorageAccountKey -  
ResourceGroupName $resGroup -Name  
$storAcct
```

```
Set-AzContext -SubscriptionId  
$subscriptionID
```

```
Get-AzKeyVaultSecret -VaultName  
$vaultName
```

```
Get-AzSubscription
```



Correct Answer:

Powershell commands

Answer Area

```
Get-AzSubscription
```

```
Set-AzContext -SubscriptionId  
$subscriptionID
```

```
Get-AzStorageAccountKey -  
ResourceGroupName $resGroup -Name  
$storAcct
```

```
$secretvalue = ConvertTo-SecureString  
$storAcctkey -AsPlainText  
-Force  
Set-AzKeyVaultSecret -VaultName  
Get-AzKeyVaultSecret -VaultName  
$vaultName
```

Section:

Explanation:

Step 1: Get-AzSubscription

If you have multiple subscriptions, you might have to specify the one that was used to create your key vault. Enter the following to see the subscriptions for your account:

```
Get-AzSubscription
```

Step 2: Set-AzContext -SubscriptionId

To specify the subscription that's associated with the key vault you'll be logging, enter:

```
Set-AzContext -SubscriptionId <subscriptionID>
```

Step 3: Get-AzStorageAccountKey

You must get that storage account key.

Step 4: \$secretvalue = ConvertTo-SecureString <storageAccountKey> -AsPlainText -Force

```
Set-AzKeyVaultSecret -VaultName <vaultName> -Name <secretName> -SecretValue $secretvalue
```

After retrieving your secret (in this case, your storage account key), you must convert that key to a secure string, and then create a secret with that value in your key vault.

Step 5: Get-AzKeyVaultSecret

Next, get the URI for the secret you created. You'll need this URI in a later step to call the key vault and retrieve your secret. Run the following PowerShell command and make note of the ID value, which is the secret's URI:

```
Get-AzKeyVaultSecret -VaultName <vaultName>
```

Reference:

<https://docs.microsoft.com/bs-latn-ba/Azure/key-vault/key-vault-key-rotation-log-monitoring>

QUESTION 10

HOTSPOT

You are building a website to access project data related to teams within your organization. The website does not allow anonymous access. Authentication is performed using an Azure Active Directory (Azure AD) app named internal.

NOTE: Each correct selection is worth one point.

Answer Area

```
{
  ...
  "appId": "d61126e3-089b-4adb-b721-d5023213df7d",
  "displayName": "internal",

  ...
  "optionalClaims": {
    "groupMembershipClaims": "All",

    ...
    "allowPublicClient": true,
    "oauth2Permissions": {
      "requiredResourceAccess": [
        {
          "resource": "https://graph.microsoft.com/...",
          "scope": "openid"
        }
      ]
    }
  }
}
```

Answer Area

```
{
  ...
  "appId": "d61126e3-089b-4adb-b721-d5023213df7d",
  "displayName": "internal",

  ...
  "optionalClaims": {
    "groupMembershipClaims": "All",

    ...
    "allowPublicClient": true,
    "oauth2Permissions": {
      "requiredResourceAccess": {
        "oauth2AllowImplicitFlow": true
      }
    }
  }
}
```

Scenario: Personalization of the website must be based on membership in Active Directory groups.

Group claims can also be configured in the Optional Claims section of the Application Manifest.

Enable group membership claims by changing the groupMembershipClaim

The valid values are:

"All"

"SecurityGroup"

"DistributionList"

"DirectoryRole"

Here we need to mention that we want to get the groups for the users. Hence we need to mention to set the groupMembershipClaims property to All.

Box 2: oAuth2AllowImplicitFlow

Azure AD users must be able to login to the website. auth2Permissions can only accept collections value like an array, not a boolean. oAuth2AllowImplicitFlow accepts boolean value. Here from the list of options given, if we want the application to fetch the required tokens, we would need to allow Implicit Flow.

QUESTION 11

You develop an app that allows users to upload photos and videos to Azure storage. The app uses a storage REST API call to upload the media to a blob storage account named Account1. You have blob storage containers named

Container1 and Container2.

Uploading of videos occurs on an irregular basis.

You need to copy specific blobs from Container1 to Container2 when a new video is uploaded.

What should you do?

- A. Copy blobs to Container2 by using the Put Blob operation of the Blob Service REST API
- B. Create an Event Grid topic that uses the Start-AzureStorageBlobCopy cmdlet
- C. Use AzCopy with the Snapshot switch to copy blobs to Container2
- D. Download the blob to a virtual machine and then upload the blob to Container2

Correct Answer: B

Section:

Explanation:

The Start-AzureStorageBlobCopy cmdlet starts to copy a blob.

Example 1: Copy a named blob

```
C:\PS>Start-AzureStorageBlobCopy -SrcBlob "ContosoPlanning2015" -DestContainer "ContosoArchives" -SrcContainer "ContosoUploads"
```

This command starts the copy operation of the blob named ContosoPlanning2015 from the container named ContosoUploads to the container named ContosoArchives.

Reference:

<https://docs.microsoft.com/en-us/powershell/module/azure.storage/start-azurstorageblobcopy?view=azurermps-6.13.0>

QUESTION 12

You are developing an ASP.NET Core website that uses Azure FrontDoor. The website is used to build custom weather data sets for researchers. Data sets are downloaded by users as Comma Separated Value (CSV) files. The data is refreshed every 10 hours.

Specific files must be purged from the FrontDoor cache based upon Response Header values.

You need to purge individual assets from the Front Door cache.

Which type of cache purge should you use?

- A. single path
- B. wildcard
- C. root domain

Correct Answer: A

Section:

Explanation:

These formats are supported in the lists of paths to purge:

Single path purge: Purge individual assets by specifying the full path of the asset (without the protocol and domain), with the file extension, for example, /pictures/strasbourg.png;

Wildcard purge: Asterisk (*) may be used as a wildcard. Purge all folders, subfolders, and files under an endpoint with /* in the path or purge all subfolders and files under a specific folder by specifying the folder followed by /*, for example, /pictures/*.

Root domain purge: Purge the root of the endpoint with "/" in the path.

Reference:

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

QUESTION 13

You are developing a Java application that uses Cassandra to store key and value data. You plan to use a new Azure Cosmos DB resource and the Cassandra API in the application. You create an Azure Active Directory (Azure AD) group named Cosmos DB Creators to enable provisioning of Azure Cosmos accounts, databases, and containers.

The Azure AD group must not be able to access the keys that are required to access the data.

You need to restrict access to the Azure AD group.

Which role-based access control should you use?

- A. DocumentDB Accounts Contributor
- B. Cosmos Backup Operator
- C. Cosmos DB Operator
- D. Cosmos DB Account Reader

Correct Answer: C

Section:

Explanation:

Azure Cosmos DB now provides a new RBAC role, Cosmos DB Operator. This new role lets you provision Azure Cosmos accounts, databases, and containers, but can't access the keys that are required to access the data. This role is intended for use in scenarios where the ability to grant access to Azure Active Directory service principals to manage deployment operations for Cosmos DB is needed, including the account, database, and containers.

Reference:

<https://azure.microsoft.com/en-us/updates/azure-cosmos-db-operator-role-for-role-based-access-control-rbac-is-now-available/>

QUESTION 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.

You are developing a website that will run as an Azure Web App. Users will authenticate by using their Azure Active Directory (Azure AD) credentials.

You plan to assign users one of the following permission levels for the website: admin, normal, and reader. A user's Azure AD group membership must be used to determine the permission level.

You need to configure authorization.

Solution: Configure the Azure Web App for the website to allow only authenticated requests and require Azure AD log on.

Does the solution meet the goal?

- A. Yes
- B. No

Correct Answer: B

Section:

Explanation:

Instead in the Azure AD application's manifest, set value of the groupMembershipClaims option to All.

Reference:

<https://blogs.msdn.microsoft.com/waws/2017/03/13/azure-app-service-authentication-aad-groups/>

QUESTION 15

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 developing a website that will run as an Azure Web App. Users will authenticate by using their Azure Active Directory (Azure AD) credentials.

You plan to assign users one of the following permission levels for the website: admin, normal, and reader. A user's Azure AD group membership must be used to determine the permission level.

You need to configure authorization.

Solution:

Create a new Azure AD application. In the application's manifest, set value of the groupMembershipClaims option to All.

In the website, use the value of the groups claim from the JWT for the user to determine permissions.

Does the solution meet the goal?

A. Yes

B. No

Correct Answer: A

Section:

Explanation:

To configure Manifest to include Group Claims in Auth Token

1. Go to Azure Active Directory to configure the Manifest. Click on Azure Active Directory, and go to App registrations to find your application:

2. Click on your application (or search for it if you have a lot of apps) and edit the Manifest by clicking on it.

3. Locate the "groupMembershipClaims" setting. Set its value to either "SecurityGroup" or "All". To help you decide which:

"SecurityGroup" - groups claim will contain the identifiers of all security groups of which the user is a member.

"All" - groups claim will contain the identifiers of all security groups and all distribution lists of which the user is a member

Now your application will include group claims in your manifest and you can use this fact in your code.

Reference:

<https://blogs.msdn.microsoft.com/waws/2017/03/13/azure-app-service-authentication-aad-groups/>

QUESTION 16

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

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

You are developing a website that will run as an Azure Web App. Users will authenticate by using their Azure Active Directory (Azure AD) credentials.

You plan to assign users one of the following permission levels for the website: admin, normal, and reader. A user's Azure AD group membership must be used to determine the permission level.

You need to configure authorization.

Solution:

Create a new Azure AD application. In the application's manifest, define application roles that match the required permission levels for the application.

Assign the appropriate Azure AD group to each role. In the website, use the value of the roles claim from the JWT for the user to determine permissions.

Does the solution meet the goal?

A. Yes

B. No

Correct Answer: B

Section:

Explanation:

To configure Manifest to include Group Claims in Auth Token

1. Go to Azure Active Directory to configure the Manifest. Click on Azure Active Directory, and go to App registrations to find your application:

2. Click on your application (or search for it if you have a lot of apps) and edit the Manifest by clicking on it.

3. Locate the "groupMembershipClaims" setting. Set its value to either "SecurityGroup" or "All". To help you decide which:

"SecurityGroup" - groups claim will contain the identifiers of all security groups of which the user is a member.
"All" - groups claim will contain the identifiers of all security groups and all distribution lists of which the user is a member
Now your application will include group claims in your manifest and you can use this fact in your code.
Reference:
<https://blogs.msdn.microsoft.com/waws/2017/03/13/azure-app-service-authentication-aad-groups/>

QUESTION 17

DRAG DROP

You are developing an application to securely transfer data between on-premises file systems and Azure Blob storage. The application stores keys, secrets, and certificates in Azure Key Vault. The application uses the Azure Key Vault APIs.

The application must allow recovery of an accidental deletion of the key vault or key vault objects. Key vault objects must be retained for 90 days after deletion.

You need to protect the key vault and key vault objects.

Which Azure Key Vault feature should you use? To answer, drag the appropriate features to the correct actions. Each feature 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:

Features	Answer Area
Access policy	
Purge protection	
Soft delete	
Shared access signature	

Action	Feature
Enable retention period and accidental deletion.	Feature
Enforce retention period and accidental deletion.	Feature

Correct Answer:

Features	Answer Area
Access policy	
Shared access signature	

Action	Feature
Enable retention period and accidental deletion.	Soft delete
Enforce retention period and accidental deletion.	Purge protection

Section:

Explanation:

Box 1: Soft delete

When soft-delete is enabled, resources marked as deleted resources are retained for a specified period (90 days by default). The service further provides a mechanism for recovering the deleted object, essentially undoing the deletion.

Box 2: Purge protection

Purge protection is an optional Key Vault behavior and is not enabled by default. Purge protection can only be enabled once soft-delete is enabled.

When purge protection is on, a vault or an object in the deleted state cannot be purged until the retention period has passed. Soft-deleted vaults and objects can still be recovered, ensuring that the retention policy will be followed.

Reference:
<https://docs.microsoft.com/en-us/azure/key-vault/general/soft-delete-overview>

QUESTION 18

You provide an Azure API Management managed web service to clients. The back-end web service implements HTTP Strict Transport Security (HSTS).

Every request to the backend service must include a valid HTTP authorization header.
You need to configure the Azure API Management instance with an authentication policy.
Which two policies can you use? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

- A. Basic Authentication
- B. Digest Authentication
- C. Certificate Authentication
- D. OAuth Client Credential Grant

Correct Answer: A, B
Section:

QUESTION 19
DRAG DROP

You are developing an ASP.NET Core website that can be used to manage photographs which are stored in Azure Blob Storage containers.
Users of the website authenticate by using their Azure Active Directory (Azure AD) credentials.
You implement role-based access control (RBAC) role permissions on the containers that store photographs. You assign users to RBAC roles.
You need to configure the website's Azure AD Application so that user's permissions can be used with the Azure Blob containers.
How should you configure the application? To answer, drag the appropriate setting to the correct location. Each setting can 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:

Settings

client_id

profile

delegated

application

user_impersonation

Answer Area

API	Permission	Type
Azure Storage	Setting	Setting
Microsoft Graph	User.Read	Setting

Correct Answer:

Settings	Answer Area		
client_id			
profile			
delegated			
application			
user_impersonation			

API	Permission	Type
Azure Storage	user_impersonation	delegated
Microsoft Graph	User.Read	delegated

Section:

Explanation:

Box 1: user_impersonation

Box 2: delegated

Example:

1. Select the API permissions section
2. Click the Add a permission button and then:

Ensure that the My APIs tab is selected

3. In the list of APIs, select the API TodoListService-aspnetcore.
4. In the Delegated permissions section, ensure that the right permissions are checked: user_impersonation.
5. Select the Add permissions button.

Box 3: delegated

Example

1. Select the API permissions section
 2. Click the Add a permission button and then,
- Ensure that the Microsoft APIs tab is selected
3. In the Commonly used Microsoft APIs section, click on Microsoft Graph
 4. In the Delegated permissions section, ensure that the right permissions are checked: User.Read. Use the search box if necessary.
 5. Select the Add permissions button

Reference:

<https://docs.microsoft.com/en-us/samples/azure-samples/active-directory-dotnet-webapp-webapi-openidconnect-aspnetcore/calling-a-web-api-in-an-aspnet-core-web-application-using-azure-ad/>

QUESTION 20

HOTSPOT

You are developing an ASP.NET Core app that includes feature flags which are managed by Azure App Configuration. You create an Azure App Configuration store named AppFeatureFlagStore that contains a feature flag named Export.

You need to update the app to meet the following requirements:

Use the Export feature in the app without requiring a restart of the app.

Validate users before users are allowed access to secure resources.

Permit users to access secure resources.

How should you complete the code segment? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

```
public void Configure(IApplicationBuilder app, IWebHostEnvironment env)
{
    if (env.IsDevelopment())
    {
        app.UseDeveloperExceptionPage();
    }
    else
    {
        app.UseExceptionHandler("/Error");
    }

    app.
    (
        UseAuthentication
        UseStaticFiles
        UseSession
        UseCookiePolicy
    );

    app.
    (
        UseAuthorization
        UseHttpsRedirection
        UseSession
        UseCookiePolicy
    );

    app.
    (
        UseAzureAppConfiguration
        UseRequestLocalization
        UseCors
        UseStaticFiles
    );

    app.UseEndpoint(endpoints =>
    {
        endpoints.MapRazorPages();
    });
}
```

Answer Area:

Answer Area

```
public void Configure(IApplicationBuilder app, IWebHostEnvironment env)
{
    if (env.IsDevelopment())
    {
        app.UseDeveloperExceptionPage();
    }
    else
    {
        app.UseExceptionHandler("/Error");
    }

    app.
    (
        UseAuthentication
        UseStaticFiles
        UseSession
        UseCookiePolicy
    );

    app.
    (
        UseAuthorization
        UseHttpsRedirection
        UseSession
        UseCookiePolicy
    );

    app.
    (
        UseAzureAppConfiguration
        UseRequestLocalization
        UseCors
        UseStaticFiles
    );

    app.UseEndpoints(endpoints =>
    {
        endpoints.MapRazorPages();
    });
}
```

Section:

Explanation:

Box 1: UseAuthentication

Need to validate users before users are allowed access to secure resources.

UseAuthentication adds the AuthenticationMiddleware to the specified IApplicationBuilder, which enables authentication capabilities.

Box 2: UseAuthorization

Need to permit users to access secure resources.

UseAuthorization adds the AuthorizationMiddleware to the specified IApplicationBuilder, which enables authorization capabilities.

Box 3: UseStaticFiles

Need to use the Export feature in the app without requiring a restart of the app.

UseStaticFiles enables static file serving for the current request path

Reference:

<https://docs.microsoft.com/en-us/dotnet/api/microsoft.aspnetcore.builder.iapplicationbuilder?view=aspnetcore-5.0>

QUESTION 21

You have an application that includes an Azure Web app and several Azure Function apps. Application secrets including connection strings and certificates are stored in Azure Key Vault.

Secrets must not be stored in the application or application runtime environment. Changes to Azure Active Directory (Azure AD) must be minimized.

You need to design the approach to loading application secrets.

What should you do?

- A. Create a single user-assigned Managed Identity with permission to access Key Vault and configure each App Service to use that Managed Identity.
- B. Create a single Azure AD Service Principal with permission to access Key Vault and use a client secret from within the App Services to access Key Vault.
- C. Create a system assigned Managed Identity in each App Service with permission to access Key Vault.
- D. Create an Azure AD Service Principal with Permissions to access Key Vault for each App Service and use a certificate from within the App Services to access Key Vault.

Correct Answer: A

Section:

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 developing a medical records document management website. The website is used to store scanned copies of patient intake forms.

If the stored intake forms are downloaded from storage by a third party, the contents of the forms must not be compromised.

You need to store the intake forms according to the requirements.

Solution: Create an Azure Key Vault key named skey. Encrypt the intake forms using the public key portion of skey. Store the encrypted data in Azure Blob storage.

Does the solution meet the goal?

- A. Yes
- B. No

Correct Answer: A

Section:

QUESTION 23

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 developing a medical records document management website. The website is used to store scanned copies of patient intake forms.

If the stored intake forms are downloaded from storage by a third party, the contents of the forms must not be compromised.

You need to store the intake forms according to the requirements.

Solution: Create an Azure Cosmos DB database with Storage Service Encryption enabled. Store the intake forms in the Azure Cosmos DB database.

Does the solution meet the goal?

- A. Yes
- B. No

Correct Answer: B

Section:

Explanation:

Instead use an Azure Key vault and public key encryption. Store the encrypted from in Azure Storage Blob storage.

QUESTION 24

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 developing a medical records document management website. The website is used to store scanned copies of patient intake forms.

If the stored intake forms are downloaded from storage by a third party, the contents of the forms must not be compromised.

You need to store the intake forms according to the requirements.

Solution: Store the intake forms as Azure Key Vault secrets.

Does the solution meet the goal?

A. Yes

B. No

Correct Answer: B

Section:

Explanation:

Instead use an Azure Key vault and public key encryption. Store the encrypted from in Azure Storage Blob storage.

QUESTION 25

HOTSPOT

You plan to deploy a new application to a Linux virtual machine (VM) that is hosted in Azure.

The entire VM must be secured at rest by using industry-standard encryption technology to address organizational security and compliance requirements.

You need to configure Azure Disk Encryption for the VM.

How should you complete the Azure CLI commands? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

```
az provider register -n Microsoft.KeyVault  
resourcegroup="myResourceGroup"  
az group create --name $resourcegroup --location westus  
keyvault_name=myvaultname$RANDOM
```

az ▼ create \

vm
keyvault
keyvault key
vm encryption

```
--name $keyvault_name \  
--resource-group $resourcegroup \  
--location eastus \  
--enabled-for-disk-encryption True
```

az ▼ create \

vm
keyvault
keyvault key
vm encryption

```
--vault-name $keyvault_name \  
--name Name1 \  
--protection software
```

az ▼ create \

vm
keyvault
keyvault key
vm encryption

```
--resource-group $resourcegroup \  
--name Name2 \  
--image Canonical:UbuntuServer:16.04-LTS:latest \  
--admin-username azureuser \  
--generate-ssh-keys \  
--data-disk-sizes-gb 5
```

az ▼ enable\

vm
keyvault
keyvault key
vm encryption

```
--resource-group $resourcegroup \  
--name Name2 \  
--disk-encryption-keyvault $keyvault_name \  
--key-encryption-key Name1 \  
--volume-type
```

▼

all
data
os

Answer Area:


Answer Area

```
az provider register -n Microsoft.KeyVault  
resourcegroup="myResourceGroup"  
az group create --name $resourcegroup --location westus  
keyvault_name=myvaultname$RANDOM
```

```
az  create \
```

vm
keyvault
keyvault key
vm encryption

```
--name $keyvault_name \  
--resource-group $resourcegroup \  
--location eastus \  
--enabled-for-disk-encryption True
```

```
az  create \
```

vm
keyvault
keyvault key
vm encryption

```
--vault-name $keyvault_name \  
--name Name1 \  
--protection software
```


```
az  create \
```

vm
keyvault
keyvault key
vm encryption

```
--resource-group $resourcegroup \  
--name Name2 \  
--image Canonical:UbuntuServer:16.04-LTS:latest \  
--admin-username azureuser \  
--generate-ssh-keys \  
--data-disk-sizes-gb 5
```

```
az  enable\
```

vm
keyvault
keyvault key
vm encryption

```
--resource-group $resourcegroup \  
--name Name2 \  
--disk-encryption-keyvault $keyvault_name \  
--key-encryption-key Name1 \  
--volume-type 
```

all
data
os

Section:**Explanation:**

Box 1: keyvault

Create an Azure Key Vault with az keyvault create and enable the Key Vault for use with disk encryption. Specify a unique Key Vault name for keyvault_name as follows:

```
keyvault_name=myvaultname$RANDOM
```

```
az keyvault create \  
--name $keyvault_name \  
--resource-group $resourcegroup \  
--location eastus \  
--enabled-for-disk-encryption True
```

Box 2: keyvault key

The Azure platform needs to be granted access to request the cryptographic keys when the VM boots to decrypt the virtual disks. Create a cryptographic key in your Key Vault with az keyvault key create. The following example creates a key named myKey:

```
az keyvault key create \  
--vault-name $keyvault_name \  
--name myKey \  
--protection software
```

Box 3: vm

Create a VM with az vm create. Only certain marketplace images support disk encryption. The following example creates a VM named myVM using an Ubuntu 16.04 LTS image:

```
az vm create \  
--resource-group $resourcegroup \  
--name myVM \  
--image Canonical:UbuntuServer:16.04-LTS:latest \  
--admin-username azureuser \  
--generate-ssh-keys \
```

Box 4: vm encryption

Encrypt your VM with az vm encryption enable:

```
az vm encryption enable \  
--resource-group $resourcegroup \  
--name myVM \  
--disk-encryption-keyvault $keyvault_name \  
--key-encryption-key myKey \  
--volume-type all
```

Note: seems to an error in the question. Should have enable instead of create.

Box 5: all

Encrypt both data and operating system.

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-machines/linux/disk-encryption-cli-quickstart>

QUESTION 26

Your company is developing an Azure API hosted in Azure.

You need to implement authentication for the Azure API to access other Azure resources. You have the following requirements:

All API calls must be authenticated.

Callers to the API must not send credentials to the API.

Which authentication mechanism should you use?

- A. Basic
- B. Anonymous
- C. Managed identity

D. Client certificate

Correct Answer: C

Section:

Explanation:

Azure Active Directory Managed Service Identity (MSI) gives your code an automatically managed identity for authenticating to Azure services, so that you can keep credentials out of your code.

Note: Use the authentication-managed-identity policy to authenticate with a backend service using the managed identity. This policy essentially uses the managed identity to obtain an access token from Azure Active Directory for accessing the specified resource. After successfully obtaining the token, the policy will set the value of the token in the Authorization header using the Bearer scheme.

Incorrect Answers:

A: Use the authentication-basic policy to authenticate with a backend service using Basic authentication. This policy effectively sets the HTTP Authorization header to the value corresponding to the credentials provided in the policy.

B: Anonymous is no authentication at all.

D: Your code needs credentials to authenticate to cloud services, but you want to limit the visibility of those credentials as much as possible. Ideally, they never appear on a developer's workstation or get checked-in to source control. Azure Key Vault can store credentials securely so they aren't in your code, but to retrieve them you need to authenticate to Azure Key Vault. To authenticate to Key Vault, you need a credential! A classic bootstrap problem.

Reference:

<https://azure.microsoft.com/en-us/blog/keep-credentials-out-of-code-introducing-azure-ad-managed-service-identity/>

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

QUESTION 27

HOTSPOT

You are building a website that is used to review restaurants. The website will use an Azure CDN to improve performance and add functionality to requests.

You build and deploy a mobile app for Apple iPhones. Whenever a user accesses the website from an iPhone, the user must be redirected to the app store.

You need to implement an Azure CDN rule that ensures that iPhone users are redirected to the app store.

How should you complete the Azure Resource Manager template? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

```
"conditions": [ {  
  "name": "IsDevice",  
  "parameters": {  
    "@odata.type": "#Microsoft.Azure.Cdn.Models.",  
    "operator": "Equal"  
    "matchValues": [ "  " ]  
  } },  
  {  
    "name": "RequestHeader",  
    "parameters": {  
      "@odata.type": "#Microsoft.Azure.Cdn.Models.",  
      "operator": "Contains",  
      "selector": "  ",  
      "matchValues": [ "  " ]  
    } }  
  ]  
}
```

DeliveryRuleDeviceConditionParameters
DeliveryRuleCookiesConditionParameters
DeliveryRulePostArgsConditionParameters
DeliveryRuleRequestHeaderConditionParameters

FROM
PRAGMA
X-POWERED-BY
HTTP_USER_AGENT

iOS
Mobile
iPhone
Desktop

Answer Area:

Answer Area

```
"conditions": [ {  
  "name": "IsDevice",  
  "parameters": {  
    "@odata.type": "#Microsoft.Azure.Cdn.Models.  
    "operator": "Equal"  
    "matchValues": [ "   
  } },  
  {  
    "name": "RequestHeader",  
    "parameters": {  
      "@odata.type": "#Microsoft.Azure.Cdn.Models.  
      "operator": "Contains",  
      "selector": "  
    "matchValues": [ "   
  } }  
]
```

iOS
Mobile
iPhone
Desktop

DeliveryRuleIsDeviceConditionParameters
DeliveryRuleCookiesConditionParameters
DeliveryRulePostArgsConditionParameters
DeliveryRuleRequestHeaderConditionParameters

FROM
PRAGMA
X-POWERED-BY
HTTP_USER_AGENT

DeliveryRuleIsDeviceConditionParameters
DeliveryRuleCookiesConditionParameters
DeliveryRulePostArgsConditionParameters
DeliveryRuleRequestHeaderConditionParameters

iOS
Mobile
iPhone
Desktop

Section:

Explanation:

Box 1: iOS

Azure AD Conditional Access supports the following device platforms:

Android

iOS

Windows Phone

Windows

macOS

Box 2: DeliveryRuleIsDeviceConditionParameters

The DeliveryRuleIsDeviceCondition defines the IsDevice condition for the delivery rule. parameters defines the parameters for the condition.

Box 3: HTTP_USER_AGENT

Incorrect Answers:

The Pragma HTTP/1.0 general header is an implementation-specific header that may have various effects along the request-response chain. It is used for backwards compatibility with HTTP/1.0 caches.

"X-Powered-By" is a common non-standard HTTP response header (most headers prefixed with an 'X-' are non-standard).

Box 4: DeliveryRuleRequestHeaderConditionParameters

DeliveryRuleRequestHeaderCondition defines the RequestHeader condition for the delivery rule. parameters defines the parameters for the condition.

Box 5: iOS

The Require approved client app requirement only supports the iOS and Android for device platform condition.

Reference:

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

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

QUESTION 28

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

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

You are developing a website that will run as an Azure Web App. Users will authenticate by using their Azure Active Directory (Azure AD) credentials.

You plan to assign users one of the following permission levels for the website: admin, normal, and reader. A user's Azure AD group membership must be used to determine the permission level.

You need to configure authorization.

Solution:

Configure and use Integrated Windows Authentication in the website.

In the website, query Microsoft Graph API to load the group to which the user is a member.

Does the solution meet the goal?

A. Yes

B. No

Correct Answer: B

Section:

Explanation:

Microsoft Graph is a RESTful web API that enables you to access Microsoft Cloud service resources.

Instead in the Azure AD application's manifest, set value of the groupMembershipClaims option to All. In the website, use the value of the groups claim from the JWT for the user to determine permissions.

Reference:

<https://blogs.msdn.microsoft.com/waws/2017/03/13/azure-app-service-authentication-aad-groups/>

QUESTION 29

DRAG DROP

You are developing an Azure solution.

You need to develop code to access a secret stored in Azure Key Vault.

How should you complete the code segment? To answer, drag the appropriate code segments to the correct locations. Each code segment 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:

Code segments

DefaultAzureCredential

ClientSecretCredential

CloudClients

SecretClient

Answer Area

```

string var1 = Environment.GetEnvironmentVariable("KEY_VAULT_URI");
var var2 = new Code segment ( new Uri(var1), new Code segment ());

```

Correct Answer:

Code segments

ClientSecretCredential

CloudClients

Answer Area

```

string var1 = Environment.GetEnvironmentVariable("KEY_VAULT_URI");
var var2 = new SecretClient ( new Uri(var1), new DefaultAzureCredential ());

```

Section:

Explanation:

Box 1: SecretClient

Box 2: DefaultAzureCredential

In below example, the name of your key vault is expanded to the key vault URI, in the format "https://<your-key-vault-name>.vault.azure.net". This example is using 'DefaultAzureCredential()' class from Azure Identity Library, which allows to use the same code across different environments with different options to provide identity.

```
string keyVaultName = Environment.GetEnvironmentVariable("KEY_VAULT_NAME"); var kvUri = "https://" + keyVaultName + ".vault.azure.net";
```

```
var client = new SecretClient(new Uri(kvUri), new DefaultAzureCredential());
```

Reference:

<https://docs.microsoft.com/en-us/azure/key-vault/secrets/quick-create-net>

QUESTION 30

You are developing an Azure App Service REST API.

The API must be called by an Azure App Service web app. The API must retrieve and update user profile information stored in Azure Active Directory (Azure AD).

You need to configure the API to make the updates.

Which two tools should you use? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Microsoft Graph API
- B. Microsoft Authentication Library (MSAL)
- C. Azure API Management
- D. Microsoft Azure Security Center
- E. Microsoft Azure Key Vault SDK

Correct Answer: A, C

Section:

Explanation:

A: You can use the Azure AD REST APIs in Microsoft Graph to create unique workflows between Azure AD resources and third-party services.

Enterprise developers use Microsoft Graph to integrate Azure AD identity management and other services to automate administrative workflows, such as employee onboarding (and termination), profile maintenance, license deployment, and more.

C: API Management (APIM) is a way to create consistent and modern API gateways for existing back-end services.

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

Reference:

<https://docs.microsoft.com/en-us/graph/azuread-identity-access-management-concept-overview>

QUESTION 31

You develop a REST API. You implement a user delegation SAS token to communicate with Azure Blob storage.

The token is compromised.

You need to revoke the token.

What are two possible ways to achieve this goal? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. Revoke the delegation keys
- B. Delete the stored access policy.
- C. Regenerate the account key.
- D. Remove the role assignment for the security principle.

Correct Answer: A, B

Section:

Explanation:

A: Revoke a user delegation SAS

To revoke a user delegation SAS from the Azure CLI, call the az storage account revoke-delegation-keys command. This command revokes all of the user delegation keys associated with the specified storage account. Any shared access signatures associated with those keys are invalidated.

B: To revoke a stored access policy, you can either delete it, or rename it by changing the signed identifier. Changing the signed identifier breaks the associations between any existing signatures and the stored access policy.

Deleting or renaming the stored access policy immediately effects all of the shared access signatures associated with it.

Reference:

<https://github.com/MicrosoftDocs/azure-docs/blob/master/articles/storage/blobs/storage-blob-user-delegation-sas-create-cli.md>

<https://docs.microsoft.com/en-us/rest/api/storageservices/define-stored-access-policy#modifying-or-revoking-a-stored-access-policy>

QUESTION 32

DRAG DROP

You are developing an Azure-hosted application that must use an on-premises hardware security module (HSM) key.

The key must be transferred to your existing Azure Key Vault by using the Bring Your Own Key (BYOK) process.

You need to securely transfer the key to Azure Key Vault.

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

Select and Place:

Actions

Generate a key transfer blob file by using the HSM vendor-provided tool.

Generate a Key Exchange Key (KEK).

Create a custom policy definition in Azure Policy.

Run the `az keyvault key import` Command.

Run the `az keyvault key restore` command.

Retrieve the Key Exchange Key (KEK) public key.

Answer Area

Correct Answer:

Actions

Create a custom policy definition in Azure Policy.

Run the `az keyvault key restore` command.

Answer Area

Generate a Key Exchange Key (KEK).

Retrieve the Key Exchange Key (KEK) public key.

Generate a key transfer blob file by using the HSM vendor-provided tool.

Run the `az keyvault key import` command.

Section:

Explanation:

To perform a key transfer, a user performs following steps:

Generate KEK.

Retrieve the public key of the KEK.

Using HSM vendor provided BYOK tool - Import the KEK into the target HSM and exports the Target Key protected by the KEK.

Import the protected Target Key to Azure Key Vault.

Step 1: Generate a Key Exchange Key (KEK).

Step 2: Retrieve the Key Exchange Key (KEK) public key.

Step 3: Generate a key transfer blob file by using the HSM vendor-provided tool.

Generate key transfer blob using HSM vendor provided BYOK tool

Step 4: Run the `az keyvault key import` command

Upload key transfer blob to import HSM-key.

Customer will transfer the Key Transfer Blob (".byok" file) to an online workstation and then run a `az keyvault key import` command to import this blob as a new HSM-backed key into Key Vault.

To import an RSA key use this command:

`az keyvault key import`

Reference:

<https://docs.microsoft.com/en-us/azure/key-vault/keys/byok-specification>

QUESTION 33

You develop and deploy an Azure Logic app that calls an Azure Function app. The Azure Function app includes an OpenAPI (Swagger) definition and uses an Azure Blob storage account. All resources are secured by using Azure Active

Directory (Azure AD).

The Azure Logic app must securely access the Azure Blob storage account. Azure AD resources must remain if the Azure Logic app is deleted.

You need to secure the Azure Logic app.

What should you do?

- A. Create a user-assigned managed identity and assign role-based access controls.
- B. Create an Azure AD custom role and assign the role to the Azure Blob storage account.
- C. Create an Azure Key Vault and issue a client certificate.
- D. Create a system-assigned managed identity and issue a client certificate.
- E. Create an Azure AD custom role and assign role-based access controls.

Correct Answer: A

Section:

Explanation:

To give a managed identity access to an Azure resource, you need to add a role to the target resource for that identity.

Note: To easily authenticate access to other resources that are protected by Azure Active Directory (Azure AD) without having to sign in and provide credentials or secrets, your logic app can use a managed identity (formerly known as Managed Service Identity or MSI). Azure manages this identity for you and helps secure your credentials because you don't have to provide or rotate secrets.

If you set up your logic app to use the system-assigned identity or a manually created, user-assigned identity, the function in your logic app can also use that same identity for authentication.

Reference:

<https://docs.microsoft.com/en-us/azure/logic-apps/create-managed-service-identity>

<https://docs.microsoft.com/en-us/azure/api-management/api-management-howto-mutual-certificates-for-clients>

QUESTION 34

HOTSPOT

You are developing an application that uses a premium block blob storage account. You are optimizing costs by automating Azure Blob Storage access tiers.

You apply the following policy rules to the storage account. You must determine the implications of applying the rules to the data. (Line numbers are included for reference only.)

```

01 {
02   "rules":
03   {
04     "name": "agingDataRule",
05     "enabled": true,
06     "type": "Lifecycle",
07     "definition": {
08       "filters": {
09         "blobTypes": [ "blockBlob" ],
10         "prefixMatch": [ "container1/salesorders", "container2/inventory" ]
11       },
12       "actions": {
13         "baseBlob": {
14           "tierToCool": { "daysAfterModificationGreaterThan": 60 },
15           "tierToArchive": { "daysAfterModificationGreaterThan": 120 }
16         }
17       }
18     },
19   },
20   {
21     "enabled": true,
22     "name": "lastAccessedDataRule",
23     "type": "Lifecycle",
24     "definition": {
25       "actions": {
26         "baseBlob": {
27           "enableAutoTierToHotFromCool": true,
28           "tierToCool": {
29             "daysAfterLastAccessTimeGreaterThan": 30
30           }
31         }
32       },
33       "filters": {
34         "blobTypes": [ "blockBlob" ]
35       }
36     },
37   },
38   {
39     "rules": [
40       {
41         "name": "expirationDataRule",
42         "enabled": true,
43         "type": "Lifecycle",
44         "definition": {
45           "filters": {
46             "blobTypes": [ "blockBlob" ]
47           },
48           "actions": {
49             "baseBlob": {
50               "delete": { "daysAfterModificationGreaterThan": 730 }
51             }
52           }
53         }
54       }
55     ]
56   }
57 ]
58 }

```

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		
	Yes	No
Block blobs prefixed with container1/salesorders or container2/inventory which have not been modified in over 60 days are moved to cool storage. Blobs that have not been modified in 120 days are moved to the archive tier.	<input type="radio"/>	<input type="radio"/>
Blobs are moved to cool storage if they have not been accessed for 30 days.	<input type="radio"/>	<input type="radio"/>
Blobs will automatically be tiered from cool back to hot if accessed again after being tiered to cool.	<input type="radio"/>	<input type="radio"/>
All block blobs older than 730 days will be deleted.	<input type="radio"/>	<input type="radio"/>

Answer Area:

Answer Area		
	Yes	No
Block blobs prefixed with container1/salesorders or container2/inventory which have not been modified in over 60 days are moved to cool storage. Blobs that have not been modified in 120 days are moved to the archive tier.	<input checked="" type="radio"/>	<input type="radio"/>
Blobs are moved to cool storage if they have not been accessed for 30 days.	<input checked="" type="radio"/>	<input type="radio"/>
Blobs will automatically be tiered from cool back to hot if accessed again after being tiered to cool.	<input checked="" type="radio"/>	<input type="radio"/>
All block blobs older than 730 days will be deleted.	<input checked="" type="radio"/>	<input type="radio"/>

Section:

Explanation:

Box 1: Yes

```

"rules":
{
  "name": "agingDataRule",
  "enabled": true,
  "type": "Lifecycle",
  "definition": {
    "filters": {
      "blobTypes": [ "blockBlob" ],
      "prefixMatch": [ "container1/salesorders", "container2/inventory" ]
    },
    "actions": {
      "baseBlob": {
        "tierToCool": { "daysAfterModificationGreaterThan": 60 },
        "tierToArchive": { "daysAfterModificationGreaterThan": 120 }
      }
    }
  }
}

```

Box 2: Yes

```

"enabled": true,
"name": "lastAccessedDataRule",
"type": "Lifecycle",
"definition": {
  "actions": {
    "baseBlob": {
      "enableAutoTierToHotFromCool": true,
      "tierToCool": {
        "daysAfterLastAccessTimeGreaterThan": 30
      }
    }
  }
}

```

Box 3: Yes

Box 4: Yes

```

"rules": [
{
  "name": "expirationDataRule",
  "enabled": true,
  "type": "Lifecycle",
  "definition": {
    "filters": {
      "blobTypes": [ "blockBlob" ]
    },
    "actions": {
      "baseBlob": {
        "delete": { "daysAfterModificationGreaterThan": 730 }
      }
    }
  }
}
]

```

QUESTION 35

You are developing a solution that will use a multi-partitioned Azure Cosmos DB database. You plan to use the latest Azure Cosmos DB SDK for development.

The solution must meet the following requirements:

Send insert and update operations to an Azure Blob storage account.

Process changes to all partitions immediately.

Allow parallelization of change processing.

You need to process the Azure Cosmos DB operations.

What are two possible ways to achieve this goal? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. Create an Azure App Service API and implement the change feed estimator of the SDK. Scale the API by using multiple Azure App Service instances.
- B. Create a background job in an Azure Kubernetes Service and implement the change feed feature of the SDK.
- C. Create an Azure Function to use a trigger for Azure Cosmos DB. Configure the trigger to connect to the container.
- D. Create an Azure Function that uses a FeedIterator object that processes the change feed by using the pull model on the container. Use a FeedRange object to parallelize the processing of the change feed across multiple functions.

Correct Answer: C

Section:

Explanation:

Azure Functions is the simplest option if you are just getting started using the change feed. Due to its simplicity, it is also the recommended option for most change feed use cases. When you create an Azure Functions trigger for Azure Cosmos DB, you select the container to connect, and the Azure Function gets triggered whenever there is a change in the container. Because Azure Functions uses the change feed processor behind the scenes, it automatically parallelizes change processing across your container's partitions.

Note: You can work with change feed using the following options:

Using change feed with Azure Functions

Using change feed with change feed processor

Reference:

<https://docs.microsoft.com/en-us/azure/cosmos-db/read-change-feed>

QUESTION 36

HOTSPOT

You have an Azure Web app that uses Cosmos DB as a data store. You create a CosmosDB container by running the following PowerShell script:

```
$resourceGroupName = "testResourceGroup"
```

```
$accountName = "testCosmosAccount"
```

```
$databaseName = "testDatabase"
```

```
$containerName = "testContainer"
```

```
$partitionKeyPath = "/EmployeeId"
```

```
$autoscaleMaxThroughput = 5000
```

```
New-AzCosmosDBSqlContainer
```

```
-ResourceGroupName $resourceGroupName
```

```
-AccountName $accountName
```

```
-DatabaseName $databaseName
```

```
-Name $containerName
```

```
-PartitionKeyKind Hash
```

```
-PartitionKeyPath $partitionKeyPath
```

```
-AutoscaleMaxThroughput $autoscaleMaxThroughput
```

You create the following queries that target the container:

```
SELECT * FROM c WHERE c.EmployeeId > '12345'
```

```
SELECT * FROM c WHERE c.UserID = '12345'
```

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		
	Yes	No
The minimum throughput for the container is 400 R/Us.	<input type="radio"/>	<input type="radio"/>
The first query statement is an in-partition query.	<input type="radio"/>	<input type="radio"/>
The second query statement is a cross-partition query.	<input type="radio"/>	<input type="radio"/>

Answer Area:

Answer Area	Yes	No
The minimum throughput for the container is 400 R/Us.	<input type="radio"/>	<input checked="" type="radio"/>
The first query statement is an in-partition query.	<input type="radio"/>	<input checked="" type="radio"/>
The second query statement is a cross-partition query.	<input checked="" type="radio"/>	<input type="radio"/>

Section:

Explanation:

Box 1: No You set the highest, or maximum RU/s Tmax you don't want the system to exceed. The system automatically scales the throughput T such that $0.1 * Tmax \leq T \leq Tmax$.

In this example we have autoscaleMaxThroughput = 5000, so the minimum throughput for the container is 500 R/Us.

Box 2: No

First query: `SELECT * FROM c WHERE c.EmployeeId > '12345'`

Here's a query that has a range filter on the partition key and won't be scoped to a single physical partition. In order to be an in-partition query, the query must have an equality filter that includes the partition key:

`SELECT * FROM c WHERE c.DeviceId = 'XMS-0001'`

Box 3: Yes

Example of In-partition query:

Consider the below query with an equality filter on DeviceId. If we run this query on a container partitioned on DeviceId, this query will filter to a single physical partition.

`SELECT * FROM c WHERE c.DeviceId = 'XMS-0001'`

Reference:

<https://docs.microsoft.com/en-us/azure/cosmos-db/how-to-choose-offer>

<https://docs.microsoft.com/en-us/azure/cosmos-db/how-to-query-container>

QUESTION 37

HOTSPOT

You are developing a web application that makes calls to the Microsoft Graph API. You register the application in the Azure portal and upload a valid X509 certificate.

You create an appsettings.json file containing the certificate name, client identifier for the application, and the tenant identifier of the Azure Active Directory (Azure AD). You create a method named ReadCertificate to return the X509 certificate by name.

You need to implement code that acquires a token by using the certificate.

How should you complete the code segment? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

```
AuthenticationConfig config = AuthenticationConfig.ReadFromJsonFile("appsettings.json");
X509Certificate2 certificate = ReadCertificate(config.CertificateName);
var app = ConfidentialClientApplicationBuilder
    .Create(config.ClientId)
    .WithCertificate(certificate)
    .WithAuthority(new Uri(config.Authority))
    .Build();
string[] scopes = new string[] { $"{config.ApiUrl}.default" };
AuthenticationResult result = await app.AcquireTokenForClient(
    scopes
    app
    config
    ).ExecuteAsync();
```

Answer Area:

Answer Area

```
AuthenticationConfig config = AuthenticationConfig.ReadFromJsonFile("appsettings.json");
X509Certificate2 certificate = ReadCertificate(config.CertificateName);
var app = ConfidentialClientApplicationBuilder
    .Create(config.ClientId)
    .WithCertificate(certificate)
    .WithAuthority(new Uri(config.Authority))
    .Build();
string[] scopes = new string[] { $"{config.ApiUrl}.default" };
AuthenticationResult result = await app.AcquireTokenForClient(
    scopes
    app
    config
    ).ExecuteAsync();
```

Section:

Explanation:

Box 1: ConfidentialClientApplicationBuilder

Here's the code to instantiate the confidential client application with a client secret:

```
app = ConfidentialClientApplicationBuilder.Create(config.ClientId)
```

```
.WithClientSecret(config.ClientSecret)
.WithAuthority(new Uri(config.Authority))
.Build();
```

Box 2: scopes

After you've constructed a confidential client application, you can acquire a token for the app by calling `AcquireTokenForClient`, passing the scope, and optionally forcing a refresh of the token.

Sample code: `result = await app.AcquireTokenForClient(scopes)`

```
.ExecuteAsync();
```

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/develop/scenario-daemon-app-configuration>

<https://docs.microsoft.com/en-us/azure/active-directory/develop/scenario-daemon-acquire-token>

QUESTION 38

HOTSPOT

You develop a containerized application. You plan to deploy the application to a new Azure Container instance by using a third-party continuous integration and continuous delivery (CI/CD) utility.

The deployment must be unattended and include all application assets. The third-party utility must only be able to push and pull images from the registry. The authentication must be managed by Azure Active Directory (Azure AD). The solution must use the principle of least privilege.

You need to ensure that the third-party utility can access the registry.

Which authentication options 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

Authentication	Option
Registry authentication method	<div><div></div><div>Service principal</div><div>Individual identity</div><div>Repository-scoped access token</div><div>Managed identity for Azure resources</div></div>
RBAC role	<div><div></div><div>AcrPull</div><div>Owner</div><div>AcrPush</div><div>Contributor</div></div>

Answer Area:

Answer Area	
Authentication	Option
Registry authentication method	<div>Service principal</div> <div>Individual identity</div> <div>Repository-scoped access token</div> <div>Managed identity for Azure resources</div>
RBAC role	<div>AcrPull</div> <div>Owner</div> <div>AcrPush</div> <div>Contributor</div>

Section:

Explanation:

Box 1: Service principal Applications and container orchestrators can perform unattended, or "headless," authentication by using an Azure Active Directory (Azure AD) service principal.

Incorrect Answers:

Individual AD identity does not support unattended push/pull

Repository-scoped access token is not integrated with AD identity

Managed identity for Azure resources is used to authenticate to an Azure container registry from another Azure resource.

Box 2: AcrPush

AcrPush provides pull/push permissions only and meets the principle of least privilege.

Incorrect Answers:

AcrPull only allows pull permissions it does not allow push permissions.

Owner and Contributor allow pull/push permissions but does not meet the principle of least privilege.

Reference:

<https://docs.microsoft.com/en-us/azure/container-registry/container-registry-authentication?tabs=azure-cli>

<https://docs.microsoft.com/en-us/azure/container-registry/container-registry-roles?tabs=azure-cli>

QUESTION 39

You deploy an Azure App Service web app. You create an app registration for the app in Azure Active Directory (Azure AD) and Twitter.

The app must authenticate users and must use SSL for all communications. The app must use Twitter as the identity provider.

You need to validate the Azure AD request in the app code.

What should you validate?

- A. ID token header
- B. ID token signature
- C. HTTP response code

D. Tenant ID

Correct Answer: A

Section:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/storage/common/storage-auth-aad-app?tabs=dotnet>

QUESTION 40

A development team is creating a new REST API. The API will store data in Azure Blob storage. You plan to deploy the API to Azure App Service.

Developers must access the Azure Blob storage account to develop the API for the next two months. The Azure Blob storage account must not be accessible by the developers after the two-month time period.

You need to grant developers access to the Azure Blob storage account.

What should you do?

- A. Generate a shared access signature (SAS) for the Azure Blob storage account and provide the SAS to all developers.
- B. Create and apply a new lifecycle management policy to include a last accessed date value. Apply the policy to the Azure Blob storage account.
- C. Provide all developers with the access key for the Azure Blob storage account. Update the API to include the Coordinated Universal Time (UTC) timestamp for the request header.
- D. Grant all developers access to the Azure Blob storage account by assigning role-based access control (RBAC) roles.

Correct Answer: A

Section:

Explanation:

Reference:

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

QUESTION 41

DRAG DROP

An organization plans to deploy Azure storage services.

You need to configure shared access signature (SAS) for granting access to Azure Storage.

Which SAS types should you use? To answer, drag the appropriate SAS types to the correct requirements. Each SAS 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:

SAS types

Account-level
Service-level
User delegation

Answer Area

Requirement

- Delegate access to resources in one or more of the storage services
- Delegate access to a resource in a single storage service
- Secure a resource by using Azure AD credentials

SAS type

Correct Answer:

SAS types

Answer Area

Requirement

- Delegate access to resources in one or more of the storage services
- Delegate access to a resource in a single storage service
- Secure a resource by using Azure AD credentials

SAS type

Account-level
Service-level
User delegation

Section:

Explanation:

Reference:

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

01 - Monitor troubleshoot and optimize Azure solutions

Case study

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

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

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

To start the case study

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such

as business requirements, existing environment, and problem statements. When you are ready to answer a question, click the Question button to return to the question.

Background

Overview

You are a developer for Contoso, Ltd. The company has a social networking website that is developed as a Single Page Application (SPA). The main web application for the social networking website loads user uploaded content from blob storage.

You are developing a solution to monitor uploaded data for inappropriate content. The following process occurs when users upload content by using the SPA:

- Messages are sent to ContentUploadService.
- Content is processed by ContentAnalysisService.
- After processing is complete, the content is posted to the social network or a rejection message is posted in its place.

The ContentAnalysisService is deployed with Azure Container Instances from a private Azure Container Registry named contosoimages.

The solution will use eight CPU cores.

Azure Active Directory

Contoso, Ltd. uses Azure Active Directory (Azure AD) for both internal and guest accounts.

Requirements

ContentAnalysisService

```
CS01 apiVersion: '2018-10-01'
CS02 type: Microsoft.ContainerInstance/containerGroups
CS03 location: westus
CS04 name: contentUploadService
CS05 properties:
CS06   containers:
CS07   - name: service
CS08     properties:
CS09       image: contoso/contentUploadService:latest
CS10       ports:
CS11       - port: 80
CS12         protocol: TCP
CS13       resources:
CS14         requests:
CS15           cpu: 1.0
CS16           memoryInGB: 1.5
CS17
CS18 ipAddress:
CS19   ip: 10.23.121.112
CS20   ports:
CS21   - port: 80
CS22     protocol: TCP
CS23
CS24
CS25 networkProfile:
CS26   id: /subscriptions/98...19/resourceGroups/container/providers/Microsoft.Network/networkProfiles/subnet
```

```

AM01 {
AM02     "id" : "2b079f03-9b06-2d44-98bb-e9182901fcb6",
AM03     "appId" : "7118a7f0-b5c2-4c9d-833c-3d711396fe65",
AM04
AM05     "createdDateTime" : "2019-12-24T06:01:44Z",
AM06     "logoUrl" : null,
AM07     "logoutUrl" : null,
AM08     "name" : "ContentAnalysisService",
AM09
AM10
AM11     "orgRestrictions" : [],
AM12     "parentalControlSettings" : {
AM13         "countriesBlockedForMinors" : [],
AM14         "legalAgeGroupRule" : "Allow",
AM15     },
AM16     "passwordCredentials" : []
AM17 }

```

The company's data science group built ContentAnalysisService which accepts user generated content as a string and returns a probable value for inappropriate content. Any values over a specific threshold must be reviewed by an employee of Contoso, Ltd.

You must create an Azure Function named CheckUserContent to perform the content checks.

Costs

You must minimize costs for all Azure services.

Manual review

To review content, the user must authenticate to the website portion of the ContentAnalysisService using their Azure AD credentials. The website is built using React and all pages and API endpoints require authentication. In order to review content a user must be part of a ContentReviewer role. All completed reviews must include the reviewer's email address for auditing purposes.

High availability

All services must run in multiple regions. The failure of any service in a region must not impact overall application availability.

Monitoring

An alert must be raised if the ContentUploadService uses more than 80 percent of available CPU cores.

Security

You have the following security requirements:

Any web service accessible over the Internet must be protected from cross site scripting attacks.

All websites and services must use SSL from a valid root certificate authority.

Azure Storage access keys must only be stored in memory and must be available only to the service.

All Internal services must only be accessible from internal Virtual Networks (VNETs).

All parts of the system must support inbound and outbound traffic restrictions.

All service calls must be authenticated by using Azure AD.

User agreements

When a user submits content, they must agree to a user agreement. The agreement allows employees of Contoso, Ltd. to review content, store cookies on user devices, and track user's IP addresses.

Information regarding agreements is used by multiple divisions within Contoso, Ltd.

User responses must not be lost and must be available to all parties regardless of individual service uptime. The volume of agreements is expected to be in the millions per hour.

Validation testing

When a new version of the ContentAnalysisService is available the previous seven days of content must be processed with the new version to verify that the new version does not significantly deviate from the old version.

Issues

Users of the ContentUploadService report that they occasionally see HTTP 502 responses on specific pages.

Code

ContentUploadService

QUESTION 1

You need to monitor ContentUploadService according to the requirements.
Which command should you use?

- A. az monitor metrics alert create -n alert -g ... - -scopes ... - -condition "avg Percentage CPU > 8"
- B. az monitor metrics alert create -n alert -g ... - -scopes ... - -condition "avg Percentage CPU > 800"
- C. az monitor metrics alert create -n alert -g ... - -scopes ... - -condition "CPU Usage > 800"
- D. az monitor metrics alert create -n alert -g ... - -scopes ... - -condition "CPU Usage > 8"

Correct Answer: B

Section:

Explanation:

Scenario: An alert must be raised if the ContentUploadService uses more than 80 percent of available CPU cores

Reference:

<https://docs.microsoft.com/sv-se/cli/azure/monitor/metrics/alert>

QUESTION 2

You need to investigate the http server log output to resolve the issue with the ContentUploadService.
Which command should you use first?

- A. az webapp log
- B. az ams live-output
- C. az monitor activity-log
- D. az container attach

Correct Answer: C

Section:

Explanation:

Scenario: Users of the ContentUploadService report that they occasionally see HTTP 502 responses on specific pages.

"502 bad gateway" and "503 service unavailable" are common errors in your app hosted in Azure App Service.

Microsoft Azure publicizes each time there is a service interruption or performance degradation.

The az monitor activity-log command manages activity logs.

Note: Troubleshooting can be divided into three distinct tasks, in sequential order:

1. Observe and monitor application behavior
2. Collect data
3. Mitigate the issue

Reference:

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

02 - Monitor troubleshoot and optimize Azure solutions

Case study

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

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

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

To start the case study

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. When you are ready to answer a question, click the Question button to return to the question.

Background

City Power & Light company provides electrical infrastructure monitoring solutions for homes and businesses. The company is migrating solutions to Azure.

Current environment

Architecture overview

The company has a public website located at <http://www.cpandl.com/>. The site is a single-page web application that runs in Azure App Service on Linux. The website uses files stored in Azure Storage and cached in Azure Content Delivery Network (CDN) to serve static content.

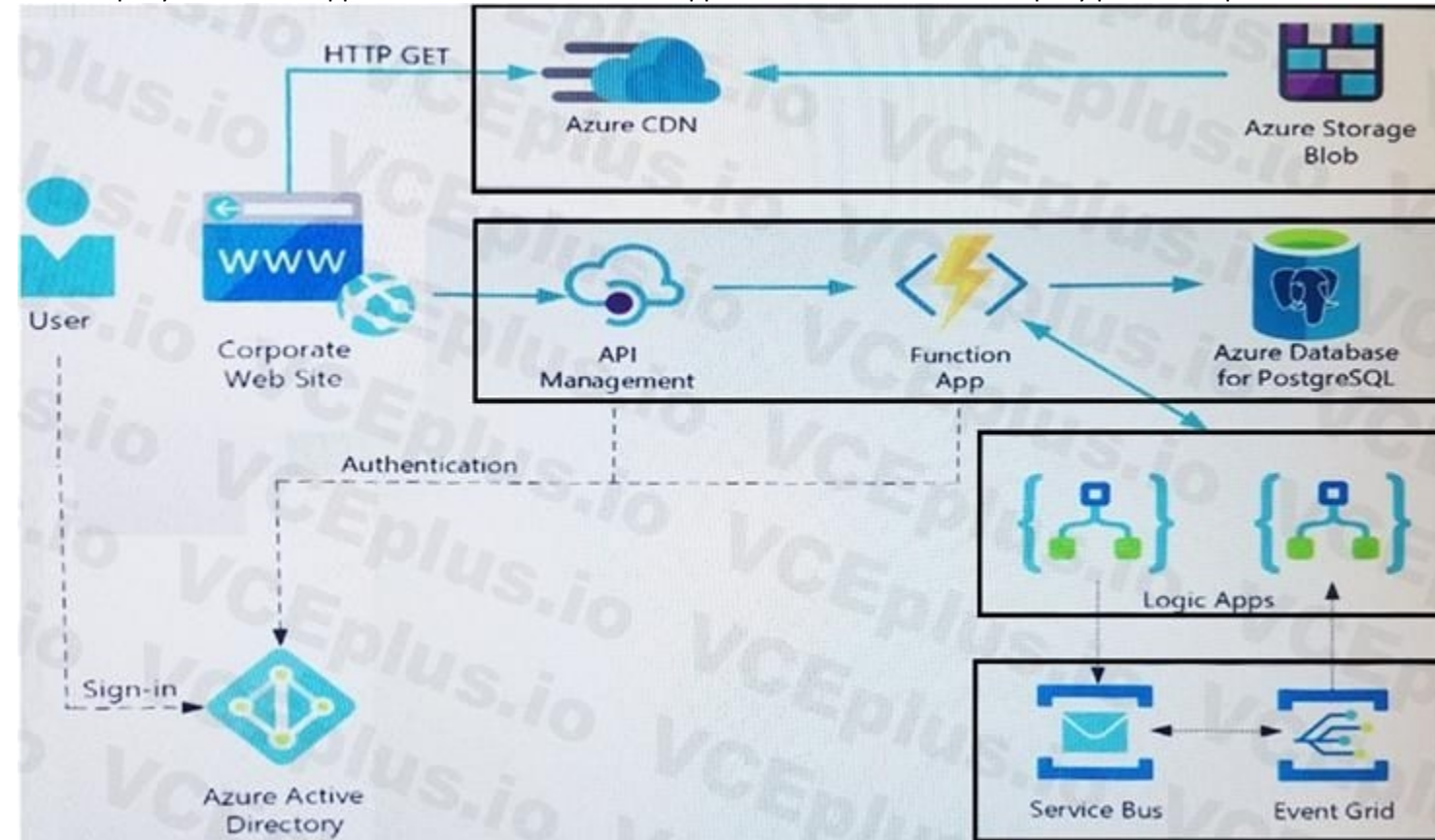
API Management and Azure Function App functions are used to process and store data in Azure Database for PostgreSQL. API Management is used to broker communications to the Azure Function app functions for Logic app integration.

Logic apps are used to orchestrate the data processing while Service Bus and Event Grid handle messaging and events.

The solution uses Application Insights, Azure Monitor, and Azure Key Vault.

Architecture diagram

The company has several applications and services that support their business. The company plans to implement serverless computing where possible. The overall architecture is shown below.



User authentication

The following steps detail the user authentication process:

The user selects Sign in in the website.

The browser redirects the user to the Azure Active Directory (Azure AD) sign in page.

The user signs in.

Azure AD redirects the user's session back to the web application. The URL includes an access token.

The web application calls an API and includes the access token in the authentication header. The application ID is sent as the audience ('aud') claim in the access token.

The back-end API validates the access token.

Requirements

Corporate website

Communications and content must be secured by using SSL.

Communications must use HTTPS.

Data must be replicated to a secondary region and three availability zones.

Data storage costs must be minimized.

Azure Database for PostgreSQL

The database connection string is stored in Azure Key Vault with the following attributes:

Azure Key Vault name: cpandlkeyvault

Secret name: PostgreSQLConn

Id: 80df3e46ffcd4f1cb187f79905e9a1e8

The connection information is updated frequently. The application must always use the latest information to connect to the database.

Azure Service Bus and Azure Event Grid

Azure Event Grid must use Azure Service Bus for queue-based load leveling.

Events in Azure Event Grid must be routed directly to Service Bus queues for use in buffering.

Events from Azure Service Bus and other Azure services must continue to be routed to Azure Event Grid for processing.

Security

All SSL certificates and credentials must be stored in Azure Key Vault.

File access must restrict access by IP, protocol, and Azure AD rights.

All user accounts and processes must receive only those privileges which are essential to perform their intended function.

Compliance

Auditing of the file updates and transfers must be enabled to comply with General Data Protection Regulation (GDPR). The file updates must be read-only, stored in the order in which they occurred, include only create, update, delete, and copy operations, and be retained for compliance reasons.

Issues

Corporate website

While testing the site, the following error message displays:

CryptographicException: The system cannot find the file specified.

Function app

You perform local testing for the RequestUserApproval function. The following error message displays:

'Timeout value of 00:10:00 exceeded by function: RequestUserApproval'

The same error message displays when you test the function in an Azure development environment when you run the following Kusto query:

FunctionAppLogs

| where FunctionName == "RequestUserApproval"

Logic app

You test the Logic app in a development environment. The following error message displays:

'400 Bad Request'

Troubleshooting of the error shows an HttpTrigger action to call the RequestUserApproval function.

Code

Corporate website

Security.cs:

```
SC01 public class Security
SC02 {
SC03     var bytes = System.IO.File.ReadAllBytes("~/var/ssl/private");
SC04     var cert = new System.Security.Cryptography.X509Certificate2(bytes);
SC05     var certName = cert.FriendlyName;
SC06 }
```

Function app

RequestUserApproval.cs:

```

RA01 public static class RequestUserApproval
RA02 {
RA03     [FunctionName("RequestUserApproval")]
RA04     public static async Task<IActionResult> Run(
RA05     [HttpTrigger(AuthorizationLevel.Function, "get", "post", Route = null)] HttpRequest req,
RA06     ILogger log)
RA07     {
RA08         log.LogInformation("RequestUserApproval function processed a request.");
RA09         ...
RA10         return ProcessRequest(req)
RA11         ? (ActionResult)new OkObjectResult($"User approval processed")
RA12         : new BadRequestObjectResult("Failed to process user approval");
RA13     }
RA14     private static bool ProcessRequest(HttpRequest req)
RA15     {
RA16         ...
RA17     }

```

QUESTION 1

You need to investigate the Azure Function app error message in the development environment. What should you do?

- A. Connect Live Metrics Stream from Application Insights to the Azure Function app and filter the metrics.
- B. Create a new Azure Log Analytics workspace and instrument the Azure Function app with Application Insights.
- C. Update the Azure Function app with extension methods from Microsoft.Extensions.Logging to log events by using the log instance.
- D. Add a new diagnostic setting to the Azure Function app to send logs to Log Analytics.

Correct Answer: A

Section:

Explanation:

Azure Functions offers built-in integration with Azure Application Insights to monitor functions.

The following areas of Application Insights can be helpful when evaluating the behavior, performance, and errors in your functions:

Live Metrics: View metrics data as it's created in near real-time.

Failures

Performance

Metrics

Reference:

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

QUESTION 2

HOTSPOT

You need to configure security and compliance for the corporate website files.
Which Azure Blob storage settings 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

Action	Setting
Restrict file access	<div>role-based access control (RBAC)</div> <div>managed identity</div> <div>shared access signature (SAS) token</div> <div>connection string</div>
	<div>access tier</div> <div>change feed</div> <div>blob indexer</div> <div>storage account type</div>

Answer Area:

Answer Area	
Action	Setting
Restrict file access	<div>role-based access control (RBAC)</div> <div>managed identity</div> <div>shared access signature (SAS) token</div> <div>connection string</div>
Enable file auditing	<div>access tier</div> <div>change feed</div> <div>blob indexer</div> <div>storage account type</div>

Section:

Explanation:

Box 1: role-based access control (RBAC)

Azure Storage supports authentication and authorization with Azure AD for the Blob and Queue services via Azure role-based access control (Azure RBAC).

Scenario: File access must restrict access by IP, protocol, and Azure AD rights.

Box 2: change feed

The purpose of the change feed is to provide transaction logs of all the changes that occur to the blobs and the blob metadata in your storage account.

The file updates must be read-only, stored in the order in which they occurred, include only create, update, delete, and copy operations, and be retained for compliance reasons.

Reference:

<https://docs.microsoft.com/en-us/azure/cdn/cdn-sas-storage-support>

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

03 - Monitor troubleshoot and optimize Azure solutions

Case study

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

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

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

To start the case study

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. When you are ready to answer a question, click the Question button to return to the question.

Background

You are a developer for Proseware, Inc. You are developing an application that applies a set of governance policies for Proseware's internal services, external services, and applications. The application will also provide a shared library for common functionality.

Requirements

Policy service

You develop and deploy a stateful ASP.NET Core 2.1 web application named Policy service to an Azure App Service Web App. The application reacts to events from Azure Event Grid and performs policy actions based on those events.

The application must include the Event Grid Event ID field in all Application Insights telemetry.

Policy service must use Application Insights to automatically scale with the number of policy actions that it is performing.

Policies

Log policy

All Azure App Service Web Apps must write logs to Azure Blob storage. All log files should be saved to a container named logdrop. Logs must remain in the container for 15 days.

Authentication events

Authentication events are used to monitor users signing in and signing out. All authentication events must be processed by Policy service. Sign outs must be processed as quickly as possible.

PolicyLib

You have a shared library named PolicyLib that contains functionality common to all ASP.NET Core web services and applications. The PolicyLib library must:

Exclude non-user actions from Application Insights telemetry.

Provide methods that allow a web service to scale itself.

Ensure that scaling actions do not disrupt application usage.

Other

Anomaly detection service

You have an anomaly detection service that analyzes log information for anomalies. It is implemented as an Azure Machine Learning model. The model is deployed as a web service. If an anomaly is detected, an Azure Function that emails administrators is called by using an HTTP WebHook.

Health monitoring

All web applications and services have health monitoring at the /health service endpoint.

Issues

Policy loss

When you deploy Policy service, policies may not be applied if they were in the process of being applied during the deployment.

Performance issue

When under heavy load, the anomaly detection service undergoes slowdowns and rejects connections.

Notification latency

Users report that anomaly detection emails can sometimes arrive several minutes after an anomaly is detected.

App code

EventGridController.cs

Relevant portions of the app files are shown below. Line numbers are included for reference only and include a two-character prefix that denotes the specific file to which they belong.

EventGridController.cs

```
EG01 public class EventGridController : Controller
EG02 {
EG03     public static AsyncLocal<string> EventId = new AsyncLocal<string>();
EG04     public IActionResult Process([FromBody] string eventsJson)
EG05     {
EG06         var events = JObject.Parse(eventsJson);
EG07
EG08         foreach (var @event in events)
EG09         {
EG10             EventId.Value = @event["id"].ToString();
EG11             if (@event["topic"].ToString().Contains("providers/Microsoft.Storage"))
EG12             {
EG13                 SendToAnomalyDetectionService(@event["data"]["url"].ToString());
EG14             }
EG15
EG16             {
EG17                 EnsureLogging(@event["subject"].ToString());
EG18             }
EG19         }
EG20         return null;
EG21     }
EG22     private void EnsureLogging(string resource)
EG23     {
EG24         . . .
EG25     }
EG26     private async Task SendToAnomalyDetectionService(string uri)
EG27     {
EG28         var content = GetLogData(uri);
EG29         var scoreRequest = new
EG30         {
EG31             Inputs = new Dictionary<string, List<Dictionary<string, string>>>()
EG32             {
EG33                 {
EG34                     "input1",
EG35                     new List<Dictionary<string, string>>()
EG36                     {
EG37                         new Dictionary<string, string>()
EG38                         {
EG39                             {
EG40                                 "logcontent", content
EG41                             }
EG42                         }
EG43                     }
EG44                 },
EG45             },
EG46             GlobalParameters = new Dictionary<string, string>() { }
EG47         };
EG48         var result = await (new HttpClient()).PostAsJsonAsync("...", scoreRequest);
EG49         var rawModelResult = await result.Content.ReadAsStringAsync();
EG50         var modelResult = JObject.Parse(rawModelResult);
EG51         if (modelResult["notify"].HasValues)
EG52         {
EG53             . . .
EG54         }
EG55     }
```


LoginEvent.cs

Relevant portions of the app files are shown below. Line numbers are included for reference only and include a two-character prefix that denotes the specific file to which they belong.

LoginEvent.cs

```
LE01 public class LoginEvent
LE02 {
LE03
LE04     public string subject { get; set; }
LE05     public DateTime eventTime { get; set; }
LE06     public Dictionary<string, string> data { get; set; }
LE07     public string Serialize()
LE08     {
LE09         return JsonConvert.SerializeObject(this);
LE10     }
LE11 }
```

QUESTION 1

DRAG DROP

You need to implement the Log policy.

How should you complete the Azure Event Grid subscription? To answer, drag the appropriate JSON segments to the correct locations. Each JSON segment may be used once, more than once, or not at all. You may need to drag the split bar between panes to view content.

NOTE: Each correct selection is worth one point.

Select and Place:

Code segment

- All
- WebHook
- EventHub
- subjectEndsWith
- Microsoft.Storage
- subjectBeginsWith
- Microsoft.Storage.BlobCreated

Answer Area

```
{
  "name": "newlogs",
  "properties": {
    "topic": "/subscriptions/. . ./providers/Microsoft.EventGrid/topics/. . .",
    "destination": {
      "endpointType": "code segment" },
    "filter": {
      "code segment": "/blobServices/default/containers/logdrop/",
      "includedEventTypes": [ "code segment" ] },
  },
  "labels": [],
  "eventDeliverySchema": "EventGridSchema"
}
```

Correct Answer:

Code segment

All
EventHub
subjectEndsWith
Mictosoft.Storage

Answer Area

```
{
  "name": "newlogs",
  "properties": {
    "topic": "/subscriptions/. . ./providers/Microsoft.EventGrid/topics/. . .",
    "destination": {
      "endpointType" : " WebHook " },
    "filter": {
      "subjectBeginsWith": "/blobServices/default/containers/logdrop/",
      "includedEventTypes": [ " Microsoft.Storage.BlobCreated " ] },
    },
    "labels": [],
    "eventDeliverySchema": "EventGridSchema"
  }
```

Section:

Explanation:

Box 1:WebHook

Scenario: If an anomaly is detected, an Azure Function that emails administrators is called by using an HTTP WebHook.

endpointType: The type of endpoint for the subscription (webhook/HTTP, Event Hub, or queue).

Box 2: SubjectBeginsWith

Box 3: Microsoft.Storage.BlobCreated

Scenario: Log Policy

All Azure App Service Web Apps must write logs to Azure Blob storage. All log files should be saved to a container named logdrop. Logs must remain in the container for 15 days.

Example subscription schema

```
{
  "properties": {
    "destination": {
      "endpointType": "webhook",
      "properties": {
        "endpointUrl": "https://example.azurewebsites.net/api/HttpTriggerCSharp1?code=VXbGWce53l48Mt8wuotr0GPmyJ/nDT4hgdFj9DpBiRt38qqnm5OFg=="
      }
    },
    "filter": {
      "includedEventTypes": [ "Microsoft.Storage.BlobCreated", "Microsoft.Storage.BlobDeleted" ],
      "subjectBeginsWith": "blobServices/default/containers/mycontainer/log",
      "subjectEndsWith": ".jpg",
      "isSubjectCaseSensitive ": "true"
    }
  }
}
```

Reference:

<https://docs.microsoft.com/en-us/azure/event-grid/subscription-creation-schema>

QUESTION 2

You need to ensure that the solution can meet the scaling requirements for Policy Service.

Which Azure Application Insights data model should you use?

- A. an Application Insights dependency
- B. an Application Insights event

- C. an Application Insights trace
- D. an Application Insights metric

Correct Answer: D

Section:

Explanation:

Application Insights provides three additional data types for custom telemetry:

Trace - used either directly, or through an adapter to implement diagnostics logging using an instrumentation framework that is familiar to you, such as Log4Net or System.Diagnostics.

Event - typically used to capture user interaction with your service, to analyze usage patterns.

Metric - used to report periodic scalar measurements.

Scenario:

Policy service must use Application Insights to automatically scale with the number of policy actions that it is performing.

Reference:

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

QUESTION 3

DRAG DROP

You need to implement telemetry for non-user actions.

How should you complete the Filter class? To answer, drag the appropriate code segments to the correct locations. Each code segment 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:

Code segments

- /health
- /status
- RequestTelemetry
- PageViewTelemetry
- ITelemetryProcessor
- ITelemetryInitializer

Answer Area

```
public class Filter : 
{
    private readonly  _next;
    public (Filter  next)
    {
        _next = next;
    }
    public void Process(ITelemetry item)
    {
        var x = item as  ;
        if (x?.Url.AbsolutePath == "")
        {
            return;
        }
        _next.Process(item);
    }
}
```

Correct Answer:

Code segments

/health

/status

RequestTelemetry

PageViewTelemetry

ITelemetryProcessor

ITelemetryInitializer

Answer Area

```
public class Filter : ITelemetryProcessor
{
    private readonly ITelemetryProcessor _next;
    public (Filter ITelemetryProcessor next)
    {
        _next = next;
    }
    public void Process(ITelemetry item)
    {
        var x = item as RequestTelemetry;
        if (x?.Url.AbsolutePath == "/health" )
        {
            return;
        }
        _next.Process(item);
    }
}
```

Section:

Explanation:

Scenario: Exclude non-user actions from Application Insights telemetry.

Box 1: ITelemetryProcessor To create a filter, implement ITelemetryProcessor. This technique gives you more direct control over what is included or excluded from the telemetry stream.

Box 2: ITelemetryProcessor

Box 3: ITelemetryProcessor

Box 4: RequestTelemetry

Box 5: /health

To filter out an item, just terminate the chain.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-monitor/app/api-filtering-sampling>

QUESTION 4

DRAG DROP

You need to ensure that PolicyLib requirements are met.

How should you complete the code segment? To answer, drag the appropriate code segments to the correct locations. Each code segment 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:

Code segments

Process
Initialize
telemetry.Sequence
ITelemetryProcessor
ITelemetryInitializer
telemetry.Context
EventGridController.EventId.Value
((EventTelemetry)telemetry).Properties["EventId"]

Answer Area

```
public class IncludeEventId :   
{  
    public void  (ITelemetry telemetry)  
    {  
        .Properties["EventId"] =  
        ;  
    }  
}
```

Correct Answer:

Code segments

Process

telemetry.Sequence
ITelemetryProcessor

EventGridController.EventId.Value

Answer Area

```
public class IncludeEventId :   
{  
    public void  (ITelemetry telemetry)  
    {  
        .Properties["EventId"] =  
        ;  
    }  
}
```

Section:

Explanation:

Scenario: You have a shared library named PolicyLib that contains functionality common to all ASP.NET Core web services and applications. The PolicyLib library must:

Exclude non-user actions from Application Insights telemetry.

Provide methods that allow a web service to scale itself.

Ensure that scaling actions do not disrupt application usage.

Box 1: ITelemetryInitializer Use telemetry initializers to define global properties that are sent with all telemetry; and to override selected behavior of the standard telemetry modules.

Box 2: Initialize

Box 3: Telemetry.Context

Box 4: ((EventTelemetry)telemetry).Properties["EventID"]

Reference:

<https://docs.microsoft.com/en-us/azure/azure-monitor/app/api-filtering-sampling>

Exam N

QUESTION 1

You manage a data processing application that receives requests from an Azure Storage queue.

You need to manage access to the queue. You have the following requirements:

Provide other applications access to the Azure queue.

Ensure that you can revoke access to the queue without having to regenerate the storage account keys. Specify access at the queue level and not at the storage account level.

Which type of shared access signature (SAS) should you use?

- A. Service SAS with a stored access policy
- B. Account SAS
- C. User Delegation SAS
- D. Service SAS with ad hoc SAS

Correct Answer: A

Section:

Explanation:

A service SAS is secured with the storage account key. A service SAS delegates access to a resource in only one of the Azure Storage services: Blob storage, Queue storage, Table storage, or Azure Files.

Stored access policies give you the option to revoke permissions for a service SAS without having to regenerate the storage account keys.

Incorrect Answers:

Account SAS: Account SAS is specified at the account level. It is secured with the storage account key. User Delegation SAS: A user delegation SAS applies to Blob storage only. Reference:

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

QUESTION 2

You need to audit the retail store sales transactions.

What are two possible ways to achieve the goal? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. Update the retail store location data upload process to include blob index tags. Create an Azure Function to process the blob index tags and filter by store location.
- B. Process the change feed logs of the Azure Blob storage account by using an Azure Function. Specify a time range for the change feed data.
- C. Enable blob versioning for the storage account. Use an Azure Function to process a list of the blob versions per day.
- D. Process an Azure Storage blob inventory report by using an Azure Function. Create rule filters on the blob inventory report.
- E. Subscribe to blob storage events by using an Azure Function and Azure Event Grid. Filter the events by store location.

Correct Answer: B, E

Section:

Explanation:

Scenario: Audit store sale transaction information nightly to validate data, process sales financials, and reconcile inventory.

"Process the change feed logs of the Azure Blob storage account by using an Azure Function. Specify a time range for the change feed data": Change feed support is well-suited for scenarios that process data based on objects that have changed.

For example, applications can:

Store, audit, and analyze changes to your objects, over any period of time, for security, compliance or intelligence for enterprise data management.

"Subscribe to blob storage events by using an Azure Function and Azure Event Grid. Filter the events by store location":

Azure Storage events allow applications to react to events, such as the creation and deletion of blobs. It does so without the need for complicated code or expensive and inefficient polling services. The best part is you only pay for what you use.

Blob storage events are pushed using Azure Event Grid to subscribers such as Azure Functions, Azure Logic Apps, or even to your own http listener. Event Grid provides reliable event delivery to your applications through rich retry policies and deadlettering.

Incorrect Answers:

"Enable blob versioning for the storage account. Use an Azure Function to process a list of the blob versions per day": You can enable Blob storage versioning to automatically maintain previous versions of an object. When blob versioning is enabled, you can access earlier versions of a blob to recover your data if it is modified or deleted. Reference:

<https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blob-change-feed> <https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blob-event-overview>

QUESTION 3

HOTSPOT

You need to implement the retail store location Azure Function.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Configuration

Value

Binding

	▼
Blob storage	
Azure Cosmos DB	
Event Grid	
HTTP	

Binding Direction

	▼
Input	
Output	

Trigger

	▼
Blob storage	
Azure Cosmos DB	
Event Grid	
HTTP	

Answer Area:

Answer Area

Configuration

Value

Binding

	▼
Blob storage	
Azure Cosmos DB	
Event Grid	
HTTP	

Binding Direction

	▼
Input	
Output	

Trigger

	▼
Blob storage	
Azure Cosmos DB	
Event Grid	
HTTP	

Section:

Explanation:

Scenario: Retail store locations: Azure Functions must process data immediately when data is uploaded to Blob storage.

Box 1: HTTP

Binding configuration example: <https://.blob.core.windows.net>

Box 2: Input

Read blob storage data in a function: Input binding

Box 3: Blob storage
The Blob storage trigger starts a function when a new or updated blob is detected.
Azure Functions integrates with Azure Storage via triggers and bindings. Integrating with Blob storage allows you to build functions that react to changes in blob data as well as read and write values.
Reference:
<https://docs.microsoft.com/en-us/azure/azure-functions/functions-bindings-storage-blob-trigger>

QUESTION 4
HOTSPOT

You are developing an Azure Function App. You develop code by using a language that is not supported by the Azure Function App host. The code language supports HTTP primitives. You must deploy the code to a production Azure Function App environment. You need to configure the app for deployment. Which configuration values 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

Configuration parameter	Configuration value
Publish	<div><div></div><div>▼</div><div>Code</div><div>Docker Container</div></div>
Runtime stack	<div><div></div><div>▼</div><div>Node.js</div><div>Python</div><div>PowerShell Core</div><div>Custom Handler</div></div>
Version	<div><div></div><div>▼</div><div>14 LTS</div><div>7.0</div><div>custom</div></div>

Answer Area:

Answer Area

Configuration parameter

Configuration value

Publish

	▼
Code	
Docker Container	

Runtime stack

	▼
Node.js	
Python	
PowerShell Core	
Custom Handler	

Version

	▼
14 LTS	
7.0	
custom	

Section:

Explanation:

Box 1: Docker container

A custom handler can be deployed to every Azure Functions hosting option. If your handler requires operating system or platform dependencies (such as a language runtime), you may need to use a custom container. You can create and deploy your code to Azure Functions as a custom Docker container.

Box 2: PowerShell core

When creating a function app in Azure for custom handlers, we recommend you select .NET Core as the stack. A "Custom" stack for custom handlers will be added in the future.

PowerShell Core (PSC) is based on the new .NET Core runtime.

Box 3: 7.0

On Windows: The Azure Az PowerShell module is also supported for use with PowerShell 5.1 on Windows.

On Linux: PowerShell 7.0.6 LTS, PowerShell 7.1.3, or higher is the recommended version of PowerShell for use with the Azure Az PowerShell module on all platforms. Reference:

<https://docs.microsoft.com/en-us/azure/azure-functions/functions-create-function-linux-custom-image>

<https://docs.microsoft.com/en-us/powershell/azure/install-az-ps?view=azps-7.1.0>

QUESTION 5

DRAG DROP

You provision virtual machines (VMs) as development environments.

One VM does not start. The VM is stuck in a Windows update process. You attach the OS disk for the affected VM to a recovery VM. You need to correct the issue. In which order should you perform the actions? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place:

Actions

Run the following command at an elevated command prompt:
dism /image:\ /get-packages > c:\temp\Patch.txt

Run the following command at an elevated command prompt:
dism /Image:<Attached OS disks>:\ /Remove
Package /PackageName:<package name to delete>

Detach the OS disk and recreate the VM

Open C:\temp\Patch.txt file and locate the update that is in a pending state

>

<

Answer Area

Correct Answer:

Actions

>

<

Answer Area

Run the following command at an elevated command prompt:
dism /image:\ /get-packages > c:\temp\Patch.txt

Open C:\temp\Patch.txt file and locate the update that is in a pending state

Run the following command at an elevated command prompt:
dism /Image:<Attached OS disks>:\ /Remove
Package /PackageName:<package name to delete>

Detach the OS disk and recreate the VM

- Section:**
- Explanation:**
- Remove the update that causes the problem
1. Take a snapshot of the OS disk of the affected VM as a backup.
 2. Attach the OS disk to a recovery VM.
 3. Once the OS disk is attached on the recovery VM, run diskmgmt.msc to open Disk Management, and ensure the attached disk is ONLINE.
 4. (Step 1) Open an elevated command prompt instance (Run as administrator). Run the following command to get the list of the update packages that are on the attached OS disk:
dism /image::\ /get-packages > c:\temp\Patch_level
 5. (Step 2) Open the C:\temp\Patch_level.txt file, and then read it from the bottom up. Locate the update that's in Install Pending or Uninstall Pending state.
 6. Remove the update that caused the problem:

dism /Image::\ /Remove-Package /PackageName:<>
7. (Step 4) Detach the OS disk and recreate the VM. Then check whether the issue is resolved. Reference:
<https://docs.microsoft.com/en-us/troubleshoot/azure/virtual-machines/troubleshoot-stuck-updating-boot-error>

QUESTION 6
HOTSPOT
You are developing an application to collect the following telemetry data for delivery drivers: first name, last name, package count, item id, and current location coordinates. The app will store the data in Azure Cosmos DB.
You need to configure Azure Cosmos DB to query the data.
Which values 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

Configuration Parameter	Value
Azure Cosmos DB API	<div><div></div><div>Gremlin</div><div>Table API</div><div>Core (SQL)</div></div>
Azure Cosmos DB partition key	<div><div></div><div>first name</div><div>last name</div><div>package count</div><div>item id</div></div>

Answer Area:

Answer Area

Configuration Parameter	Value
Azure Cosmos DB API	<div> <div></div> <div> <div>▼</div> <div> Gremlin Table API Core (SQL) </div> </div> </div>
Azure Cosmos DB partition key	<div> <div></div> <div> <div>▼</div> <div> first name last name package count item id </div> </div> </div>

Section:

Explanation:

Box 1: Core (SQL)

Core(SQL) API stores data in document format. It offers the best end-to-end experience as we have full control over the interface, service, and the SDK client libraries. SQL API supports analytics and offers performance isolation between operational and analytical workloads.

Box 2: item id item id is a unique identifier and is suitable for the partition key. Reference:

<https://docs.microsoft.com/en-us/azure/cosmos-db/choose-api>
<https://docs.microsoft.com/en-us/azure/cosmos-db/partitioning-overview>

QUESTION 7

HOTSPOT

You are developing an ASP.NET Core app that includes feature flags which are managed by Azure App Configuration. You create an Azure App Configuration store named AppFeatureflagStore as shown in the exhibit:

Key	Label	State	Description	Last modified
Export	Export	<div> <div>Off</div> <div>On</div> </div>	Ability to export data.	6/11/2020, 9:13:26 ...

You must be able to use the feature in the app by using the following markup:

```
<feature name="Export">
  <li class="nav-item">
    <a class="nav-link text-dark" asp-area="" asp-controller="Home" asp-action="Export">Export Data</a>
  </li>
</feature>
```

You need to update the app to use the feature flag.
Which values 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

Code section	Value
Controller attribute	<div><div></div><div>FeatureGate</div><div>Route</div><div>ServiceFilter</div><div>TypeFilter</div></div>
Startup method	<div><div></div><div>AddAzureAppConfiguration</div><div>AddControllersWithViews</div><div>AddUserSecrets</div></div>
AppConfig endpoint setting	<div><div></div><div>https://appfeatureflagstore.azconfig.io</div><div>https://appfeatureflagstore.vault.azure.net</div><div>https://export.azconfig.io</div><div>https://export.vault.azure.net</div></div>

Answer Area:

Answer Area

Code section	Value
Controller attribute	<div>▼</div> <div>FeatureGate</div> <div>Route</div> <div>ServiceFilter</div> <div>TypeFilter</div>
Startup method	<div>▼</div> <div>AddAzureAppConfiguration</div> <div>AddControllersWithViews</div> <div>AddUserSecrets</div>
AppConfig endpoint setting	<div>▼</div> <div>https://appfeatureflagstore.azconfig.io</div> <div>https://appfeatureflagstore.vault.azure.net</div> <div>https://export.azconfig.io</div> <div>https://export.vault.azure.net</div>

Section:

Explanation:

Box 1: FeatureGate

You can use the FeatureGate attribute to control whether a whole controller class or a specific action is enabled.

Box 2: AddAzureAppConfiguration

The extension method AddAzureAppConfiguration is used to add the Azure App Configuration Provider.

Box 3: https://appfeatureflagstore.azconfig.io

You need to request the access token with resource=https://.azconfig.io Reference:

<https://docs.microsoft.com/en-us/azure/azure-app-configuration/use-feature-flags-dotnet-core>

<https://csharp.christiannagel.com/2020/05/19/azureappconfiguration/> <https://stackoverflow.com/questions/61899063/how-touse-azure-app-configuration-rest-api>

QUESTION 8

HOTSPOT

You have a single page application (SPA) web application that manages information based on data returned by Microsoft Graph from another company's Azure Active Directory (Azure AD) instance.

Users must be able to authenticate and access Microsoft Graph by using their own company's Azure AD instance.

You need to configure the application manifest for the app registration.

How should you complete the manifest? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:


```
{
  "oauth2AllowImplicitFlow": 

|       |   |
|-------|---|
|       | ▼ |
| add   |   |
| false |   |
| spa   |   |
| true  |   |

,
  " 

|                         |   |
|-------------------------|---|
|                         | ▼ |
| addIns                  |   |
| orgRestrictions         |   |
| availableToOtherTenants |   |
| requiredResourceAccess  |   |

 ":[{
    "resourceAppId": "00000003-0000-0000-c000-000000000000",
    "resourceAccess:[{
      "id" : "24a6cdd6-fab1-4aaf-91b8-3cc8225e90d0",
      "type": "Scope"
    }
  ]],
  "signInAudience": " 

|                                    |   |
|------------------------------------|---|
|                                    | ▼ |
| All                                |   |
| AzureADMyOrg                       |   |
| AzureADMultipleOrgs                |   |
| AzureADandPersonalMicrosoftAccount |   |

 "
}
```

Answer Area:


```

{
  "oauth2AllowImplicitFlow": true,
  "addIns": {
    "orgRestrictions": null,
    "availableToOtherTenants": false,
    "requiredResourceAccess": [
      {
        "resourceAppId": "00000003-0000-0000-c000-000000000000",
        "resourceAccess": [
          {
            "id": "24a6cdd6-fab1-4aaf-91b8-3cc8225e90d0",
            "type": "Scope"
          }
        ]
      }
    ]
  },
  "signInAudience": "AzureADMyOrg"
}

```

Section:

Explanation:

Box 1: true

The `oauth2AllowImplicitFlow` attribute Specifies whether this web app can request OAuth2.0 implicit flow access tokens. The default is false. This flag is used for browser-based apps, like JavaScript singlepage apps. In implicit flow, the app receives tokens directly from the Azure Active Directory (Azure AD) authorize endpoint, without any server-to-server exchange. All authentication logic and session handling is done entirely in the JavaScript client with either a page redirect or a pop-up box.

Box 2: `requiredResourceAccess`

With dynamic consent, `requiredResourceAccess` drives the admin consent experience and the user consent experience for users who are using static consent. However, this parameter doesn't drive the user consent experience for the general case. `resourceAppId` is the unique identifier for the resource that the app requires access to. This value should be equal to the `appId` declared on the target resource app. `resourceAccess` is an array that lists the OAuth2.0 permission scopes and app roles that the app requires from the specified resource. Contains the `id` and `type` values of the specified resources.

Example:

```

"requiredResourceAccess": [
  {
    "resourceAppId": "00000002-0000-0000-c000-000000000000",
    "resourceAccess": [
      {
        "id": "311a71cc-e848-46a1-bdf8-97ff7156d8e6",
        "type": "Scope"
      }
    ]
  }
],

```

Incorrect Answers:

The legacy attribute `availableToOtherTenants` is no longer supported.

The `addIns` attribute defines custom behavior that a consuming service can use to call an app in specific contexts. For example, applications that can render file streams may set the `addIns` property for its "FileHandler" functionality. This parameter will let services like Microsoft 365 call the application in the context of a document the user is working on.

Example:

```
"addIns": [  
  {  
    "id": "968A844F-7A47-430C-9163-07AE7C31D407",  
    "type": "FileHandler",  
    "properties": [  
      {  
        "key": "version",  
        "value": "2"  
      }  
    ]  
  }  
],
```

Box 3: AzureADMyOrg

The signInAudience attribute specifies what Microsoft accounts are supported for the current application. Supported values are: AzureADMyOrg - Users with a Microsoft work or school account in my organization's Azure AD tenant (for example, single tenant)

AzureADMultipleOrgs - Users with a Microsoft work or school account in any organization's Azure AD tenant (for example, multi-tenant)

AzureADandPersonalMicrosoftAccount - Users with a personal Microsoft account, or a work or school account in any organization's Azure AD tenant Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/develop/reference-app-manifest> <https://docs.microsoft.com/enus/azure/active-directory/develop/v2-oauth2-implicit-grant-flow>

QUESTION 9

HOTSPOT

You are developing an application to store and retrieve data in Azure Blob storage. The application will be hosted in an on-premises virtual machine (VM). The VM is connected to Azure by using a Site-to-Site VPN gateway connection. The application is secured by using Azure Active Directory (Azure AD) credentials.

The application must be granted access to the Azure Blob storage account with a start time, expiry time, and read permissions. The Azure Blob storage account access must use the Azure AD credentials of the application to secure data access. Data access must be able to be revoked if the client application security is breached.

You need to secure the application access to Azure Blob storage.

Which security features 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	
Component	Security Feature
Application (Client)	
	Storage Account Access Key
	System-assigned Managed Identity
	Shared access signature (SAS) token
Azure Storage (Server)	
	Stored Access Policy
	User-assigned Managed Identity
	Cross-Origin Resource Sharing (CORS)

Answer Area:

Answer Area	
Component	Security Feature
Application (Client)	
	Storage Account Access Key
	System-assigned Managed Identity
	Shared access signature (SAS) token
Azure Storage (Server)	
	Stored Access Policy
	User-assigned Managed Identity
	Cross-Origin Resource Sharing (CORS)

Section:

Explanation:

QUESTION 10

You are developing an Azure Function App that runs in an App Service Plan. The Azure Function is triggered by a Timer object. You observe that the Azure Function does not reliably trigger when scheduled. Which two actions should you perform?

- A. Verify that Always On is enabled.
- B. Modify the trigger to use a SignalR trigger.
- C. Ensure that the function has a retry configured.
- D. Modify the trigger to use Consumption mode instead of the App Service plan.

Correct Answer: A, C

Section:

QUESTION 11

You are developing a complex workflow by using Azure Durable Functions.

During testing you observe that the results of the workflow differ based on how many instances of the Azure Function are running.

You need to resolve the issue.

What should you do?

- A. Ensure that all Orchestrator code is deterministic.
- B. Read all state data from the durable function context
- C. Configure the Azure Orchestration function to run on an App Service Plan with one instance.
- D. Implement the monitor pattern within the workflow.

Correct Answer: A

Section:

QUESTION 12

You are developing an Azure Function App that generates end of day reports (for retail stores). All stores close at 11 PM each day. Reports must be run one hour after closing. You configure the function to use a Timer trigger that runs at midnight. Customers in the Western United States Pacific Time zone (UTC - 8) report that the Azure Function runs before the stores close. You need to ensure that the Azure Function runs at midnight in the Pacific Time zone.

What should you do?

- A. Configure the Azure Function to run in the West US region.
- B. Add an app setting named WEBSITE_TIME_ZONE that uses the value Pacific Standard Time
- C. Change the Timer trigger to run at 7 AM
- D. Update the Azure Function to a Premium plan.

Correct Answer: A

Section:

QUESTION 13

You are developing an application to manage shipping information for cargo ships. The application will use Azure Cosmos DB for storage.

The application must run offline when ships are at sea. The application must be connected to Azure when ships are in port.

Which Azure Cosmos DB API should you use for the application?

- A. Core
- B. MongoDB

- C. Cassandra
- D. Gremlin

Correct Answer: C

Section:

QUESTION 14

You are a developing a SaaS application that stores data as key value pairs.

You must make multiple editions of the application available. In the lowest cost edition, the performance must be best-effort, and there is no regional failover.

In higher cos! editions customers must be able to select guaranteed performance and support for multiple regions. Azure costs must be minimized.

Which Azure Cosmos OB API should you use for the application?

- A. Core
- B. MongoDB
- C. Cassandra
- D. Table API

Correct Answer: D

Section:

QUESTION 15

You are developing an application to store information about the organizational structure for a company.

Users must be able to determine which people report to a particular manager, the office where employees work, and the projects that are assigned to an employee.

Which Azure Cosmos DB API should you use for the application?

- A. Core
- B. Cassandra
- C. Table API
- D. Gremlin
- E. MongoDB

Correct Answer: E

Section:

QUESTION 16

You are a developing a SaaS application that stores data as key value pairs.

You must make multiple editions of the application available. In the lowest cost edition, the performance must be best-effort, and there is no regional failover.

In higher cos! editions customers must be able to select guaranteed performance and support for multiple regions. Azure costs must be minimized.

Which Azure Cosmos OB API should you use for the application?

- A. Core
- B. MongoDB
- C. Cassandra
- D. Table API

Correct Answer: C

Section:

QUESTION 17

You are developing a mobile app that uses an API which stores geospabal data in Azure Cosmos D& The app will be used to find restaurants in a particular area and related information including food types, menu information and the optimal route to a selected restaurant from the user's current location.

Which Azure Cosmos DB API should you use for the API?

- A. MongoDB
- B. Gremlin
- C. Cassandra
- D. Core

Correct Answer: A

Section:

QUESTION 18

You are designing a web application to manage user satisfaction surveys. The number of questions that a survey includes is variable.

Application users must be able to display results for a survey as quickly as possible. Users must also be able to quickly compute statistical measures including average values across various groupings of answers.

Which Azure Cosmos DB API should you use for the application?

- A. Core
- B. Mongo DB
- C. Gremlin
- D. Table API

Correct Answer: D

Section:

QUESTION 19

You are developing an application that allows users to find musicians that are looking for work. The application must store information about musicians, the instruments that they play, and other related data.

The application must also allow users to determine which musicians have played together, including groups of three or more musicians that have performed together at a specific location.

Which Azure Cosmos DB API should you use for the application?

- A. Core
- B. MongoDB
- C. Cassandra
- D. Gremlin

Correct Answer: B

Section:

QUESTION 20

You deploy an API to API Management

You must secure all operations on the API by using a client certificate.

You need to secure access to the backend service of the API by using client certificates.

Which two security features can you use?

- A. Azure AD token
- B. Self-signed certificate

- C. Certificate Authority (CA) certificate
- D. Triple DES (3DES) cipher
- E. Subscription key

Correct Answer: B, C

Section:

QUESTION 21

You have an Azure Cosmos DB instance that uses the Strong consistency level and 10,000 Request Units (RUs) per container. <3eo-replication is enabled.

The instance stores restaurant information including location, menu items, and staff. You currently store information for 1,000 restaurant locations, 500 menu items, and 10,000 staff members. You select the location id as the partition key.

How many logical partitions will be created for the container?

- A. 500
- B. 1,100
- C. 10,000
- D. 10,000,000

Correct Answer: C

Section:

QUESTION 22

You are designing a small app that will receive web requests containing encoded geographic coordinates. Calls to the app will occur infrequently.

Which compute solution should you recommend?

- A. Azure Functions
- B. Azure App Service
- C. Azure Batch
- D. Azure API Management

Correct Answer: B

Section:

QUESTION 23

Your company has several containers based on the following operating systems:

- Windows Server 2019 Nano Server
- Windows Server 2019 Server Core
- Windows Server 2022 Nano Server
- Windows Server 2022 Server Core
- Linux

You plan to migrate the containers to an Azure Kubernetes cluster. What is the minimum number of node pools that the cluster must have?

- A. 1
- B. 2
- C. 3
- D. 6

Correct Answer: C

Section:

QUESTION 24

Your company purchases an Azure subscription and plans to migrate several on-premises virtual machines to Azure. You need to design the infrastructure required for the Azure virtual machines solution. What should you include in the design?

- A. the number of Azure Storage accounts
- B. the settings of the Azure virtual networks
- C. the size of the virtual machines
- D. the number of Azure regions

Correct Answer: C

Section:

QUESTION 25

You need to design network connectivity for a subnet in an Azure virtual network. The subnet will contain 30 virtual machines. The virtual machines will establish outbound connections to internet hosts by using the same pool of four public

IP addresses, inbound connections to the virtual machines will be prevented.

What should include in the design?

- A. Azure Private Link
- B. NAT Gateway
- C. User Defined Routes
- D. Azure Virtual WAN

Correct Answer: D

Section:

QUESTION 26

Your company is designing an application named App1 that will use data from Azure SQL Database.

App1 will be accessed over the internet by many users.

You need to recommend a solution for improving the performance of App1.

What should you include in the recommendation?

- A. Azure HPC cache
- B. ExpressRoute
- C. a CDN profile
- D. Azure Cache for Redis

Correct Answer: D

Section:

QUESTION 27

You are designing a multi-tiered application that will be hosted on Azure virtual machines. The virtual machines will run Windows Server. Front-end servers will be accessible from the Internet over port 443. The other servers will NOT be directly accessible over the internet You need to recommend a solution to manage the virtual machines that meets the following requirement

- Allows the virtual machine to be administered by using Remote Desktop.

- Minimizes the exposure of the virtual machines on the Internet Which Azure service should you recommend?

- A. Azure Bastion
- B. Service Endpoint
- C. Azure Private Link
- D. Azure Front Door

Correct Answer: C
Section:

QUESTION 28

You develop and deploy an Azure App Service web app to a production environment. You enable the Always On setting and the Application Insights site extensions. You deploy a code update and receive multiple failed requests and exceptions in the web app. You need to validate the performance and failure counts of the web app in near real time. Which Application Insights tool should you use?

- A. Snapshot Debugger
- B. Profiler
- C. Smart Detection
- D. Live Metrics Stream
- E. Application Map

Correct Answer: D
Section:

QUESTION 29

You are building a web application that uses the Microsoft identity platform for user authentication.

You are implementing user identification for the web application. You need to retrieve a claim to uniquely identify a user. Which claim type should you use?

- A. oid
- B. aud
- C. idp
- D. nonce

Correct Answer: A
Section:

QUESTION 30

DRAG DROP

You develop and deploy a web app to Azure App Service in a production environment. You scale out the web app to four instances and configure a staging slot to support changes.

You must monitor the web app in the environment to include the following requirements:

- Increase web app availability by re-routing requests away from instances with error status codes and automatically replace instances if they remain in an error state after one hour.
- Send web server logs, application logs, standard output and standard error messaging to an Azure Storage blob account.

You need to configure Azure App Service.

Which values should you use? To answer, drag the appropriate configuration value to the correct requirements. Each configuration value may be used once, more than....

Select and Place:

Configuration values

Health check

Diagnostic setting

Deployment slot

Autoscale rule

Zone redundancy

Answer Area

Requirement

Increase availability

Send logs

Configuration value

Correct Answer:

Configuration values

Health check

Diagnostic setting

Deployment slot

Answer Area

Requirement

Increase availability

Send logs

Configuration value

Autoscale rule

Zone redundancy

Section:

Explanation:

QUESTION 31

HOTSPOT

You are developing an application that runs in several customer Azure Kubernetes Service clusters, Within each cluster, a pod runs that collects performance data to be analyzed later, a large amount of data is collected so saving latency must be minimized.The performance data must be stored so that pod restarts do not impact the stored data. Write latency should be minimized.

You need to configure blob storage.

How should you complete the YAML configuration? To answer, select the appropriate options in the answer area.

Hot Area:

apiVersion: storage.k8s.io/v1
kind:
metadata: PodStorage
StorageClass
PersistentVolume
PersistentVolumeClaim
name: data-store
provisioner: kubernetes.io/
azure-disk
azure-file
portworx-volume
scaleio
parameters:
skuName: Premium_LRS
reclaimPolicy:
local
retain
delete

Answer Area:

apiVersion: storage.k8s.io/v1
kind:
metadata: PodStorage
StorageClass
PersistentVolume
PersistentVolumeClaim
name: data-store
provisioner: kubernetes.io/
azure-disk
azure-file
portworx-volume
scaleio
parameters:
skuName: Premium_LRS
reclaimPolicy:
local
retain
delete

Section:
Explanation:

QUESTION 32
DRAG DROP

You have an application that provides weather forecasting data to external partners. You use Azure API Management to publish APIs. You must change the behavior of the API to meet the following requirements:

- Support alternative input parameters.
- Remove formatting text from responses.
- Provide additional context to back-end services.

Which types of policies should you implement? To answer, drag the policy types to the correct scenarios. Each policy 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:

Policy types

Inbound

Outbound

Backend

Answer Area

Requirement

Support alternative input parameters.

Remove formatting text from responses.

Provide additional context to back-end services.

Policy type

policy type

policy type

Correct Answer:

Policy types

Inbound

Outbound

Backend

Answer Area

Requirement

Support alternative input parameters.

Remove formatting text from responses.

Provide additional context to back-end services.

Policy type

Inbound

Outbound

Inbound

Section:
Explanation:

QUESTION 33
HOTSPOT

You are a developer building a web site using a web app. The web site stores configuration data in Azure App Configuration. Access to Azure App Configuration has been configured to use the identity of the web app for authentication.

Security requirements specify that no other authentication systems must be used.

You need to load configuration data from Azure App Configuration.

How should you complete the code? To answer, select the appropriate options in the answer area.

Hot Area:


```

public static IHostBuilder CreateHostBuilder(string[] args) =>
    Host.CreateDefaultBuilder(args)
        .ConfigureWebHostDefaults(web =>
        {
            web.ConfigureAppConfiguration((hc, config) =>
            {
                var settings = config.Build();
                config.
                    AddAzureKeyVault
                    DefaultAzureCredential
                    ChainedTokenCredential
                    ManagedIdentityCredential
                    AddAzureAppConfiguration
                    (options =>
                    options.Connect(new Uri(settings["AppConfig:Endpoint"]),
                    new
                    AddAzureKeyVault
                    DefaultAzureCredential
                    ChainedTokenCredential
                    ManagedIdentityCredential
                    AddAzureAppConfiguration
                    ());
            }
        }
    );

```

Answer Area:



Section:

Explanation:

QUESTION 34

DRAG DROP

You are Implementing an Azure solution that uses Azure Cosmos DB and the latest Azure Cosmos DB SDK. You add a change feed processor to a new container instance.

You attempt to lead a batch of 100 documents. The process falls when reading one of the documents. The solution must monitor the progress of the change feed processor instance on the new container as the change feed is read. You must prevent the change feed processor from retrying the entire batch when one document cannot be read.

You need to implement the change feed processor to read the documents.

Which features should you use? To answer, drag the appropriate features to the correct requirements. Each feature may be used once, More than once, or not at all. You may need to drag The split bat between panes or scroll to view content.

Each correct selection is worth one point

Select and Place:

Features

Change feed estimator
Dead-letter queue
Deployment unit
Lease container

Answer Area

Requirement

Monitor the progress of the change feed processor.

Feature

Feature

Prevent the change feed processor from retrying the entire batch when one document cannot be read.

Feature

Feature

Correct Answer:

Features

Change feed estimator
Lease container

Answer Area

Requirement

Monitor the progress of the change feed processor.

Feature

Dead-letter queue

Prevent the change feed processor from retrying the entire batch when one document cannot be read.

Feature

Deployment unit

Section:

Explanation:

QUESTION 35

You are building a web application that performs image analysis on user photos and returns metadata containing objects identified. The image is very costly in terms of time and compute resources. You are planning to use Azure Redis

Cache so duplicate uploads do not need to be reprocessed.

In case of an Azure data center outage, metadata loss must be kept to a minimum. You need to configure the Azure Redis cache instance.

Which two actions should you perform?

- A. Configure Azure Redis with rob persistence
- B. Configure second storage account far persistence.
- C. Set backup frequency to the minimum value.
- D. Configure Azure Redis with AOF persistence

Correct Answer: B, C

Section:

QUESTION 36

HOTSPOT

You develop and deploy the following staticwebapp.config.json file to the app_location value specified in the workflow file of an Azure Static Web app.

```
{
  "routes": [
    {
      "route": "*/api/*",
      "methods": ["GET"],
      "allowedRoles": ["registeredusers"]
    },
    {
      "route": "*/api/*",
      "methods": ["PUT", "POST", "PATCH", "DELETE"]
    }
  ]
}
```

Hot Area:

Statements	Yes	No
Unauthenticated users are challenged to authenticate with Github.	<input type="radio"/>	<input type="radio"/>
A non-existent file in the /images/ folder will generate a 404 response code.	<input type="radio"/>	<input type="radio"/>
HTTP GET method requests from authenticated users in the role named registeredusers are sent to the API folder.	<input type="radio"/>	<input type="radio"/>
Authenticated users that are not in the role named registeredusers and unauthenticated users are served a 401 HTTP error when accessing the API folder.	<input type="radio"/>	<input type="radio"/>

Answer Area:

Statements	Yes	No
Unauthenticated users are challenged to authenticate with Github.	<input checked="" type="radio"/>	<input type="radio"/>
A non-existent file in the /images/ folder will generate a 404 response code.	<input checked="" type="radio"/>	<input type="radio"/>
HTTP GET method requests from authenticated users in the role named registeredusers are sent to the API folder.	<input checked="" type="radio"/>	<input type="radio"/>
Authenticated users that are not in the role named registeredusers and unauthenticated users are served a 401 HTTP error when accessing the API folder.	<input checked="" type="radio"/>	<input type="radio"/>

Section:

Explanation:

QUESTION 37

HOTSPOT

You develop and deploy a web app to Azure App service. The web app allows users to authenticate by using social identity providers through the Azure B2C service. All user profile information is stored in Azure B2C.

You must update the web app to display common user properties from Azure B2C to include the following information:

Email address

Job title

First name
Last name
Office Location
You need to implement the user properties in the web app.

Hot Area:

Requirement	Value
API to access user properties	<div><div></div><div>Microsoft Graph</div><div>Azure AD Graph</div><div>Azure Key Vault</div><div>Azure AD entitlement management</div></div>
Code library to interface to Azure AD B2C	<div><div></div><div>Microsoft Authentication Library (MSAL)</div><div>Microsoft Azure Key Vault SDK</div><div>Azure Identity library</div></div>

Answer Area:

Requirement	Value
API to access user properties	<div><div></div><div>Microsoft Graph</div><div>Azure AD Graph</div><div>Azure Key Vault</div><div>Azure AD entitlement management</div></div>
Code library to interface to Azure AD B2C	<div><div></div><div>Microsoft Authentication Library (MSAL)</div><div>Microsoft Azure Key Vault SDK</div><div>Azure Identity library</div></div>

Section:
Explanation:

QUESTION 38

You are building a web application that performs image analysis on user photos and returns metadata containing objects identified. The image analysis is very costly in terms of time and compute resources. You are planning to use Azure
Redo Cache so Cache uploads do not need to be reprocessed.
In case of an Azure data center outage metadata loss must be kept to a minimum.
You need to configure the Azure Redis cache instance.
Which two actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection in worth one point.

- A. Configure Azure Redis with persistence
- B. Configure second storage account for persistence
- C. Set backup frequency to the minimum value
- D. Configure Azure Redis with RDS persistence

Correct Answer: B, D
Section:

QUESTION 39

HOTSPOT
YOU need to reliably identify the delivery driver profile information.
How should you configure the system? To answer, select the appropriate options in the answer area.
NOTE Each correct selection is worth one point.

Hot Area:

Configuration	Value
JSON web token (JWT) type	<div><div></div><div>ID</div><div>Refresh</div><div>Access</div></div>
Payload claim value	<div><div></div><div>oid</div><div>aad</div><div>idp</div></div>

Answer Area:

Configuration	Value
JSON web token (JWT) type	<div> <div></div> <div>ID</div> <div>Refresh</div> <div>Access</div> </div>
Payload claim value	<div> <div></div> <div>oid</div> <div>aad</div> <div>idp</div> </div>

Section:

Explanation:

QUESTION 40

HOTSPOT

You need to implement event routing for retail store location data.

Which configuration should you use?

Hot Area:

Event data	Configuration
Source	<div> <div></div> <div>Azure Blob Storage</div> <div>Azure Event Grid</div> <div>Azure Service Bus</div> <div>Azure Event Hub</div> </div>
Receiver	<div> <div></div> <div>Azure Event Grid</div> <div>Azure Event Hub</div> <div>Azure Service Bus</div> <div>Azure Blob Storage</div> </div>
Handler	<div> <div></div> <div>Azure Function App</div> <div>Azure Logic App</div> <div>Azure Event Grid</div> <div>Azure Blob Storage</div> </div>

Answer Area:

Event data	Configuration
Source	<div> <div>▼</div> <div> Azure Blob Storage Azure Event Grid Azure Service Bus Azure Event Hub </div> </div>
Receiver	<div> <div>▼</div> <div> Azure Event Grid Azure Event Hub Azure Service Bus Azure Blob Storage </div> </div>
Handler	<div> <div>▼</div> <div> Azure Function App Azure Logic App Azure Event Grid Azure Blob Storage </div> </div>

Section:

Explanation:

QUESTION 41

HOTSPOT

You need to implement the delivery service telemetry data

How should you configure the solution?

NOTE: Each correct selection is worth one point.

Hot Area:

Azure Cosmos DB	Value
API	<div> <div>▼</div> <div> Core (SQL) Gremlin Table MongoDB </div> </div>
Partition Key	<div> <div>▼</div> <div> Item id Vehicle license plate Vehicle package capacity Vehicle location coordinates </div> </div>

Answer Area:



Section:

Explanation:

QUESTION 42

You need to reduce read latency for the retail store solution.

What are two possible ways to achieve the goal? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. Create a new composite index for the store location data queries in Azure Cosmos DB. Modify the queries to support parameterized SQL and update the Azure function app to call the new Queries.
- B. Configure Azure Cosmos DB consistency to strong consistency Increase the RUs for the container supporting store location data.
- C. Provision an Azure Cosmos DB dedicated gateway, update blob storage to use the new dedicated gateway endpoint.
- D. Configure Azure Cosmos DB consistency to session consistency. Cache session tokens in a new Azure Redis cache instance after every write. Update reads to use the session token stored in Azure Redis.
- E. Provision an Azure Cosmos DB dedicated gateway Update the Azure Function app connection string to use the new dedicated gateway endpoint.

Correct Answer: A, C

Section:

QUESTION 43

HOTSPOT

You need to implement the corporate website.

How should you configure the solution?

Hot Area:

Answer Area

Azure

Configuration

Plan

	▼
Free	
Standard	
Premium	
Isolated	

Service

	▼
App Service Web App	
App Service Static Web App	
Azure Function App	
Azure Blob Storage	

Answer Area:

Answer Area

Azure

Configuration

Plan

	▼
Free	
Standard	
Premium	
Isolated	

Service

	▼
App Service Web App	
App Service Static Web App	
Azure Function App	
Azure Blob Storage	

Section:

Explanation:

QUESTION 44

You need to test the availability of the corporate website.

Which two test types can you use?

- A. Custom testing using the TrackAvailability API method
- B. Standard
- C. URL Ping
- D. Multi-step

Correct Answer: A, B

Section:

QUESTION 45

You develop and deploy an Azure App Service web app named App1. You create a new Azure Key Vault named Vault 1. You import several API keys, passwords, certificates, and cryptographic keys into Vault1.

You need to grant App1 access to Vault1 and automatically rotate credentials. Credentials must not be stored in code.

What should you do?

- A. Enable App Service authentication for App1. Assign a custom RBAC role to Vault1.
- B. Add a TLS/SSL binding to App1.
- C. Assign a managed identity to App1.

D. Upload a self-signed client certificate to Vault1. Update App1 to use the client certificate.

Correct Answer: D

Section:

QUESTION 46

You a web application that provides access to legal documents that are stored on Azure Blob Storage with version level immutability policies. Documents are protected with both time-based policies legal hold policies. All time,Ä"based retention policies have AllowProtectedAppendWrites property enabled.

You have a requirement to prevent the user from attempting to perform operations that would fail only a legal is in effect and when all other are expired.

You need to meet the requirement.

Which two operations you prevent?

- A. overwriting existing
- B. adding data to documents
- C. deleting documents
- D. creating document

Correct Answer: B, D

Section:

QUESTION 47

You are developing an Azure Durable Function to manage an online ordering process.

The process must call an external API to gather product discount information.

You need to implement Azure Durable Function.

Which Azure Durable Function types should you use? Each correct answer presents part of the solution

NOTE: Each correct selection is worth ore point

- A. Orchestrator
- B. Entity
- C. Activity
- D. Client

Correct Answer: A, B

Section:

Explanation:

<https://learn.microsoft.com/en-us/azure/azure-functions/durable/durable-functions-types-featuresoverview>

QUESTION 48

You develop a Python application for image rendering that uses GPU resources to optimize rendering processes. You deploy the application to an Azure Container Instances (ACI) Linux container.

The application requires a secret value to be passed when the container is started. The value must only be accessed from within the container.

You need to pass the secret value.

What are two possible ways to achieve this goal? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. Create an environment variable Set the secureValue property to the secret value.
- B. Add the secret value to the container image. Use a managed identity.
- C. Add the secret value to the application code Set the container startup command.

- D. Add the secret value to an Azure Blob storage account. Generate a SAS token.
- E. Mount a secret volume containing the secret value in a secrets file.

Correct Answer: A, E

Section:

Explanation:

Objects with secure values are intended to hold sensitive information like passwords or keys for your application. Using secure values for environment variables is both safer and more flexible than including it in your container's image.

Another option is to use secret volumes, described in Mount a secret volume in Azure Container Instances..... <https://docs.microsoft.com/en-us/azure/containerinstances/container-instances-environment-variables>

QUESTION 49

The solution must receive and store messages until they can be processed. You create an Azure Service Bus instance by providing a name, pricing tier, subscription, resource group, and location.

You need to complete the configuration.

Which Azure CLI or PowerShell command should you run?

A.

```
New-AzureRmResourceGroup
-Name fridge-rg
-Location fridge-loc
```

B.

```
connectionStrings$(az servicebus namespace authorization-rule keys list
--resource-group fridge-rg
--fridge-ns fridge-ns
--name RootManageSharedAccessKey
--query primaryConnectionString --output tsv)
```

C.

```
New-AzureRmServiceBusQueue
-ResourceGroupName fridge-rg
-NamespaceName fridge-ns
-Name fridge-q
-EnablePartitioning $False
```

D.

```
New-AzureRmServiceBusNamespace
-ResourceGroupName fridge-rg
-NamespaceName fridge-ns
-Location fridge-loc
```

Correct Answer: C

Section:

QUESTION 50

You need to grant access to the retail store location data for the inventory service development effort. What should you use?

- A. Azure AD access token
- B. Azure RBAC role
- C. Azure AD ID token
- D. Shared access signature (SAS) token
- E. Azure AD refresh token

Correct Answer: D

Section:

QUESTION 51

You develop Azure solutions.You must connect to a No-SQL globally-distributed database by using the .NET API.You need to create an object to configure and execute requests in the database. Which code segment should you use?

- A. new Container(EndpointUri, PrimaryKey)
- B. new Database(Endpoint, PrimaryKey);
- C. new CosmosClient(EndpointUri, PrimaryKey);

Correct Answer: C

Section:

Explanation:

Example: // Create a new instance of the Cosmos Client this.cosmosClient = new CosmosClient(EndpointUri, PrimaryKey)//ADD THIS PART TO YOUR CODEawait this.CreateDatabaseAsync();Reference:<https://docs.microsoft.com/en-us/ azure/cosmos-db/sql-api-get-started>

QUESTION 52

DRAG DROP

You are developing an application to store millions of images in Azure blob storage. The images are uploaded to an Azure blob storage container named companyimages contained in an Azure blob storage account named companymedia.

The stored images are uploaded with multiple blob index tags across multiple blobs in the container.

You must find all blobs whose tags match a search expression in the container. The search expression must evaluate an index tag named status with a value of final.

You need to construct the GET method request URL How should you complete the URI? To answer, drag the appropriate parameters to the correct request URI targets. Each parameter 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.

Select and Place:

Parameters

Status='Final'

Status<='Final'

companymedia

companyimages

Answer Area

https://

.blob.core.windows.net/

?restype=container&comp=blobs&where=

Correct Answer:

Parameters

Status<='Final'

Answer Area

https://

companymedia

 .blob.core.windows.net/

companyimages

 ?restype=container&comp=blobs&where=

Status='Final'

Section:

Explanation:

QUESTION 53

HOTSPOT

You are building a software-as-a-service (SaaS) application that analyzes DNA data that will run on Azure virtual machines (VMs) in an availability zone. The data is stored on managed disks attached to the VM. The performance of the analysis is determined by the speed of the disk attached to the VM.

You have the following requirements:

- The application must be able to quickly revert to the previous day's data if a systemic error is detected.
- The application must minimize downtime in the case of an Azure datacenter outage.

You need to provision the managed disk for the VM to maximize performance while meeting the requirements. Which type of Azure Managed Disk 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

Requirement	Solution
Disk type	<div>Premium SSD Premium SSD Standard SSD Standard HDD</div>
Redundancy	<div>Geo-redundant storage (GRS) Geo-redundant storage (GRS) Zone-redundant storage (ZRS) Locally-redundant storage (LRS)</div>

Answer Area:

Answer Area

Requirement	Solution
Disk type	<div>Premium SSD Premium SSD Standard SSD Standard HDD</div>
Redundancy	<div>Geo-redundant storage (GRS) Geo-redundant storage (GRS) Zone-redundant storage (ZRS) Locally-redundant storage (LRS)</div>

Section:

Explanation:

QUESTION 54

HOTSPOT

You are developing an online game that allows players to vote for their favorite photo that illustrates a word. The game is built by using Azure Functions and uses durable entities to track the vote count. The voting window is 30 seconds. You must minimize latency. You need to implement the Azure Function for voting. How should you complete the code? To answer, select the appropriate options in the answer area.

Hot Area:

Answer Area

```
[FunctionName("Vote")]
public static async Task<HttpStatusCode> Run(
    [HttpTrigger("POST", Route = "pic/{id}")] HttpRequestMessage req,
    [SignalEntityAsync] IDurableEntityClient c,
    [DurableClient] IDurableOrchestrationClient o
)
{
    return req.CreateResponse(HttpStatusCode.OK);
}

{
    var eid = new EntityId("pic", id);
    await c.
    return req.Cr
}
```

SignalEntityAsync

CallEntityAsync

SignalEntityAsync

[DurableClient] IDurableEntityClient

[DurableClient] IDurableOrchestrationClient

[DurableClient] IDurableEntityClient

CallEntityAsync

SignalEntityAsync

[DurableClient] IDurableEntityClient

[DurableClient] IDurableOrchestrationClient

Answer Area:

Answer Area

```
[FunctionName("Vote")]
public static async Task<HttpResponseMessage> Run(
    [HttpTrigger("POST", Route = "pic/{id}")] HttpRequestMessage req,
    [SignalEntityAsync] IDurableEntityClient c,
    [DurableClient] IDurableOrchestrationClient o)
{
    return req.CreateResponse(HttpStatusCode.OK);
}

{
    var eid = new EntityId("pic", id);
    await c.
    return req.Cr
}
```

Dropdown 1 (after `c,`):

- SignalEntityAsync
- CallEntityAsync
- SignalEntityAsync
- [DurableClient] IDurableEntityClient
- [DurableClient] IDurableOrchestrationClient

Dropdown 2 (after `await c.`):

- [DurableClient] IDurableEntityClient
- CallEntityAsync
- SignalEntityAsync
- [DurableClient] IDurableEntityClient
- [DurableClient] IDurableOrchestrationClient

Section:

Explanation:

QUESTION 55

HOTSPOT

All functions in the app meet the following requirements:

- Run until either a successful run or until 10 run attempts occur.
- Ensure that there are at least 20 seconds between attempts for up to 15 minutes.

You need to configure the hostjson file.

How should you complete the code segment? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

retry

retry

healthMonitor

singleton

"strategy": "exponentialBackoff",

maxRe exponentialBackoff

counterThreshold

fixedDelay

maxRetryCount": 10,

maxRetryCount

healthCheckInterval

healthCheckThreshold

Answer Area:

Answer Area

retry

retry

healthMonitor

singleton

"strategy": "exponentialBackoff",

maxRe exponentialBackoff

counterThreshold

fixedDelay

maxRetryCount": 10,

maxRetryCount

healthCheckInterval

healthCheckThreshold

Section:

Explanation:

Answer Area

```
{
  "retry": {
    "strategy": "exponentialBackoff",
    "maxRetryCount": 10,
    "minimumInterval": "00:00:20",
    "maximumInterval": "00:15:00"
  }
}
```

QUESTION 56

HOTSPOT

You are developing an Azure Durable Function based application that processes a list of input values.

The application is monitored using a console application that retrieves JSON data from an Azure Function diagnostic endpoint. During processing a single instance of invalid input does not cause the function to fail. Invalid input must be available to the monitoring application.

You need to implement the Azure Durable Function and the monitoring console application.

How should you complete the code segments? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

```
[FunctionName("App")]
public static async Task<List<string>> RunOrchestrator(
    [OrchestrationTrigger] IDurableOrchestrationContext context) {
    EntityId[] input = . . .
    int errIndex = . . .

    await context.CallEntityAsync(input[errIndex], "error");
    context.SetOutput(input[errIndex])
    context.SetCustomStatus(input[errIndex])
    context.SignalEntity(input[errIndex], "error")
    await context.CallEntityAsync(input[errIndex], "error")
}

using (var client = new HttpClient())
{
    while (true)
    {
        var response = await client.GetAsync(". . .");
        response.EnsureSuccessStatusCode();
        var json = await response.Content.ReadAsStringAsync();
        dynamic result = JsonConvert.DeserializeObject(json);
        if (result.runtimeStatus == "Failed")
        {
            . . .
        }
    }
}
```

Answer Area:

Answer Area

```
[FunctionName("App")]
public static async Task<List<string>> RunOrchestrator(
    [OrchestrationTrigger] IDurableOrchestrationContext context) {
    EntityId[] input = . . .
    int errIndex = . . .

    await context.CallEntityAsync(input[errIndex], "error");
    context.SetOutput(input[errIndex])
    context.SetCustomStatus(input[errIndex])
    context.SignalEntity(input[errIndex], "error")
    await context.CallEntityAsync(input[errIndex], "error")
}

using (var client = new HttpClient())
{
    while (true)
    {
        var response = await client.GetAsync(". . .");
        response.EnsureSuccessStatusCode();
        var json = await response.Content.ReadAsStringAsync();
        dynamic result = JsonConvert.DeserializeObject(json);
        if (result.runtimeStatus == "Failed")
        {
            . . .
        }
    }
}
```

Section:

Explanation:

QUESTION 57

You are developing an Azure-based web application. The application goes offline periodically to perform offline data processing. While the application is offline, numerous Azure Monitor alerts fire which result in the on-call developer being paged.

The application must always log when the application is offline for any reason.

You need to ensure that the on-call developer is not paged during offline processing.

What should you do?

- A. Add Azure Monitor alert processing rules to suppress notifications.
- B. Create an Azure Monitor Metric Alert.
- C. Build an Azure Monitor action group that suppresses the alerts.

D. Disable Azure Monitor Service Health Alerts during offline processing.

Correct Answer: C

Section:

QUESTION 58

HOTSPOT

You develop new functionality in a web application for a company that provides access to seismic data from around the world. The seismic data is stored in Redis Streams within an Azure Cache for Redis instance. The new functionality includes a real-time display of seismic events as they occur. You need to implement the Azure Cache for Redis command to receive seismic data. How should you complete the command? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

The screenshot shows the command editor for the Azure Cache for Redis. It consists of three dropdown menus and a text input field. The first dropdown menu is set to 'XREAD'. The second dropdown menu is set to 'BLOCK 0'. The third dropdown menu is set to '\$'. The text input field contains 'STREAMS seismicData'.

Answer Area:

Answer Area

The screenshot shows the command editor for the Azure Cache for Redis. It consists of three dropdown menus and a text input field. The first dropdown menu is set to 'XREAD'. The second dropdown menu is set to 'BLOCK 0'. The third dropdown menu is set to '\$'. The text input field contains 'STREAMS seismicData'.

Section:

Explanation:

QUESTION 59

You develop an ASP.NET Core app that uses Azure App Configuration. You also create an App Configuration containing 100 settings. The app must meet the following requirements:

- Ensure the consistency of all configuration data when changes to individual settings occur.
- Handle configuration data changes dynamically without causing the application to restart.
- Reduce the overall number of requests made to App Configuration APIs.

You must implement dynamic configuration updates in the app.

What are two ways to achieve this goal? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Increase the App Configuration cache expiration from the default value.
- B. Create and implement environment variables for each App Configuration store setting.
- C. Decrease the App Configuration cache expiration from the default value.
- D. Register all keys in the App Configuration store. Set the refreshAll parameter of the Register method to false.
- E. Create and register a sentinel key in the App Configuration store. Set the refreshAll parameter of the Register method to true.
- F. Create and configure Azure Key Vault. Implement the Azure Key Vault configuration provider.

Correct Answer: A, E
Section:

QUESTION 60
HOTSPOT

You develop a web app that interacts with Azure Active Directory (Azure AD) groups by using Microsoft Graph.
You build a web page that shows all Azure AD groups that are not of the type 'Unified'.
You need to build the Microsoft Graph query for the page.
How should you complete the query? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

The screenshot shows the Microsoft Graph query builder interface. The URL is `https://graph.microsoft.com/v1.0/groups?`. There are three dropdown menus for filtering. The first dropdown is set to `$count=true`. The second dropdown is set to `filter`. The third dropdown is set to `groupTypes/any(s:s ne 'Unified')`. The query is `https://graph.microsoft.com/v1.0/groups?$count=true&filter=groupTypes/any(s:s ne 'Unified')`.

Answer Area:

Answer Area

<https://graph.microsoft.com/v1.0/groups?>

filter

filter

search

contains

groupTypes/any(s:s ne 'Unified')

groupTypes/any(s:s ne 'Unified')

not groupTypes/contains('Unified')

not groupTypes/any(s:s eq 'Unified')

groupTypes/contains('Unified') eq false

&\$

\$count=true

\$stop=true

\$count=true

\$filter=nested

\$consistencylevel=eventual

Section:

Explanation:

QUESTION 61

You are updating an application that stores data on Azure and uses Azure Cosmos DB for storage. The application stores data in multiple documents associated with a single username. The application requires the ability to update multiple documents for a username in a single ACID operation.

You need to configure Azure Cosmos DB.

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

NOTE: Each correct selection is worth one point.

- A. Configure Azure Cosmos DB to use the Azure Cosmos DB for Apache Gremlin API.
- B. Configure Azure Cosmos DB to use the Azure Cosmos DB for MongoDB API.
- C. Create a collection sharded on username to store documents.
- D. Create an unsharded collection to store documents.

Correct Answer: B, D

Section:

QUESTION 62

HOTSPOT

An organization deploys a blob storage account. Users take multiple snapshots of the blob storage account over time. You need to delete all snapshots of the blob storage account. You must not delete the blob storage account itself. How should you complete the code segment? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

```
Delete (Azure.Storage.Blobs.Models.DeleteSnapshotsOption
```

```
snapshotsOption = Azure.Storage.Blobs.Models.
```

- DeleteSnapshotsOption
- DeletelfExists
- DeleteSnapshotsOption
- WithSnapshot
- WithSnapshotCore

- OnlySnapshots
- IncludeSnapshots
- None
- OnlySnapshots

Answer Area:

Answer Area

```
Delete (Azure.Storage.Blobs.Models.DeleteSnapshotsOption
```

```
snapshotsOption = Azure.Storage.Blobs.Models.
```

- DeleteSnapshotsOption
- DeletelfExists
- DeleteSnapshotsOption
- WithSnapshot
- WithSnapshotCore

- OnlySnapshots
- IncludeSnapshots
- None
- OnlySnapshots

Section:

Explanation:

QUESTION 63

You are developing a Java application to be deployed in Azure. The application stores sensitive data in Azure Cosmos DB. You need to configure Always Encrypted to encrypt the sensitive data inside the application. What should you do first?

- A. Create a customer-managed key (CMK) and store the key in a new Azure Key Vault instance.
- B. Create an Azure AD managed identity and assign the identity to a new Azure Key Vault instance.
- C. Create a data encryption key (DEK) by using the Azure Cosmos DB SDK and store the key in Azure Cosmos DB.
- D. Create a new container to include an encryption policy with the JSON properties to be encrypted.

Correct Answer: C

Section: