QBank Quiz May 16, 2022

Test ID: 209306473

Question #1 of 135

Question ID: 1287184

You are the administrator of the Nutex Corporation. You want to configure OAuth 2.0 authentication for your API in the API management service. You need to choose the right authorization grant type. You have some third-party clients that you do not trust. You need to configure specific user permissions to access the data.

Which setting should you choose when you add the OAuth2 service to your API?

A) Resource Owner Password

B) Implicit

C) Client Credentials

D) Authorization Code

Explanation

You would use the Implicit authorization type. This authorization type is intended to be used for user-agent-based clients that cannot keep a client secret because all of the application code and storage is easily accessible. Therefore, you would use this authorization type for untrusted third-party clients. The authorization server returns an access token.

You would not use the Authorization Code authorization type. This authorization type returns an authorization code which is exchanged for an access token and is used with public or confidential clients. You should not use this authorization type for untrusted third-party clients.

You would not use Resource Owner Password, because this type grants access to a protected resource for trusted first-party clients on the web and in native device applications. You should not use this authorization type for untrusted third-party clients.

You would not use Client Credentials because this is the simplest of all the OAuth 2.0 grants. This grant is suitable for machine-to-machine authentication, where a specific user permission to access data is not required. You should not use this authorization type for untrusted third-party clients.

Objective:
Implement Azure security

Sub-Objective:
Implement user authentication and authorization

References:

Alex Bilbie > A Guide to Oauth 2.0 Grants

OAuth > OAuth 2.0 > OAuth Grant Types

Microsoft Azure > API Management > How to authorize developer accounts using OAuth 2.0 in Azure API Management

Question #2 of 135

Question ID: 1403553

You are the administrator of the Nutex Corporation. You want to upload an nginx image to Azure Container Registry.

Which of the following commands is the correct one?

A) `docker run -it --rm -p 8080:80 myregistry.azurecr.io/samples/nginx`

B) `docker rmi myregistry.azurecr.io/samples/nginx`

C) `az acr login`

D) `docker run -it --rm -p 8080:80 nginx`

E) `docker push myregistry.Azurecr.io/samples/nginx`

F) `docker pull nginx`

G) `docker login`

H) `docker tag nginx myregistry.azurecr.io/samples/nginx`

Explanation

You would use `docker push myregistry.Azurecr.io/samples/nginx`. The `docker push` command allows you to upload an image or a repository to the Azure Container Registry.

You would not use the `az acr login` command because this command allows you to log in to the Azure Container Registry service.

You would not use the `docker login` command because this command allows you to log in to Docker.

You would not use the `docker pull nginx` command. With this command you download (pull) the public nginx image to your local computer.

You would not use the `docker run -it --rm -p 8080:80 nginx` command. This command allows you to run the container locally.

You would not use the `docker tag nginx myregistry.Azurecr.io/samples/nginx` command, because with this command you create an alias of the image.

You would not use the `docker run -it --rm -p 8080:80 myregistry.azurecr.io/samples/nginx` command because with this command you run the image you have pulled from your registry.

You would not use the `docker rmi myregistry.azurecr.io/samples/nginx command` because with this command you delete the image.

Objective:
Develop Azure compute solutions

Sub-Objective:
Implement IaaS solutions

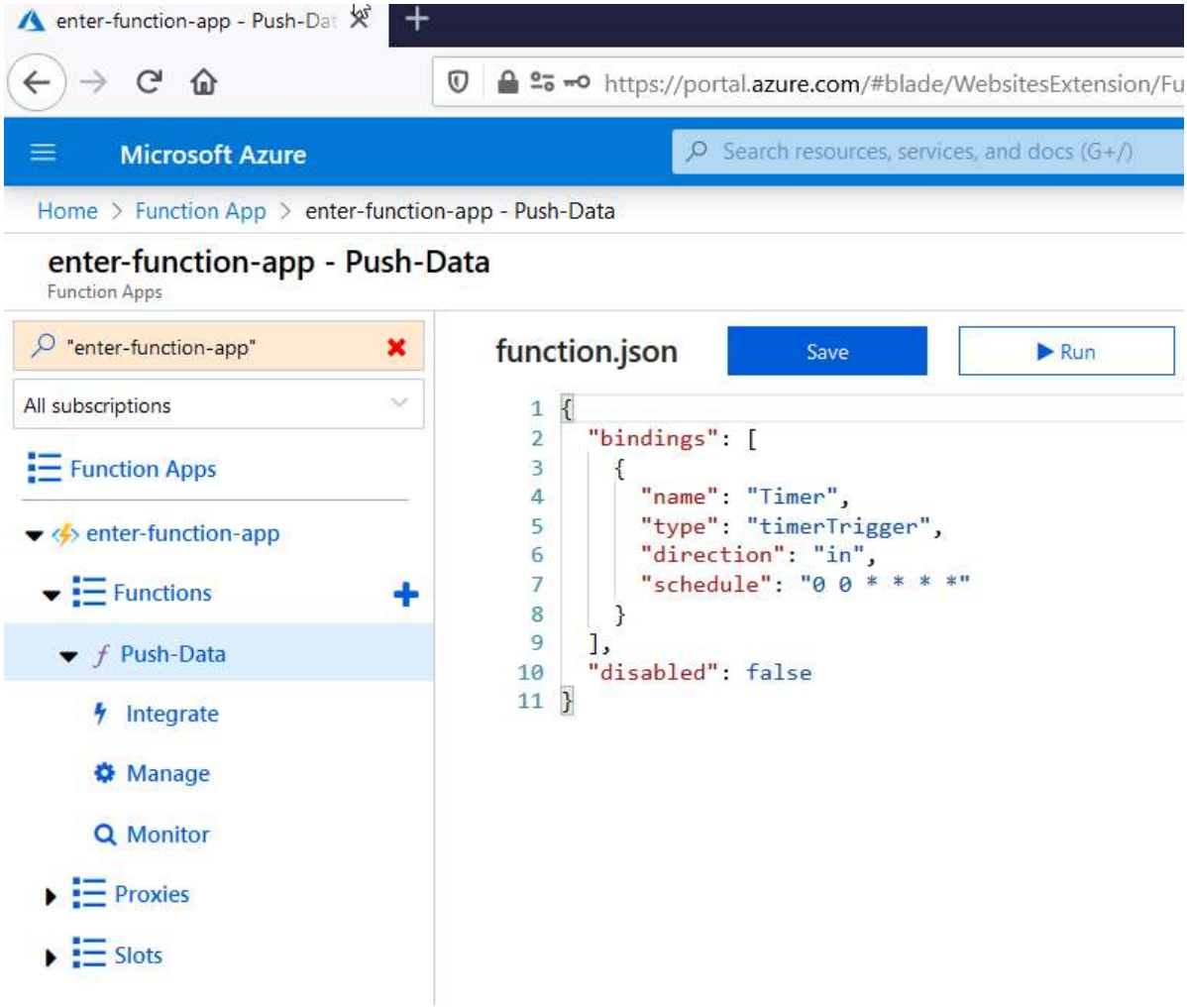
References:

Microsoft Azure > Container Registry > Push your first image to a private Docker container registry using the Docker CLI

Question #3 of 135

Question ID: 1404418

You are working as a senior developer for the Nutex Corporation. Your colleague created a function to send data to your Nutex Corporation subsidiary. The trigger of that function is displayed in the following graphic:



You need to run this function every weekday at 7 AM.

How should you modify **function.json**?

A)

```
{
    "bindings": [
      {
        "name": "Timer",
        "type": "timerTrigger",
        "direction": "in",
        "schedule": "0 7 1-5 * * *"
      }
    ],
    "disabled": false
}
```

B)
```
{
    "bindings": [
      {
        "name": "Timer",
        "type": "timerTrigger",
        "direction": "in",
        "schedule": "0 0 0 7 1-5 *"
      }
    ],
    "disabled": false
  }
```

C)
```
{
    "bindings": [
      {
        "name": "Timer",
        "type": "timerTrigger",
        "direction": "in",
        "schedule": "0 0 7 1-5 * *"
      }
    ],
    "disabled": false
  }
```

D)
```
{
    "bindings": [
      {
        "name": "Timer",
        "type": "timerTrigger",
        "direction": "in",
        "schedule": "0 0 7 * * 1-5"
      }
    ],
    "disabled": false
  }
```

Explanation

You would modify **function.json** as follows:

```
{
  "bindings": [
    {
      "name": "Timer",
      "type": "timerTrigger",
      "direction": "in",
      "schedule": "0 0 7 * * 1-5"
    }
  ],
  "disabled": false
}
```

The function uses Cron Style (NCRONTAB expressions) for scheduling, in the format second, minute, hour, day, month, and day of week**.** The value `"0 0 7 * * 1-5"` states that the function runs at 07:00 am, not every day but only Monday through Friday**.**

You would not modify **function.json** as follows:

```
{
  "bindings": [
    {
      "name": "Timer",
      "type": "timerTrigger",
      "direction": "in",
      "schedule": "0 0 0 7 1-5 *"
    }
  ],
  "disabled": false
}
```

The line "**schedule": "0 0 0 7 1-5 ***" means that the function runs at 12:00 am, on day 7 of the months January through May.

You would not modify **function.json** as follows:

```
{
  "bindings": [
    {
      "name": "Timer",
      "type": "timerTrigger",
      "direction": "in",
      "schedule": "0 0 7 1-5 * *"
    }
  ],
  "disabled": false
}
```

The line "**schedule": "0 0 7 1-5 * ***" means that the function runs at 07:00 am, from day 1 to day 5 of the month.

You would not modify **function.json** as follows:

```
{
  "bindings": [
    {
      "name": "Timer",
      "type": "timerTrigger",
      "direction": "in",
      "schedule": "0 7 1-5 * * *"
    }
  ],
  "disabled": false
}
```

The line "**schedule": "0 7 1-5 * * ***" means that the function runs at 7 minutes past the hour, between 01:00 am and 05:59 am.

Objective:
Develop Azure compute solutions

Sub-Objective:
Implement Azure functions

References:

Cron Expression Descriptor > Describes Cron expressions as human readable text

Microsoft Azure > Functions > Timer trigger for Azure Functions

Question #4 of 135

Question ID: 1287152

You are working as an Azure developer for your company and are involved in an application review for a corporate system implemented around the globe. You want to split your Cosmo DB across containers and in this way provide guaranteed throughput for each container.

What would you consider first?

A) Data access patterns

B) Retry logic in your application

C) Throughput for each container

D) Create a partition key for each container

Explanation

You would first create a partition key for each container. All containers created inside a database with a provisioned throughput must be created with a partition key. If you provision throughput on a container, the throughput is guaranteed for that container, backed by the SLA. A good partitioning strategy is a primary role in cost optimization in Azure Cosmos DB.

You would not consider the throughput for each container. The throughput for the container can be adjusted later.

You would not retry logic in your application first. Retry logic is a code implementation pattern than can always be fixed.

You would not consider data access patterns. These patterns are code implementation patterns than can always be fixed at a later stage.

Objective:
Develop for Azure storage

Sub-Objective:
Develop solutions that use Cosmos DB storage

References:

Microsoft Azure > Cosmos DB > Provision throughput on containers and databases

Microsoft Azure > Cosmos DB > Optimize provisioned throughput cost in Azure Cosmos DB

Question #5 of 135

Question ID: 1287191

You work as an Azure architect for your company and are involved in an application review for a corporate system implemented around the globe via regions in Azure. The system is installed on a VM that looks for new vaccines and automatically interacts with a blob storage account by sending and receiving sensitive DNA data. Every branch which contains a VM uploads and downloads data to a different blob storage account. Currently, there are five thousand VMs across multiple Azure regions operating worldwide. Your company does not want to change the infrastructure. Permission for downloaded data depends on the location and is often changed. The audited code is as follows:

```
public async Task ConnectionStringAsync()
    {
        string connectionString = ConnectionString;
        BlobServiceClient service = new BlobServiceClient(connectionString);
        await service.GetPropertiesAsync();
    }
```

Security is the company's primary goal. What change would you make to better secure the application?

A) Use Key Vault to store credentials in the storage account.

B) Use a token credential that can use an Azure Active Directory application to authenticate.

C) Use Azure AD OAuth2 Implicit grant flow to authenticate.

D) Use Active Directory Federation Services to authenticate.

E) Use Azure AD-managed identities.

F) Use SAS tokens.

G) Use a third party solution such as KeyCloak or Ping.ID.

Explanation

You would use Azure AD-managed identities. The managed identities for Azure resources solves the problems of logins and passwords. Azure AD-managed identities provides Azure services with a managed identity in Azure AD. You can use the identity to authenticate to Key Vault or any service that uses Azure AD authentication, without needing to provide credentials in your code. The code that runs on the VM requests a token from two endpoints that are accessible only from the VM. You can use Managed Identity in permissions definition for different storage accounts.

You would not use SAS tokens because the permission for downloaded data depends on the location and is often changed. SAS tokens do not resolve problems of often-changed permissions.

You would not use the Azure AD Oauth2 Implicit grant flow. A suitable scenario for the OAuth2 Implicit grant flow is to enable user-agent applications, such as JavaScript applications executing within a browser. Azure AD Oauth2 Implicit grant flow will not integrate with Azure Active Directory for storage of logins and passwords.

Using Active Directory Federation Services (ADFS) is not a complete solution and needs more changes. You need to implement ADFS as two additional virtual machines and integrate it with Active Directory. The question asks what changes you should implement in the code, not to build a new infrastructure.

Using a third-party solution such as KeyCloak or Ping.ID is not a complete solution. It is not the best answer because you need to implement KeyCloak or PingID on additional virtual machines and integrate it with Azure Active Directory. The question asks what changes you should implement in the code, not to build a new infrastructure.

You would not use a token credential that can use an Azure Active Directory application to authenticate. This solution still needs to store a login and password in the code.

You would not use Key Vault to store credentials in the storage account. While Key Vault can store SAS tokens, it does not resolve the problem of often-changed permissions.

Objective:
Implement Azure security

Sub-Objective:
Implement secure cloud solutions

References:

Microsoft Docs > Azure > Active Directory > Tutorial: Use a Windows VM system-assigned managed identity to access Azure Storage

---

Question #6 of 135

Question ID: 1403554

You prepare an application for Azure Kubernetes Service (AKS). The application consists of a front-end web component and a backend Redis instance. The web component is packaged into a custom container image. You download the application, create the container image, download the Redis image, and start the application.

You want to deploy an Azure Container Registry (ACR) instance and push the container image to it.

Choose the appropriate steps and place them in the correct order.

{UCMS id=6276178862145536 type=Activity}

Explanation

You would perform the following steps:

1. Create a resource group with the **az group create** command.
2. Create an Azure Container Registry with the **az acr create** command.
3. Tag each container image with the *loginServer* name of the registry.
4. Push the appropriate image to the registry.

You will first need to create a resource group in order to deploy an Azure Container Registry. The Azure resource group will be the logical container where the Azure resources will be deployed and managed. You can use the **az group create** command to create a resource group. The following creates a resource group named NutexResourceGroup in the eastus region:

```
az group create --name NutexResourceGroup --location eastus
```

You will need to create an Azure Container Registery (ACR). You can use the **az acr create** command to create the ACR, as follows. The ACR must have a unique name.

```
az acr create --resource-group NutexResourceGroup  --name acrNutex --sku Basic
```

You will then need to tag the images. Each container image needs to be tagged with the *loginServer* of the registry. The tag is needed for routing and pushing container images to an image registry. To find the the loginServer name, use the **az acr list** command. You can use the **docker images** command to list the images. Once you locate the appropriate image, you can use the **docker tag** command to tag the image with the loginServer of the container registry. The following tags the azure-MyApp image with the loginServer of the container registry, and adds :**v1** to the end of the image name:

```
docker tag azure-Myapp acrNutex/azure-Myapp:v1
```

Once the image has been tagged, you would push the image to the registry with the **docker push** command. The following pushes the image to the acrNutex loginServer:

```
docker push azure-Myapp acrNutex/azure-Myapp:v1
```

You would not use the **docker-compose up** command to upload the image to the registry. This command is used to automate the build out of container images and the deployment of multi-container applications, but does not upload an image to the ACR.

Objective:
Develop Azure compute solutions

Sub-Objective:
Implement IaaS solutions

References:

Microsoft Azure > AKS > Tutorial: Deploy and use Azure Container Registry

---

Question #7 of 135

Question ID: 1287201

You are working as a developer for the Nutex Corporation. You are responsible for an online e-store system using PHP 7.4 with Azure CDN that uses default settings, which has been in place for more than ten months. You figured out that some content that is dedicated to specific people and/or for specific cooperating companies should not be cached.

How can you achieve this?

A) Use .htaccess.

B) Use headers in your e-store system.

C) Use token authentication.

D) Use caching rules in CDN.

Explanation

You would use token authentication. You can use token authentication to prevent the Azure Content Delivery Network (CDN) from serving assets to unauthorized clients. Token authentication prevents hotlinking, which is when a different website links to an asset of yours such as a message board without

permission to do so. Token authentication on CDN ensures that requests are authenticated by a CDN edge server prior to delivery of the content.

You would not use .htaccess. You can use .htaccess to configure PHP in a limited way, but not to prevent caching for specific destinations.

You would not use caching rules in CDN, nor would you use headers in your e-store system. Both of these methods are ways to control the time to live (TTL) for content in CDN, but will not prevent caching for specific destinations. CDN allows files from publicly accessible origin web servers to be cached for as long as their time to live (TTL) allows. The `Cache-Control` header determines the time of the TTL in the HTTP response from the origin server.

The expiration of web content in Azure CDN can be done in the following ways:

- Setting Cache-Control headers by using CDN caching rules.
- Setting Cache-Control headers by using configuration files.

Objective:
Monitor, troubleshoot, and optimize Azure solutions

Sub-Objective:
Integrate caching and content delivery within solutions

References:

Microsoft Azure > Networking > CDN > Securing Azure CDN assets with token authentication

---

Question #8 of 135

Question ID: 1287181

You are the administrator of the Nutex Corporation. You have requested a user delegation key to sign your shared access signatures (SAS) to secure Azure storage resources with Azure AD credentials. You want to implement that through the stored access policy feature.

For which kind of Azure storage can you implement a user delegation SAS in this way?

A) Queues
B) File shares
C) It is not possible
D) Tables
E) Blob service

Explanation

You cannot implement user delegation SAS through the stored access policy feature. Stored access policies are not supported for a user delegation SAS. A user delegation SAS is only supported for the Blob service.

You would not use the Blob service because you want to use the stored access policy feature to implement user delegation SAS. The user delegation SAS feature is supported only for Blob service directly.

You would not use File shares because the user delegation SAS feature is not possible for File shares.

You would not use Queues because the user delegation SAS feature is not possible for Queues.

You would not use Tables because the user delegation SAS feature is not possible for Tables.

Objective:
Implement Azure security

Sub-Objective:
Implement user authentication and authorization

References:

Microsoft Azure > Storage Services > Create a user delegation SAS

Microsoft Azure > Storage Services > Define a stored access policy

Microsoft Azure > Blog > Announcing user delegation SAS tokens preview for Azure Storage Blobs HYPERLINK "https://azure.microsoft.com/en-us/blog/announcing-user-delegation-sas-tokens-preview-for-azure-storage-blobs/"

Question #9 of 135

Question ID: 1287195

You are the administrator of the Nutex Corporation. You have created a resource group for your CDN profile, and you have given Azure AD application permission to manage CDN profiles and endpoints within that group. Now you want to create your project. For authentication, you use ADAL to retrieve a token.

Which constant do you NOT need?

A) backendAddressPools

B) endpointName

C) clientID

D) subscriptionId

E) clientSecret

F) profileName

G) resourceLocation

H) authority

I) resourceGroupName

Explanation

Constants need to be defined so that they can be used by methods. You can add constants in the `Program` class before the `Main` method. When adding constants, the values need to be in quotes. The following adds constants for the tenant app and the application:

```
//Tenant app constants
private const string clientID = "<YOUR CLIENT ID>";
private const string clientSecret = "<YOUR CLIENT AUTHENTICATION KEY>"; //Only for service principals
private const string authority = "https://login.microsoftonline.com/<YOUR TENANT ID>/<YOUR TENANT DOMAIN NAME>";

//Application constants
private const string subscriptionId = "<YOUR SUBSCRIPTION ID>";
private const string profileName = "CdnConsoleApp";
private const string endpointName = "<A UNIQUE NAME FOR YOUR CDN ENDPOINT>";
private const string resourceGroupName = "CdnConsoleTutorial";
private const string resourceLocation = "<YOUR PREFERRED AZURE LOCATION, SUCH AS Central US>";
```

The `backendAddressPools` constant is part of an Azure load balancing deployment and not CDN.

Objective:
Monitor, troubleshoot, and optimize Azure solutions

Sub-Objective:
Integrate caching and content delivery within solutions

References:

Microsoft Azure > Networking > CDN > Get started with Azure CDN development

Microsoft Azure > Load Balancer > Load Balancers - Create Or Update

Question #10 of 135

Question ID: 1287125

You need to monitor containers with Log Analytics. You need to get information from error logs about an image name “ubuntu” that has failed. You find the container name as **UbuntuContainer1** by typing the following search in Log Analytics:

```
ContainerInventory | where Image == "ubuntu" and ContainerState == "Failed"
```

You type the following search to find the error logs that have information on **UbuntuContainer1**:

[ ] | where Name == “UbuntuContainer1”

Type the missing code in the textbox provided.

Explanation

Acceptable answer(s) for field 1:

- ContainerLog

You would type **ContainerLog.** This data type can display any log entries, container IDs, container names, when an entry was generated, the computer name, the log entry source, and the source system.

Objective:
Develop Azure compute solutions

Sub-Objective:
Implement IaaS solutions

References:

Microsoft Azure > Azure Monitor > Container Monitoring solution in Azure Monitor

Question #11 of 135

Question ID: 1403561

You are working as a developer for the Nutex Corporation. You are responsible for developing a new online e-store system using PHP 7.4. You need to add a custom .dll extension to PHP.

How can you achieve this? (Choose all that apply.)

A) Use a custom PHP runtime.
B) Add `php.ini` to the `wwwroot` directory.
C) Add `.htaccess` to the `wwwroot` directory.
D) Add `PHP_INI_SCAN_DIR` to App Settings.
E) Enable Composer automation in Azure.
F) Add the `PHP_EXTENSIONS` key in the **Application Settings** section of the Configuration blade.

Explanation

You would do the following:

- Add `PHP_INI_SCAN_DIR` to App Settings.
- Add the `PHP_EXTENSIONS` key in the **Application Settings** section of the Configuration blade.

You can enable extensions in the default PHP runtime by putting the `extension.dll` and `extensions.ini` files with the correct content into the directory. You can add `PHP_INI_SCAN_DIR` Application Settings that point to the `extensions.ini` file. Alternatively, you can add `PHP_EXTENSIONS` to the Application Settings

section of the Configuration blade.

You would not use a custom PHP runtime. This solution could resolve the problem if that extension is compiled to a custom PHP, but the scenario does not mention that the extension will be compiled to a custom PHP.

You would not enable Composer automation in Azure. Composer automation allows you to perform git add, git commit, and git push to your app. Composer automation will not add a custom .dll extension to PHP.

You would not add `php.ini` to the `wwwroot` directory. A `php.ini` file does not work in the web app.

You would not add `.htaccess` to the `wwwroot` directory because `.htaccess` cannot load an extension.

Objective:
Develop Azure compute solutions

Sub-Objective:
Create Azure App Service Web Apps

References:

Microsoft Azure > App Service > Web Apps > Configure PHP in Azure App Service

---

Question #12 of 135

Question ID: 1287228

You are the administrator of the Nutex Corporation. You want to use the API Management Azure service.

Which of the following statements about API management service are correct? (Choose all that apply.)

A) Create consistent and API gateways.
B) Publish your API's to external developers.
C) Enable a virtual network gateway.
D) Manage Application Gateway.

Explanation

You would publish your API's to external developers because Azure API management (APIM) helps organizations publish APIs to external, partner, and internal developers to get the most out of their data and services.

You would create consistent API gateways because APIM enables you to create modern API gateways for existing backend services that are hosted anywhere. The API gateway is the endpoint that accepts API calls and routes them to your backends, verifies API keys, JWT tokens, certificates, and other credentials, and enforces usage quotas and rate limits.

You would not enable a virtual network gateway because you cannot enable virtual network gateways through APIM.

You would not choose to manage Application Gateway because you cannot manage or create Application gateways with APIM.

Objective:
Connect to and consume Azure services and third-party services

Sub-Objective:
Implement API management

References:

Microsoft Azure > About API Management

Question #13 of 135

Question ID: 1287108

You are the administrator of the Nutex Corporation. You want to deploy an ARM template using C#. The template deploys a single virtual machine in a new virtual network with a single subnet. You create the Visual Studio project and install the necessary NuGet packages.

You need to create the necessary template files. Which files you should you create? (Choose three.)

A) Parameters.json
B) CreateVMTemplate.json
C) CreateVMTemplate.txt
D) Parameters.properties
E) azureauth.properties
F) azureauth.json

Explanation

You need to create a template file, a parameter file, and an authorization file. You would create the following files:

- **CreateVMTemplate.json** as the template file
- **Parameters.json** as the parameters file
- **azureauth.properties** as the authorization file.

Of the above choices, you would create the file named **CreateVMTemplate.json** for the template file. The file can have any name, but an ARM template must always have the **.json** file extension.

You would use **Parameters.json** as the name of the parameter file. The parameter file specifies values for the resource parameters in the template and needs the **.json** file extension.

You would use **azureauth.properties** as the name of the authorization file, because the ARM template authorization file must have the file extension name ***.properties***.

You would not use **CreateVMTemplate.txt** as the name of the template file, because an ARM template file cannot work with the **.txt** file extension.

You would not use **Parameters.properties** as the name of the parameters file, because an ARM parameter file must have the **.json** file extension.

You would not use **azureauth.json** as the name of the authorization file, because an authorization file does not work with the **.json** file extension. Instead it has to have the **.properties** file extension.

Objective:
Develop Azure compute solutions

Sub-Objective:
Implement IaaS solutions

References:

Microsoft Azure > Virtual Machines > Windows > Deploy an Azure Virtual Machine using C# and a Resource Manager template

---

Question #14 of 135

Question ID: 1287159

You are the administrator of the Nutex Corporation. You have to develop a web application, which relies on Azure table storage data. For better load balancing, more partitions are required. You have to plan your partition scheme and the partition keys for each entity. You have to describe the advantages and disadvantages of different partition keys with their respective sizes.

Which of the following are true? (Choose all that apply.)

A) Using a unique partition key for every entity does not allow for entity group transactions.

B) An application can perform multiple insert, update, delete, replace, or merge operations as an atomic unit in an Azure table, as long as the transaction does not include more than 1,000 entities and the payload of the request does not exceed 16 MB.

C) You should hash the partition keys that are generated using a monotonic sequence (such as "0001", "0002", "0003"), and each partition only contains a limited amount of data.

D) Using a unique partition key for every entity makes it possible to group related entities in the same partition.

E) The same partition key for every entity results in a single partition that is held on one server.

F) Using a unique partition key for every entity prevents the partition from scaling out and focuses the load on a single server.

Explanation

The following are true:

- The same partition key for every entity results in a single partition that is held on one server.
- Using a unique partition key for every entity does not allow for entity group transactions.
- You should hash the partition keys that are generated using a monotonic sequence (such as "0001", "0002", "0003"), and each partition only contains a limited amount of data.

A partition key is used to group related or similar entities. The granularity of the partition key determines the partition size. If you have the same partition key for every entity then a single partition is held on one server. The partition will not be able to scale out and the load will be on that one server. You should only take this approach if you are storing a small number of entities. When you have the same partition key for every entity, all entities can participate in enitity group transactions.

You can create a separate partition for each entity in an Azure table storage service by using a unique partition key for every entity. This approach results in lots of small partitions. Although it may be more scalable than using the same partition key, you cannot have entity group transactions by using a unique partition key for every entity.

If the partition keys are generated in a monotonic sequence, such as "0001", "0002", "0003", and each partition only contains a limited amount of data, then Azure table storage will group the partitions on the same server. Azure storage optimizes queries based on the assumption that the application is most likely to perform queries across a contiguous range of partitions. Unfortunately, this optimization can reduce scalability because insertions of new entities are likely to be concentrated at one end of the contiguous range. To ensure that the load is distributed evenly, you should hash the partition key.

The limit for a transaction of an application that performs multiple insert, update, delete, replace, or merge operations as an atomic unit in an Azure table is no more than 100 enities, not 1,000, and the payload of the request maximum is 4 MB, not 16 MB.

Using a unique partition key for every entity prevents entity group transactions.

Using a unique partition key for every entity does not prevent the partition from scaling out and focusing the load on a single server. This happens if you use a single partition key for every entity.

Objective:
Develop for Azure storage

Sub-Objective:
Develop solutions that use Cosmos DB storage

References:

Microsoft Azure > Architecture > Best Practices > Data partitioning strategies

C# Corner > Azure Table Storage Design Manage and Scale Table Partitions

C# Corner > Introduction To Azure Table Storage

Question #15 of 135

Question ID: 1422640

You are the administrator of the Nutex Corporation. You want to do the following tasks:

Copy a blob to another storage account.

Copy a directory to another storage account.

Copy a container to another storage account.

Copy all containers, directories, and blobs to another storage account.

You have the following AzCopy commnds:

Example A:

```
azcopy copy 'https://mysourceaccount.blob.core.windows.net/mycontainer/myTextFile.txt?sv=2018-03-28&ss=bfqt&srt=sco&sp=rwdlacup&se=2019-07-04T05:30:08Z&st=2019-07-03T21:30:08Z&spr=https&sig=CAfhgnc9gdGktvB=ska7bAiqIddM845yiyFwdMH481QA8%3D' 'https://mydestinationaccount.blob.core.windows.net/mycontainer/myTextFile.txt'
```

Example B:

```
azcopy copy 'https://mysourceaccount.blob.core.windows.net/mycontainer/myBlobDirectory?sv=2018-03-28&ss=bfqt&srt=sco&sp=rwdlacup&se=2019-07-04T05:30:08Z&st=2019-07-03T21:30:08Z&spr=https&sig=CAfhgnc9gdGktvB=ska7bAiqIddM845yiyFwdMH481QA8%3D' 'https://mydestinationaccount.blob.core.windows.net/mycontainer' -recursive
```

Example C:

```
azcopy copy 'https://mysourceaccount.blob.core.windows.net/mycontainer?sv=2018-03-28&ss=bfqt&srt=sco&sp=rwdlacup&se=2019-07-04T05:30:08Z&st=2019-07-03T21:30:08Z&spr=https&sig=CAfhgnc9gdGktvB=ska7bAiqIddM845yiyFwdMH481QA8%3D' 'https://mydestinationaccount.blob.core.windows.net/mycontainer' -recursive
```

Example D:

```
azcopy copy 'https://mysourceaccount.blob.core.windows.net?sv=2018-03-28&ss=bfqt&srt=sco&sp=rwdlacup&se=2019-07-04T05:30:08Z&st=2019-07-03T21:30:08Z&spr=https&sig=CAfhgnc9gdGktvB=ska7bAiqIddM845yiyFwdMH481QA8%3D' 'https://mydestinationaccount.blob.core.windows.net' -recursive
```

Which of the AzCopy command examples applies to which task? Match the appropriate AzCopy command to the correct example.

{UCMS id=4600148949729280 type=Activity}

Explanation

You should choose the following:

You can use the following example to copy a blob to another storage account:

```
azcopy copy 'https://mysourceaccount.blob.core.windows.net/mycontainer/myTextFile.txt?sv=2018-03-28&ss=bfqt&srt=sco&sp=rwdlacup&se=2019-07-04T05:30:08Z&st=2019-07-
```

03T21:30:08Z&spr=https&sig=CAfhgnc9gdGktvB=ska7bAiqIddM845yiyFwdMH481QA8%3D'
'https://**mydestinationaccount**.blob.core.windows.net/**mycontainer**/**myTextFile.txt**'

This command uses the following syntax:

azcopy copy 'https://<source-storage-account-name>.blob.core.windows.net/<container-name>/<blob-path>?<SAS-token>'
'https://<destination-storage-account-name>.blob.core.windows.net/<container-name>/<blob-path>'

In the above example, **mysourceaccount** is the source storage account. The value of the first **mycontainer** is the container name. The blob path is the first **myTextFile.txt**. The SAS token is represented by *sv=2018-03-28&ss=bfqt&srt=sco&sp=rwdlacup&se=2019-07-04T05:30:08Z&st=2019-07-03T21:30:08Z&spr=https&sig=CAfhgnc9gdGktvB=ska7bAiqIddM845yiyFwdMH481QA8%3D*. The destination storage account is **mydestinationaccount**. The destination container is the second **mycontainer**. The destination blob path is the second **myTextFile.txt**.

You can use the following example to copy a directory to another storage account:

azcopy copy 'https://**mysourceaccount**.blob.core.windows.net/**mycontainer**/**myBlobDirectory**?*sv=2018-03-28&ss=bfqt&srt=sco&sp=rwdlacup&se=2019-07-04T05:30:08Z&st=2019-07-03T21:30:08Z&spr=https&sig=CAfhgnc9gdGktvB=ska7bAiqIddM845yiyFwdMH481QA8%3D'*
'https://**mydestinationaccount**.blob.core.windows.net/**mycontainer**' --recursive

The above example uses the following syntax:

azcopy copy 'https://<source-storage-account-name>.blob.core.windows.net/<container-name>/<directory-path>?<SAS-token>'
'https://<destination-storage-account-name>.blob.core.windows.net/<container-name>' –recursive

In the above example, **mysourceaccount** is the source storage account. The value of the first **mycontainer** is the container name. The directory path is **myBlobDirectory**. The SAS token is represented by *sv=2018-03-28&ss=bfqt&srt=sco&sp=rwdlacup&se=2019-07-04T05:30:08Z&st=2019-07-03T21:30:08Z&spr=https&sig=CAfhgnc9gdGktvB=ska7bAiqIddM845yiyFwdMH481QA8%3D*. The destination storage account is **mydestinationaccount**. The destination container is the second **mycontainer**. The `--recursive` parameter checks sub-directories when coping from a local file system.

You would use the following example to copy a container to another storage account:

azcopy copy 'https://**mysourceaccount**.blob.core.windows.net/**mycontainer**?*sv=2018-03-28&ss=bfqt&srt=sco&sp=rwdlacup&se=2019-07-04T05:30:08Z&st=2019-07-03T21:30:08Z&spr=https&sig=CAfhgnc9gdGktvB=ska7bAiqIddM845yiyFwdMH481QA8%3D'*
'https://**mydestinationaccount**.blob.core.windows.net/**mycontainer**' –recursive

The above example uses the following syntax:

azcopy copy 'https://<source-storage-account-name>.blob.core.windows.net/<container-name>?<SAS-token>' 'https://<destination-storage-account-name>.blob.core.windows.net/<container-name>' –recursive

In the above example, **mysourceaccount** is the source storage account. The value of the first **mycontainer** is the container name. The directory path is **myBlobDirectory**. The SAS token is represented by *sv=2018-03-28&ss=bfqt&srt=sco&sp=rwdlacup&se=2019-07-04T05:30:08Z&st=2019-07-03T21:30:08Z&spr=https&sig=CAfhgnc9gdGktvB=ska7bAiqIddM845yiyFwdMH481QA8%3D*. The destination storage account is **mydestinationaccount**. The destination container is the second **mycontainer**. The `--recursive` parameter checks sub-directories when coping from a local file system.

You would use the following example to copy all containers, directories, and blobs to another storage account:

azcopy copy 'https://**mysourceaccount**.blob.core.windows.net?s*v=2018-03-28&ss=bfqt&srt=sco&sp=rwdlacup&se=2019-07-04T05:30:08Z&st=2019-07-03T21:30:08Z&spr=https&sig=CAfhgnc9gdGktvB=ska7bAiqIddM845yiyFwdMH481QA8%3D'*
'https://**mydestinationaccount**.blob.core.windows.net' –recursive

The above example uses the following syntax:

azcopy copy 'https://<source-storage-account-name>.blob.core.windows.net/?<SAS-token>' 'https://<destination-storage-account-name>.blob.core.windows.net/' --recursive'

In the above example, **mysourceaccount** is the source storage account. The SAS token is represented by *sv=2018-03-28&ss=bfqt&srt=sco&sp=rwdlacup&se=2019-07-04T05:30:08Z&st=2019-07-03T21:30:08Z&spr=https&sig=CAfhgnc9gdGktvB=ska7bAiqIddM845yiyFwdMH481QA8%3D*. The destination storage account is **mydestinationaccount**. The `--recursive` parameter checks sub-directories when coping from a local file system.

Objective:
Develop for Azure storage

Sub-Objective:
Develop solutions that use blob storage

References:

Microsoft Docs > Azure > Storage > Transfer data with AzCopy and Blob storage

---

Question #16 of 135

Question ID: 1403601

You are the administrator of the Nutex Corporation. You develop an event-based solution using Azure queue storage. You want to add a message that does not expire. You create the following code:

```
await theQueue.AddMessageAsync(message, MISSING
, null, null, null);
```

Which of the following is the code that is missing?

A) `Timespan.FromSeconds(1)`

B) `Timespan.FromSeconds(-1)`

C) `TTL.FromSeconds(0)`

D) `Timespan.FromSeconds(0)`

E) `TTL.FromSeconds(1)`

F) `TTL.FromSeconds(-1)`

Explanation

The missing piece of code is `Timespan.FromSeconds(-1)`. A message has a maximum time to live of 7 days by default. You can set the time to live on the message or have the message not expire by using `Timespan.FromSeconds(-1)` in your call to the **AddMessageAsync** method.

If you use `Timespan.FromSeconds(1)`, the time to live is set to 1 second. If you use `Timespan.FromSeconds(0)`, the time to live is set to 0 seconds and the message expires immediately.

You cannot use any number with `TTL.FromSeconds()` with the **AddMessageAsync** method. This can be used with DNS functions.

Objective:
Connect to and consume Azure services and third-party services

Sub-Objective:
Develop message-based solutions

References:

Microsoft Docs > Azure > Storage > Tutorial: Work with Azure storage queues

---

Question #17 of 135

Question ID: 1403565

You are the administrator of the Nutex Corporation. You have the following CRON expression for your Azure function:

```
[FunctionName("TimerTriggerCSharp")]
public static void Run([TimerTrigger("0 */5 * * * *")]TimerInfo myTimer, ILogger log)
{
```

```
    if (myTimer.IsPastDue)
    {
        log.LogInformation("Timer is running late!");
    }
    log.LogInformation($"C# Timer trigger function executed at: {DateTime.Now}");
}
```

Which hosting plan must you use to run the Timer trigger?

A) Dedicated plan

B) Consumption plan

C) Premium plan

Explanation

The attribute's constructor takes a CRON expression or a TimeSpan. You can use TimeSpan only if the function app is running on a Dedicated App Service plan. TimeSpan is not supported on the Consumption and Premium Plans.

Objective:
Develop Azure compute solutions

Sub-Objective:
Implement Azure functions

References:

Microsoft Azure > Functions > Timer trigger for Azure Functions

Microsoft Azure > Functions > Azure Functions scale and hosting

---

Question #18 of 135

Question ID: 1403562

You are the administrator of the Nutex Corporation. You want to build an ASP.NET Core and SQL database app in Azure App Service. You have created the production SQL database along with an SQL database server-level firewall rule and the connection string. You need to create the Azure app.

Choose the appropriate tasks and place them in the correct order.

{UCMS id=6279897167167488 type=Activity}

Explanation

You would choose the following:

1. Configure the deployment user.
2. Create the App Service plan.
3. Create the web app.
4. Configure the connection string.
5. Configure the environment variable.
6. Connect to the SQL database in production.
7. Push to Azure from Git.

First you would configure the deployment user because you can use FTP and local Git to deploy an Azure web app by using a deployment user. To configure the deployment user, you can use the `az webapp deployment user set` command in Azure Cloud Shell. For example, the following creates a deployment user:

```
az webapp deployment user set --user-name DanQuinn --password N0t@g0odC0@¢h
```

You would then create the App Service plan. Before you can create an Azure web app, you always need an App Service plan. For example, the following creates an App Service plan named NutexServicePlan in the Free pricing tier:

```
az appservice plan create --name NutexServicePlan --resource-group NutexResourceGroup --sku FREE
```

After creating the app service plan, you can create the web app. You can do that with the `az webapp create` command. The following creates a web app named NutexApp in the NutexServicePlan.

```
az webapp create --resource-group NutexResourceGroup --plan NutexServicePlan --name NutexApp --deployment-local-git
```

You would then configure the connection string. You have to configure the SQL database connection string to the web app. You can do that with the `az webapp config connection-string set` command.

Next you would configure environment variables. You have to set the `ASPNETCORE_ENVIRONMENT` app setting to Production. This environment variable lets you know that you are running the app in Azure as opposed to SQLite. You can do that with the `az webapp config appsetting set` command.

You would then connect to the SQL database in production. When the code reads the value of the `ASPNETCORE_ENVIRONMENT` app as the database which is running in production, the connection string that you configured is used to connect to the SQL database.

Then you would push to Azure from Git because with that you deploy your app. You can do that with the `git remote add azure` command.

Objective:
Develop Azure compute solutions

Sub-Objective:
Create Azure App Service Web Apps

References:

Microsoft Azure > App Service > Web Apps > Tutorial: Build an ASP.NET Core and SQL Database app in Azure App Service

---

Question #19 of 135

Question ID: 1287215

You are working as a developer for the Nutex Corporation. You are responsible for an online e-store system using PHP 7.4. You are preparing for the Black Friday and Cyber Monday period. Your CEO is afraid that during this period, Azure Cosmos DB will be overloaded and will not respond fast enough.

What do you propose to use to mitigate Azure Cosmos DB potential problems?

A) Implement Sharding pattern.
B) Implement Transient fault handling.
C) Implement Retry pattern.
D) Implement Competing Consumers pattern.

Explanation

You would implement the Sharding pattern. This pattern is used for splitting data across databases, disks, files, or partitions. It can prevent the Azure Cosmos DB from being overloaded when responding to requests.

You would not implement the Competing Consumers pattern. This type of pattern is used for queue implementation and can be a part of a solution, but it does not prevent the Azure Cosmos DB from being overloaded when responding to requests.

You would not implement the Retry pattern. The Retry pattern improves the stability of an application by allowing an application to retry a failed operation when intermittent failures of connecting to a network resource or a service occur. It will not prevent the Azure Cosmos DB from being overloaded when responding to requests.

You would not implement Transient fault handling. Transient fault handling works well for a function that does work, but not all the time. Transient faults could mean the temporary unavailability of a service because of a sudden loss of network connectivity to components and services, or timeouts that occur when a service is busy. Often these faults are not issues because they are mostly self-correcting, and if the action can be repeated after a short delay, the action more than likely will succeed. However, it will not prevent the Azure Cosmos DB from being overloaded when responding to requests.

Objective:
Monitor, troubleshoot, and optimize Azure solutions

Sub-Objective:
Instrument solutions to support monitoring and logging

References:

Microsoft Azure > Architecture > Cloud Design Patterns > Sharding pattern

---

Question #20 of 135

Question ID: 1403589

You are the administrator of the Nutex Corporation. You have created an Azure function app. You want to document your function app.

Which steps do you need to perform to enable the download of the API definition?

Place the appropriate steps from the left in the correct order on the right.

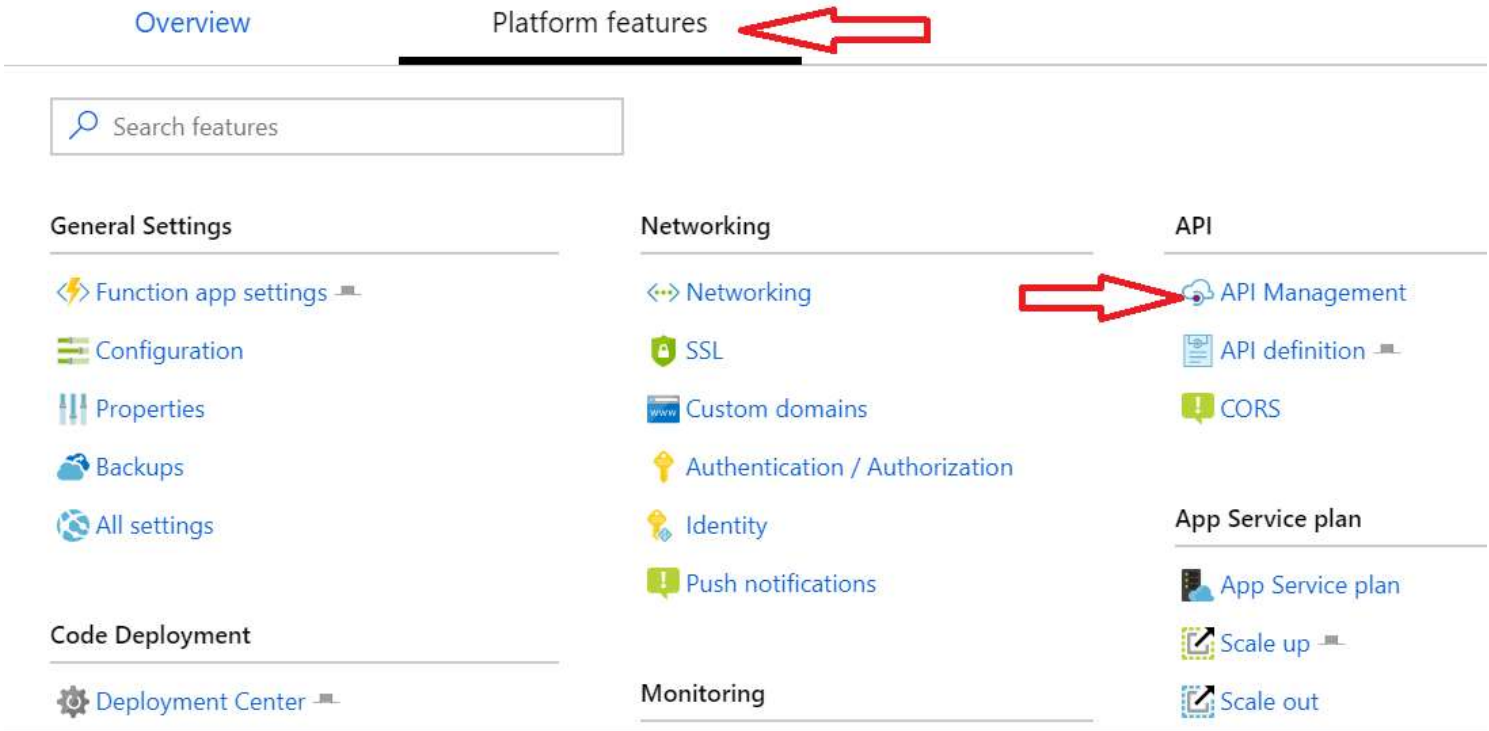
{UCMS id=5680594949242880 type=Activity}

Explanation

You would perform the following steps:

1. Create an API Management service.
2. Enable Application Insights.
3. Link the API.
4. Test the API.

Since you have created the Azure function app, you will need to generate an OpenAPI definition. You should choose your function app, then, in Platform features, choose API Management and select Create new under API Management.



After creating the API Management service, you would enable Application Insights. This action will send logs to the same place as the function application.

You would then select **Link API**.

You must verify that the API works before you use the OpenAPI definition.

Objective:
Monitor, troubleshoot, and optimize Azure solutions

Sub-Objective:
Instrument solutions to support monitoring and logging

References:

Microsoft Azure > Functions > Create an OpenAPI definition for a serverless API using Azure API Management

Microsoft Azure Blog > Announcing the preview of OpenAPI Specification v3 support in Azure API Management

Marketplace Visual Studio > OpenAPI Document Tools

Question #21 of 135

Question ID: 1404428

You are the administrator of the Nutex Corporation. You want to cache .NET objects in Azure Redis Cache. What must you do in Visual Studio?

A) Add the global-packages folder.

B) Add a Newtonsoft.Json package.

C) Disable package cache in Visual Studio.

D) Add StackExchange.Redis.

Explanation

You would add a Newtonsoft.Json package because Azure Cache for Redis can cache both .NET objects and primitive data types. Before a .NET object can be cached, it must be serialized. This .NET object serialization is done by the application developer and gives the developer flexibility in the choice of the serializer.

You would not disable package cache in Visual Studio. The package caches installed packages in Visual Studio in case you need to repair Visual Studio or other related products, if you have no internet connection.

You would not add StackExchange.Redis because this is the basic Redis Cache package.

You would not add the global-packages folder because the global-packages folder is where NuGet installs any downloaded package.

Objective:
Monitor, troubleshoot, and optimize Azure solutions

Sub-Objective:
Integrate caching and content delivery within solutions

References:

Quickstart: Use Azure Cache for Redis in .NET Framework | Microsoft DocsHYPERLINK "https://docs.microsoft.com/en-us/azure/azure-cache-for-redis/cache-dotnet-how-to-use-azure-redis-cache"

Disable or move the package cache - Visual Studio (Windows) | Microsoft Docs

How to manage the global packages, cache, temp folders in NuGet | Microsoft Docs

---

Question #22 of 135

Question ID: 1287145

You are the administrator of the Nutex Corporation. You want to orchestrate the execution of other durable functions within your function app.

Which API category should you NOT have to avoid calling?

A) Threading

B) NewGUID (.NET)

C) Async

D) GUIDs/UUIDs

E) Blocking

Explanation

You would choose NewGuid (.NET) because this is a deterministic API. A deterministic API returns the same value given the same input. Although orchestrator functions can call any API, it is important that orchestrator functions call only deterministic APIs.

You would not use GUIDs/UUIDs, because this API is a non-deterministic API. A non-deterministic API returns a different generated value for every replay.

You would not use Async because the orchestrator code must never initiate any async operation except by using the DurableOrchestrationContext API or context.df objects API.

You would not use Blocking because this can cause performance and scale problems for orchestrator functions and should be avoided. In the Azure Functions Consumption plan, they can even result in unnecessary execution-time charges.

You would not use Threading because the durable task framework executes orchestrator code on a single thread and cannot interact with any other threads. Introducing new threads into an orchestration's execution can result in non-deterministic execution or deadlocks.

Objective:
Develop Azure compute solutions

Sub-Objective:
Implement Azure functions

References:

Microsoft Azure > Function > Orchestrator function code constraints

GitHub > .NET API Reference > Microsoft.Azure.WebJobs > NewGuid()

Question #23 of 135

Question ID: 1403599

You are the administrator of the Nutex Corporation. You have developed an event-based solution that uses Azure Service Bus namespaces. Because you want to use dedicated resources per namespaces for predictable latency and increased throughput, you want to migrate your existing namespaces to the relevant tier.

Place the migration steps in the correct order.

{UCMS id=5658794131456000 type=Activity}

Explanation

You would perform the following steps:

1. Create a new premium namespace.
2. Pair the standard and premium namespaces to each other.
3. Sync (copy-over) entities from the standard to the premium namespace.
4. Commit the migration.
5. Drain entities in the standard namespace by using the post-migration name of the namespace.
6. Delete the standard namespace.

First, you would create a new premium namespace because you must migrate your standard namespace to premium so that you can use dedicated resources per namespace.

Then you would pair the standard and premium namespaces to each other because all entities in the standard namespace must be copied to the premium namespace during the migration process.

Then you would sync (copy-over) entities from the standard to the premium namespace to run the copy process.

Then you would commit the migration.

After the migration has been committed, you must drain the queues and subscriptions from the old standard namespace by using the post-migration name of the namespace. The messages may be sent to the new premium namespace to be processed by the receiver applications after they have been drained.

After the queues and subscriptions have been drained, you would delete the old standard namespace.

Objective:
Connect to and consume Azure services and third-party services

Sub-Objective:
Develop message-based solutions

References:

Microsoft Azure > Messaging services > Service Bus Messaging > Migrate existing Azure Service Bus standard namespaces to the premium tier

---

Question #24 of 135

Question ID: 1287199

You are creating a web application to be deployed to Azure, and you are concerned about the cloud services' performance. You need to improve the user experience for end users who are far from content sources. You decide to use the Azure Content Delivery Network (CDN).

From the following choices, select the option that is incorrect for a CDN.

A) CDN caches content in Azure Blobs at physical locations across the world.

B) Only use the CDN to cache static content.

C) Only publicly available Blobs are cached with CDN.

D) Provides access to content over HTTPS for a site on your custom domain.

Explanation

You would select the option providing access to content over HTTPS for a site on your custom domain. It is actually possible to provide access to content over HTTPS with some limitations. Currently, you cannot use HTTPS with a custom domain name. You have to use the certificate provided by the CDN. You cannot yet use your own domain/SSL certificate with Azure CDN.

You would not select the option that CDN caches content in Azure Blobs at physical locations across the world. As a matter of fact, that is exactly what a CDN does. Having the content cached will maximize the bandwidth for delivering content to users.

You would not select the option that only publicly available Blobs are cached with CDN. Blobs that are in public containers and are available for anonymous access can be cached by the CDN.

You would not select the option to only use the CDN to cache static content. This is actually one of the constraints. The CDN is used to cache static content only.

Objective:
Monitor, troubleshoot, and optimize Azure solutions

Sub-Objective:
Integrate caching and content delivery within solutions

References:

Microsoft Azure > Networking > CDN > What is a content delivery network on Azure?

Ben Foster > Using HTTPS with the Azure CDN

Question #25 of 135

Question ID: 1403585

You are the administrator of the Nutex Corporation. You want to upload a certificate into the certificate portion of an Azure key vault. You want to do that with PowerShell. You must fill the empty spaces in the following PowerShell script:

```
function Add-CertificateToKeyVaultCertificateIfNotExists {
[CmdletBinding()]
    Param(
        [Parameter(Mandatory)] [string] $CertificatePath,
        [Parameter(Mandatory)] [SecureString] $CertificatePassword,
        [Parameter(Mandatory)] [string] $VaultName,
        [Parameter(Mandatory)] [string] $Name,
        [switch] $Replace
    )
     Begin {
        $ErrorActionPreference = 'stop'
    }
     Process {
        $certificate = A
-VaultName $VaultName -Name $Name
         if ($certificate -and $Replace -eq $FALSE) {
            Write-Verbose -Message ('Skipped replacing certificate ‘{0}’ in vault ''{1}''.' -f $VaultName, $Name)
        }
        else {
            if ($Replace -eq $TRUE) {
                $vault = B
-VaultName $VaultName
                if ($vault.EnableSoftDelete) {
                    C
-VaultName $VaultName -Name $Name -InRemovedState -Force
                }
                else {
                    Remove-AzKeyVaultCertificate -VaultName $VaultName -Name $Name -Force
                }}
            D
-VaultName $VaultName -Name $Name -Password $CertificatePassword -FilePath $CertificatePath
        }}}
```

Map the correct code to the corresponding letter.

{UCMS id=6065567061508096 type=Activity}

Explanation

```
function Add-CertificateToKeyVaultCertificateIfNotExists {
    [CmdletBinding()]
    Param(
```

```
        [Parameter(Mandatory)] [string] $CertificatePath,
        [Parameter(Mandatory)] [SecureString] $CertificatePassword,
        [Parameter(Mandatory)] [string] $VaultName,
        [Parameter(Mandatory)] [string] $Name,
        [switch] $Replace
    )

    Begin {
        $ErrorActionPreference = 'stop'
    }

    Process {
        $certificate = Get-AzKeyVaultCertificate -VaultName $VaultName -Name $Name

        if ($certificate -and $Replace -eq $FALSE) {
            Write-Verbose -Message ('Skipped replacing certificate ‘{0}’ in vault ‘{1}’.' -f $VaultName, $Name)
        }
        else {
            if ($Replace -eq $TRUE) {
                $vault = Get-AzKeyVault -VaultName $VaultName
                if ($vault.EnableSoftDelete) {
                    Remove-AzKeyVaultCertificate -VaultName $VaultName -Name $Name -InRemovedState -Force
                }
                else {
                    Remove-AzKeyVaultCertificate -VaultName $VaultName -Name $Name -Force
                }
            }

            Import-AzKeyVaultCertificate -VaultName $VaultName -Name $Name -Password $CertificatePassword -FilePath
$CertificatePath
        }
    }
```

First you would use the **Get-AzKeyVaultCertificate** cmdlet. This cmdlet is used to search for an existing certificate in the key vault. You verify if a certificate exists. If yes, the text `'Skipped replacing certificate…'` will be displayed.

You would use the **Get-AzKeyVault** cmdlet to retrieve and store the key vault in the variable `$vault`.

You would use the **Remove-AzKeyVaultCertificate** cmdlet to remove an existing certificate from the key vault.

You would use the **Import-AzKeyVaultCertificate** cmdlet to upload a new certificate into the key vault.

You would not use the **Remove-AzureKeyVaultManagedStorageAccount** cmdlet. This cmdlet removes a key vault storage account and any SAS definitions. In this scenario, you want to upload a certificate into the certificate portion of an Azure key vault, not remove the key vault.

You would not use the **Get-AzureKeyVaultSecret** cmdlet. This cmdlet retrieves secrets in a key vault. In this scenario, you need to retrieve the certificate in the key vault, not the secrets of the key vault.

Objective:
Implement Azure security

Sub-Objective:
Implement secure cloud solutions

References:

Dominique St-Amand > Loading a X509 certificate from Azure KeyVault into a .NET Core application

Microsoft Azure > Key Vault > Import Certificate

Question #26 of 135

Question ID: 1403583

You work as an Azure developer for your company and are involved in API development. You need to limit access to the API Management service to only the network with the IP address of 192.168.0.0/24.

How should you define the policy?

A)
```
<ip-filter action="forbid">
    <address>192.168.0.0/24</address>
</ip-filter>
```

B)
```
<ip-filter action="allow">
    <address>192.168.0.0/24</address>
</ip-filter>
```

C)
```
<ip-filter action="allow">
    <address-range from="192.168.0.0" to="192.168.0.254"/>
</ip-filter>
```

D)
```
<ip-filter action="forbid">
    <address-range from="192.168.0.0" to="192.168.0.254"/>
</ip-filter>
```

Explanation

The correct configuration is as follows:

```
<ip-filter action="allow">
    <address-range from="192.168.0.0" to="192.168.0.254"/>
</ip-filter>
```

The `<ip-filter action="allow">` statement allows traffic only from specific addresses. The `<address-range from="192.168.0.0" to="192.168.0.254"/>` statement specifies the IP addresses allowed.

The choices with the `<ip-filter action="forbid">` statement are incorrect because this restricts, not allows, certain IP addresses.

The choices with the `<address>192.168.0.0/24</address>` are incorrect. The `<address></address>` statement can include only one IP address, not a network address.

Objective:
Implement Azure security

Sub-Objective:
Implement secure cloud solutions

References:

Microsoft Azure > API Management > API Management access restriction policies

Question #27 of 135

Question ID: 1403593

You are the administrator of the Nutex Corporation. You must define a policy for an API named **YourAPI** on operation scope. In API Management, you navigate to your APIM instance. You must configure the policy.

Which setting do you use?

A) YourAPI – All operations

B) YourAPI – Create resource

C) Products

D) All APIs

Explanation

You would use **YourAPI – Create resource** because there you can choose the Code editor to configure a policy on the scope of an Operation. Policies can be configured globally or at the scope of a Product, API, or Operation, and are evaluated in the following order:

1. Global scope
2. Product scope
3. API scope
4. Operation scope

You would not use **All APIs** because it creates a policy on a global scope, not on the scope of an Operation.

You would not use **Products** because it creates a policy on the scope of a Product, not on the scope of an Operation.

You would not use **YourAPI – All operations** because it creates a policy on the scope of an API, not on the scope of an Operation.

Objective:
Connect to and consume Azure services and third-party services

Sub-Objective:
Implement API management

References:

Microsoft Azure > API Management > How to set or edit Azure API Management policies:

Question #28 of 135

Question ID: 1287207

The Nutex application services team needs to track metrics for the various VMs that support their applications. Lindsay is responsible for ensuring that this is possible.

What metrics should Lindsay expect to see in Azure Monitor for these existing VMs? (Choose all that apply.)

A) Disk operations per second

B) CPU usage

C) Network usage

D) Boot diagnostics

E) Application logs

Explanation

The following metrics can be seen in Azure Monitor:

- CPU usage – This level of information is available in the Azure Monitor right from spinning up a new VM, with no further configuring.
- Network usage – Bytes in and out are available in the Azure Monitor screens by default.
- Disk operations per second – She should also expect to see disk bytes with no further configuration.

Lindsay would NOT expect to see:

- Boot diagnostics – Lindsay would be required to enable the Boot Diagnostics by clicking **Enabled for Boot Diagnostics** under the **Monitoring** section of the Settings screen when creating the VM in the Azure Portal.
- Application logs – She would have to enable the Azure Diagnostics Extension on the VMs in question in order to collect these bits of data.

Objective:
Monitor, troubleshoot, and optimize Azure solutions

Sub-Objective:
Instrument solutions to support monitoring and logging

References:

Microsoft Azure > Virtual Machines > How to monitor virtual machines in Azure

Microsoft Azure > Virtual Machines > Use PowerShell to enable Azure Diagnostics in a virtual machine running Windows

Microsoft Azure > Azure Monitor overview

Question #29 of 135

Question ID: 1403552

You are the administrator of the Nutex Corporation. You want to create an Azure Managed Kubernetes Service (AKS) cluster. You want to do that through an ARM template. You do not want to use existing Azure resources for the AKS cluster.

Which template parameters should you NOT have to define in the template? (Choose all that apply.)

A) `--name`

B) `--kubernetesVersion`

C) `--servicePrincipalClientSecret`

D) `--osDiskSizeGB`

E) `--agentCount`

F) `--servicePrincipalClientId`

G) `--dns-name-prefix`

H) `--sshRSAPublicKey`

I) `--linuxAdminUsername`

J) `--osType`

K) `--location`

L) `--agentVMSize`

M) `--vnet-subnet-id`

N) `--workspace-resource-id`

Explanation

You do not have to define the following in an ARM template:

`--vnet-subnet-id`
`--workspace-resource-id`

The `--vnet-subnet-id` parameter specifies the subnet in a VNet where the new AKS cluster will be deployed. This information is optional.

The `--workspace-resource-id` parameter is only used if you want to store AKS monitoring data in an existing log analytics workspace. This parameter specifies the resource ID of an existing Log Analytics Workspace to use for storing monitoring data.

The `--dns-name-prefix` parameter specifies the prefix for hostnames. If this parameter is not specified, a hostname is generated using the managed cluster and resource group names. This parameter is optional.

All the other parameters are used to create new Azure resources.

The `--name` parameter is the name of the managed cluster.

The `--location` parameter specifies the location.

The `--osDiskSizeGB` parameter specifies the size of the disk to provision each of the agent pool nodes.

The `--agentCount` parameter specifies the number of nodes in the cluster.

The `--agentVMSize` parameter specifies the size of the virtual machine.

The `--linuxAdminUsername` parameter specifies the user name to be used on the Linux virtual machines.

The `--sshRSAPublicKey` parameter specifies the SSH RSA public key string configured on the Linux virtual machines.

The `--servicePrincipalClientId` parameter specifies the Client ID which is used by the cloud provider.

The `--servicePrincipalClientSecret` parameter specifies the Service Principal Client Secret.

The `--osType` parameter specifies the operating system type.

The `--kubernetesVersion` parameter specifies the Kubernetes version.

Objective:
Develop Azure compute solutions

Sub-Objective:
Implement IaaS solutions

References:

Microsoft Azure > Templates > Azure Container Service (AKS)

Microsoft Azure > Azure CLI > Reference > az aks create

Question #30 of 135

Question ID: 1403581

You are the administrator of the Nutex Corporation. You have a backend application API named **APINutex** and a client application named **ClientNutex** that needs to call the API. You want to configure **ClientNutex** so that it can call **APINutex** using OAuth 2.0.

Choose the appropriate tasks and place them in the correct order.

{UCMS id=5041974248734720 type=Activity}

Explanation

You would choose the following:

1. Register APINutex in Azure AD to represent the API.
2. Register ClientNutex in Azure AD to represent a client application that needs to call the API.
3. In Azure AD, grant permissions to allow ClientNutex to call the APINutex.
4. Configure ClientNutex to call APINutex using OAuth 2.0 user authorization.

First, you would register **APINutex** in Azure AD to represent the API. To protect an API with Azure AD, you first need to register the application that represents the API in Azure AD.

You would then register **ClientNutex** in Azure AD to represent a client application that needs to call the API **APINutex.** A client application that calls the API must be registered as an application in Azure AD. In this example, the client application is **ClientNutex** in the API Management developer portal.

The third step is to grant permissions to allow ClientNutex to call the APINutex in Azure AD. After you have registered the two applications, you need to grant permissions to allow **ClientNutex** to call **APINutex**.

You would then configure **ClientNutex** to call **APINutex** using OAuth 2.0 user authorization. Once this has been done, you can specify the client registration page URL, the authorization endpoint URL, and the Token endpoint URL to configure an OAuth 2.0 authorization server, so that the **ClientNutex** application can obtain access tokens from Azure AD.

Objective:
Implement Azure security

Sub-Objective:
Implement user authentication and authorization

References:

Azure > API Management > Protect an API by using OAuth 2.0 with Azure Active Directory and API Management

---

Question #31 of 135

Question ID: 1287116

Lana has been asked to deploy a complex solution in Azure involving multiple VMs running various custom service applications. She has been asked to do this at least three times because Test, Development, and Production environments are required. The Test and Development solutions will need to be able to be destroyed and recreated regularly, incorporating new data from production each time. The Nutex system administration team is already using Ansible internally to accomplish deployments.

What will Lana need to do to get things started in Azure?

A) On each Ansible managed node, Lana will need to install Azure Dependencies using pip.

B) Using the Azure Cloud Shell, Lana needs to install the Ansible modules.

C) On the Ansible control machine, Lana will need to install Azure Resource Manager modules using pip.

D) Working in a local Windows Powershell, Lana will need to install the Ansible modules.

Explanation

Lana needs to install Azure Resource Manager modules on the Ansible control machine using pip. The Ansible control machine will need the Azure Resource Manager modules to appropriately communicate with Azure. Using pip allows for an easier managment of Python modules.

She would not use the Azure Cloud Shell to install the Ansible Modules. This is not necessary because the Ansible Modules are already installed in the Azure Cloud Shell.

She would not use a local Windows Powershell to install the Ansible modules. This is not currently possible because the Ansible Control Machine cannot currently run on a Windows PC, and therefore cannot be managed with a Windows Powershell.

She would not install Azure Dependencies on each Ansible managed node using pip. The managed nodes do not need any Azure Dependencies installed, that is one of the biggest selling points! They only require a Python install and SSH access.

Objective:
Develop Azure compute solutions

Sub-Objective:
Implement IaaS solutions

References:

Ansible Docs > Microsoft Azure Guide

Ansible Docs > Installation Guide > Installing Ansible

Question #32 of 135

Question ID: 1403577

You are the administrator of the Nutex Corporation. You have some Azure blob's and you want to perform lease blob operations. You want to end the lease but ensure that another client cannot acquire a new lease until the current lease period has expired.

Which lease blob operation mode should you select?

A) `Renew`

B) `Break`

C) `Change`

D) `Acquire`

E) `Release`

Explanation

You would use `Break` because with this mode you can end the lease but ensure that another client cannot acquire a new lease until the current lease period has expired.

You would not use the `Acquire` mode because this operation mode is to request a new lease.

You would not use the `Renew` mode because this operation mode is to renew an existing lease.

You would not use the `Change` mode because with this operation mode you change the ID of an existing lease.

You would not use the `Release` mode because with this operation mode you free the lease if it is no longer needed so that another client may immediately acquire a lease against the blob.

Objective:
Develop for Azure storage

Sub-Objective:
Develop solutions that use blob storage

References:

Microsoft Azure > Storage Services > Lease Blob

Question #33 of 135

Question ID: 1287137

You are the administrator of the Nutex Corporation. You have created different Azure functions. You must decide which kind of input and output binding you have to choose for which type of function. The trigger causes the function to run. The input and output bindings to the function connect another resource to the function.

Scenario 1:

A new queue message arrives which runs a function to write to another queue.

Apply the relevant input and output bindings.

{UCMS id=5710223747579904 type=Activity}

Explanation

Example scenario	Trigger	Input binding	Output binding
A new queue message arrives which runs a function to write to another queue.	Queue*	*None*	Queue
A scheduled job reads Blob Storage contents and creates a new Cosmos DB document.	Timer	Blob Storage	Cosmos DB
The Event Grid is used to read an image from Blob Storage and a document from Cosmos DB to send an email.	Event Grid	Blob Storage and Cosmos DB	SendGrid
A webhook that uses Microsoft Graph to update an Excel sheet.	HTTP	*None*	Microsoft Graph

In this scenario, a new queue message arrives which runs a function to write to another queue. The new queue message must trigger the function. The function will use Queue as the output binding because messages have to be written to another queue as output. This scenario does not need an input binding.

The function trigger is not HTTP because, in this scenario, no HTTP request has been received. The function trigger is not Event Grid, because this function does not have to respond to an event sent to an event grid topic. The function trigger is not Timer, because this function does not have to run on a schedule.

The function will not use only Blob storage for the input binding because, in this scenario, the function does not have to react to changes in the blob data along with changes in read and write values. The function is not using Cosmos DB, because the function does not have to listen for inserts and/or updates across partitions. Cosmos DB Trigger uses the Azure Cosmos DB Change Feed to listen for tasks like that.

The function will not use Cosmos DB as the output binding because, in this scenario, the function does not have to write a new document to an Azure Cosmos DB database. The function will not use SendGrid as the output binding because the function does not have to send email through SendGrid. The function will not use Microsoft Graph as the output binding because, in this scenario, you do not need an Excel spreadsheet, OneDrive, or Outlook as output.

Objective:
Develop Azure compute solutions

Sub-Objective:
Implement Azure functions

References:

Microsoft Azure > Functions > Azure Functions triggers and binding concepts

Microsoft Azure > Functiions > Azure Event Grid bindings for Azure Functions

Microsoft Azure > Functions > Timer trigger for Azure Functions

Microsoft Azure > Functions > Azure Blob storage bindings for Azure Functions overview

Microsoft Azure > Functions > Azure Cosmos DB bindings for Azure Functions 1.x

---

Question #34 of 135

Question ID: 1287139

You are the administrator of the Nutex Corporation. You have created different Azure functions. You must decide which kind of input and output binding you have to choose for which type of function. The trigger causes the function to run. The input and output bindings to the function connect another resource to the function.

Scenario 3:

The Event Grid is used to read an image from Blob Storage and a document from Cosmos DB to send an email.

Apply the relevant input and output bindings.

{UCMS id=4885559794204672 type=Activity}

Explanation

Example scenario	Trigger	Input binding	Output binding
A new queue message arrives which runs a function to write to another queue.	Queue*	*None*	Queue*
A scheduled job reads Blob Storage contents and creates a new Cosmos DB document.	Timer	Blob Storage	Cosmos DB
The Event Grid is used to read an image from Blob Storage and a document from Cosmos DB to send an email.	Event Grid	Blob Storage and Cosmos DB	SendGrid
A webhook that uses Microsoft Graph to update an Excel sheet.	HTTP	*None*	Microsoft Graph

The trigger will be Event Grid because the Event Grid trigger can be used to read an image. The function will use Blob Storage and Cosmos DB as the input binding because it must read an image from blob storage and a document from Cosmos DB. The output binding of this function is SendGrid because the function must send an email.

The function trigger is not HTTP because, in this scenario, no HTTP request has been received. The function trigger is not Timer because this function does not have to run on a schedule. The function trigger is not Queue, because this function is not based on another queue.

The function will not use only Blob Storage as the input binding because this function must also use Cosmos DB. This function will not use None as the input binding because the Event Grid must read an image from Blob Storage and a document from Cosmos DB.

The output binding of this function is not Queue because this function does not have to write content into another queue. The output binding of this function is not Cosmos DB because this function does not have to create documents in a Cosmos DB. The output binding of this function is not Microsoft Graph because this function not has to output something to Excel, OneDrive, or Outlook.

Objective:
Develop Azure compute solutions

Sub-Objective:
Implement Azure functions

References:

Microsoft Azure > Functions > Azure Functions triggers and binding concepts

Microsoft Azure > Functiions > Azure Event Grid bindings for Azure Functions

Microsoft Azure > Functions > Timer trigger for Azure Functions

Microsoft Azure > Functions > Azure Blob storage bindings for Azure Functions overview

Microsoft Azure > Functions > Azure Cosmos DB bindings for Azure Functions 1.x

---

Question #35 of 135

Question ID: 1403569

You work as an Azure developer for your company and are involved in a code review for a corporate system implemented around the globe. The code look likes the following:

```
private static async Task ReadDocumentAsync()
        {
            Console.WriteLine("\n1.2 - Reading Document by Id");
            // Note that Reads require a partition key to be spcified.
            var response = await client.ReadDocumentAsync(
                UriFactory.CreateDocumentUri(databaseName, collectionName, "SalesOrder1"),
                new RequestOptions { PartitionKey = new PartitionKey("Account1") });
            // You can measure the throughput consumed by any operation by inspecting the RequestCharge property
            Console.WriteLine("Document read by Id {0}", response.Resource);
            Console.WriteLine("Request Units Charge for reading a Document by Id {0}", response.RequestCharge);
            SalesOrder readOrder = (SalesOrder)(dynamic)response.Resource;
            //************************************************************************************************************
            // 1.3 - Read ALL documents in a Collection
            //************************************************************************************************************
            Console.WriteLine("\n1.3 - Reading all documents in a collection");
            string continuationToken = null;
            do
            {
            //code
            }
```

Another developer proposes to remove the part of the code that reads the partition key.

When will it be possible to remove the code and have the application work?

A) It is possible. The code that reads the partition key can be skipped – collection DB just does a full scan, but it is not recommended because it will be slower.

B) It is possible. The code that reads the partition key can be skipped – collection DB just does a full scan.

C) It is not possible. The code that reads the partition key is mandatory.

D) It is possible. The code that reads the partition key can be skipped if your collection is not partitioned.

E) It is possible. The code that reads the partition key can be skipped – collection DB just gets a default Partition Key.

Explanation

The code that reads the partition key can be skipped if your collection is not partitioned. Reads require a partition key to be specified. However, this can be skipped if your collection is not partitioned. i.e. does not have a partition key defined during creation.

The option that states the partition key is mandatory is the wrong choice when the collection is not partitioned.

The statement that says, “The code that reads the partition key can be skipped – collection just gets default Partition Key” is not true because the collection will not get a default Partition Key.

The following statements are incorrect because the collection DB does not perform a full scan:

- The code that reads the partition key can be skipped – collection DB just does a full scan.
- The code that reads the partition key can be skipped – collection DB just does a full scan, but it is not recommended because it will be slower.

Objective:
Develop for Azure storage

Sub-Objective:
Develop solutions that use Cosmos DB storage

References:

GitHub > Azure > azure-cosmos-dotnet-v2

Question #36 of 135

Question ID: 1287246

You are the administrator of Nutex. You host a distributed on-premises web application named NutexApp. The application has to be securely integrated with Azure Table Storage. You must provide an intermediary configuration to support the existing on-premises application and Azure. NutexApp cannot be rewritten and cannot be exposed externally, but has to communicate with other web roles in Azure.

You need to recommend a method of allowing permanently IPSec-secured connections between your on-premises application servers and Azure Table Storage. The application has to be made accessible for other Azure applications. Costs have to be minimized.

What should you recommend? (Choose two.)

A) Azure CDN

B) Azure Point-to-Site VPN

C) Azure Site-to-Site VPN

D) Azure ExpressRoute

E) Azure Service Bus

F) Azure Access Control

Explanation

You would use Azure Site-to-Site VPN to permanently secure a connection between your on-premises application servers and Azure, so that the on-premises application servers hosting NutexApp can access Azure Table Storage through the S2S connection. This is a secure connection solution to Azure that uses IPSec encryption.

You would use Azure Service Bus because of the Azure Service Bus Relay feature, which makes it possible to interact between on-premises services or applications and Azure web applications.

You would not use Azure Access Control because Azure AD Access Control (ACS) is a solution to authenticate users from IdPs (Microsoft, Google, Yahoo, or Facebook) when those authenticated users try to access a web application. This is an identity solution and this scenario does not need an identity solution design.

You would not use Azure CDN in this scenario. Azure CDN improves the performance for websites, media, or mobile service for static audio/video content by moving the relevant content closer to end users. Azure CDN will not permanently secure a connection between your on-premises application servers and Azure.

You would not use Azure ExpressRoute because with Microsoft Azure ExpressRoute you can extend your on-premises network into Azure over a dedicated private connection through a connectivity provider in a secure manner. An S2S connection is less expensive than ExpressRoute. In this scenario, you have to consider the cost factor. Azure ExpressRoute is not a possible solution.

You would not use Azure Point-to-Site (P2S) VPN because with that you have no permanent connection to Azure between your on-premises site and Azure. P2S VPN is not using IPSec, instead it works with SSTP.

Objective:
Connect to and consume Azure services and third-party services

Sub-Objective:
Develop message-based solutions

References:

Microsoft Azure > Messaging services > Service Bus Relay > Expose an on-premises WCF service to a web application in the cloud by using Azure Relay

Microsoft Azure > Networking > CDN documentation

Microsoft Azure > Networking > ExpressRoute documentation

Microsoft Azure > Networking > VPN Gateway > Configure a Point-to-Site connection by using certificate authentication (classic)

Question #37 of 135

Question ID: 1292144

You are working as a developer for the Nutex Corporation. You are responsible for an online e-store system using PHP 7.4. For the time period after Black Friday and Cyber Monday, the CEO plans to implement sending push messages to mobile users who use the Nutex Corporation mobile app. In this way, the CEO plans to increase sales during the off-season period.

Which Azure service should you plan to use?

A) Azure Cognitive Service
B) Azure Notification Hubs
C) Azure SignalR
D) Azure Service Bus
E) Azure Event Hubs

Explanation

You would use Azure Notification Hubs. Azure Notification Hubs can be used for sending push notifications to Android, iOS, Windows, and more.

You would not use Azure Cognitive Service. This is used for AI recognition tasks such as picture recognition and voice recognition, but it is not used for sending push notifications.

You would not use Azure Event Hubs. This is a data stream service for receiving and processing millions of events per second and sending messages to multiple sources, but it is not used for sending push notifications.

You would not use Azure Service Bus. Azure Service Bus is a message service queue and is not used for sending push notifications.

You would not use Azure SignalR. This is a realtime messaging subsystem for the web and is not used for sending push notifications.

Objective:

Connect to and consume Azure services and third-party services

Sub-Objective:

Develop event-based solutions

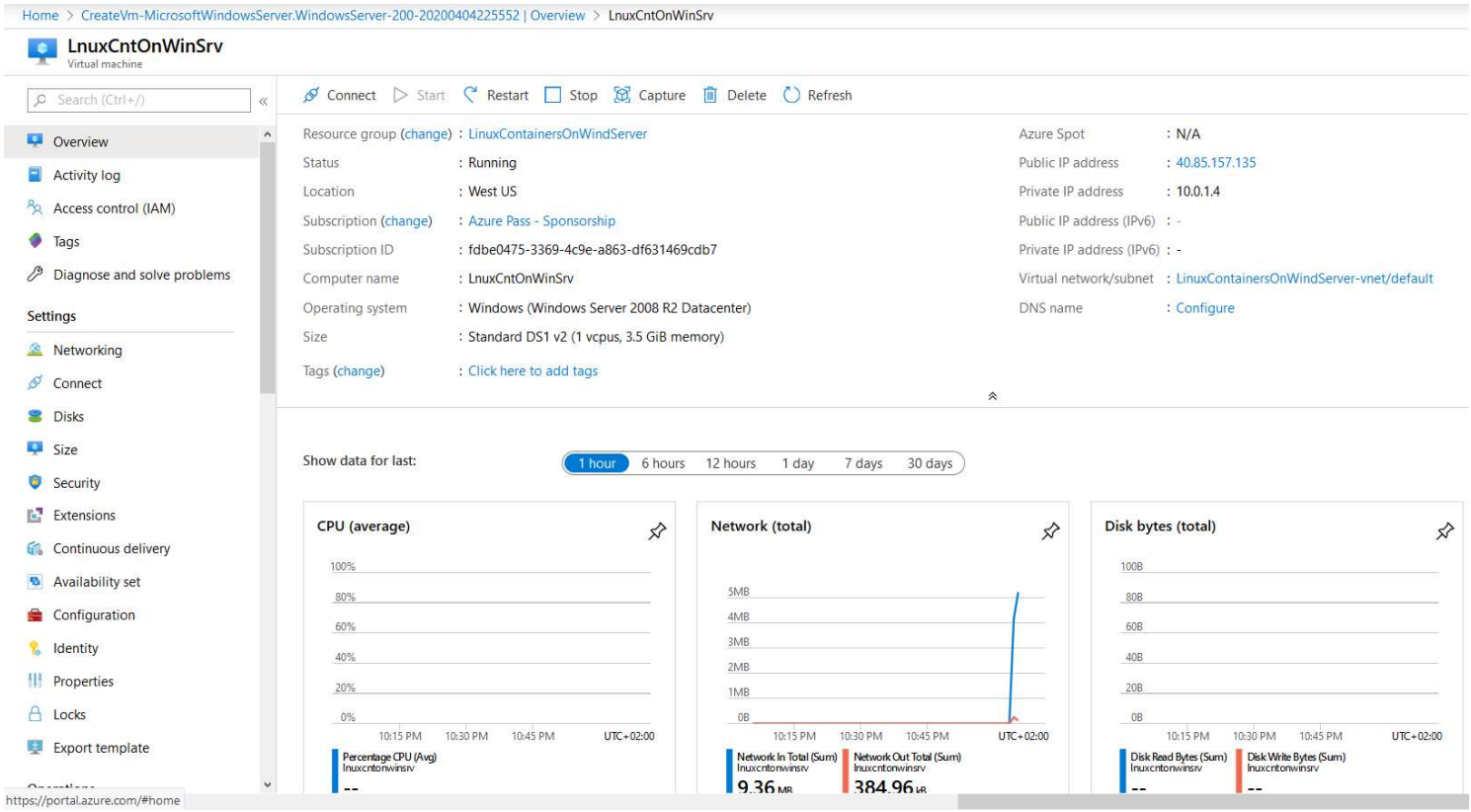
References:

Microsoft Azure > Notification Hubs > What is Azure Notification Hubs?

Question #38 of 135

Question ID: 1287106

You need to test some solutions that use Linux Containers on Windows Server. You deploy a VM named **LnuxCntOnWinSrv**. The following graphic shows the properties of **LnuxCntOnWinSrv**:



You notice that you cannot run Linux Containers in that VM.

Which two actions do you need to take to be able to run Linux Containers on Windows Server?

A) Add tag NestedVirtualisation.

B) Choose the Standard_NV6s_v2 size.

C) Add tag KVM.

D) Deploy Windows Server 2012 R2 Datacenter.

E) Deploy Windows Server 2019 Datacenter.

F) Choose the Standard_D4s_v3 size.

Explanation

You would deploy Windows Server 2019 Datacenter and choose VMs with the Standard_D4s_v3 size.

Linux Containers on Windows needs to have Hyper-V installed. Hyper-V can be run on a virtual machine (VM) only with nested virtualization. Nested virtualization allows you to run a hypervisor inside of a VM, which itself runs on a hypervisor. Nested virtualization is available on Windows Server 2016 and above.

You cannot deploy Windows Server 2012 R2 Datacenter because nested virtualization is only available on Windows Server 2016 and above.

You would not choose the Standard_NV6s_v2 size. Dv3 or Ev3 VM size is needed for nested virtualization.

You would not choose to add a tag NestedVirtualization or add a tag KVM. Adding a tag is just for information. It is not used for any physical behavior of Azure resources.

Objective:
Develop Azure compute solutions

Sub-Objective:
Implement IaaS solutions

References:

Microsoft Azure > Virtual Machines > Windows > How to enable nested virtualization in an Azure VM

Microsoft Docs > Virtualization > Containers on Windows > Linux containers on Windows 10

Question #39 of 135

Question ID: 1287208

Leslie has been asked to enable Application Insights on the Nutex Sales Web Application that is already deployed and running on an Azure VM.

When deployed, the Nutex Sales App management team wants to know what metrics and benefits they should expect to see from runtime Application Insights activation.

What should Leslie tell them? (Choose all that apply.)

A) Trace log integration
B) Detailed SQL command text
C) Code rebuild and redeploy required
D) System performance counters
E) Page view and user data
F) More detailed exceptions

Explanation

The benefits for Application Insights activation are as follows:

- More detailed exceptions
- System performance counters
- Detailed SQL command text.

By enabling Application Insights at runtime, Leslie will be able to get more detailed exceptions than when enabled during build-time.

Application Insights enabled at runtime can report on System Performance Counters.

Dependency diagnostics collection for runtime Application Insights can collect SQL commands being executed from the app in question.

Page view and user data is not a benefit of runtime Application Insights activation. When implemented at runtime, Application Insights cannot capture Page view and user data.

Trace log integration is not a benefit of runtime Application Insights activation. Application Insights implemented during the app build process can integrate with trace logging, but runtime activation cannot.

Code rebuild and redeploy required is not a benefit of runtime Application Insights activation. When Application Insights is activated at runtime, there is no required code rebuild or redeploy for the app in question.

Objective:
Monitor, troubleshoot, and optimize Azure solutions

Sub-Objective:
Instrument solutions to support monitoring and logging

References:

Microsoft Azure > Azure Monitor > Instrument web apps at runtime with Application Insights Codeless Attach

Microsoft Azure > Azure Monitor > What is Application Insights?

Question #40 of 135

Question ID: 1403586

You want to use the Azure Key Vault feature of Azure encrypt keys and secrets (such as authentication keys, storage account keys, data encryption keys, .PFX files, and passwords) by using keys that are protected by hardware security modules (HSMs). You sign in with your Azure account and create a new resource group as follows:

```
New-AzResourceGroup –Name 'NutexResourceGroup' –Location 'East Asia'
```

You attempt to create a key vault by running the following from the PowerShell prompt:

```
New-AzKeyVault -VaultName 'NutexKeyVault' -ResourceGroupName 'NutexResourceGroup' -Location 'East Asia'
```

However, you see the '`The subscription is not registered to use namespace 'Microsoft.KeyVault'` error after you run the above command.

What should you do to fix the error?

A) run `Register-AzProviderFeature -ProviderNamespace "Microsoft.KeyVault"` and then rerun the **New-AzKeyVault** command.

B) run `Register-AzResourceProvider -ProviderNamespace "Microsoft.KeyVault"` and then run the **Add-AzureKeyVaultKey** command to add a secret to the vault.

C) run `Register-AzResourceProvider -ProviderNamespace "Microsoft.KeyVault"` and then rerun the **New-AzKeyVault** command.

D) run `Register-AzProviderFeature -ProviderNamespace "Microsoft.KeyVault"` and then run the **Add-AzureKeyVaultKey** command to add a secret to the vault.

Explanation

You would run `Register-AzResourceProvider -ProviderNamespace "Microsoft.KeyVault"` and then rerun the **New-AzKeyVault** command. The **Register-AzResourceProvider** cmdlet registers a resource provider. This action is required if you receive the `The subscription is not registered to use namespace 'Microsoft.KeyVault'` error after you attempt to create a key vault.

You would not run `Register-AzResourceProvider -ProviderNamespace "Microsoft.KeyVault"` and then run the **Add-AzureKeyVaultKey** command to add a secret to the vault. You will need to add a key or secret to the key vault with the **Add-AzureKeyVaultKey** command after the key vault is created. However, the error that you received said that the Azure Key vault was not created yet.

You would not run `Register-AzProviderFeature -ProviderNamespace "Microsoft.KeyVault"`. The **Register-AzProviderFeature** cmdlet registers an Azure provider feature. In this scenario, you want to register a resource provider, not a feature of a provider.

Objective:
Implement Azure security

Sub-Objective:

Implement secure cloud solutions

References:

Microsoft Azure > Key Vault > About Azure Key Vault

Microsoft Docs > .NET > ASP.NET Core > Azure Key Vault Configuration Provider in ASP.NET Core

---

Question #41 of 135

Question ID: 1403602

You want to access data sources on-premises from your logic apps. You take the following actions:

- You download and install the data gateway on a Windows Server 2012 R2 server.
- You create an Azure resource for the gateway.
- You attempt to create a connection between your logic app and your on-premises data source by using the gateway.

You run the following **Test-NetConnection** command and see the following output:

```
Test-NetConnection -ComputerName watchdog.servicebus.windows.net -Port 9350

ComputerName            : watchdog.servicebus.windows.net
RemoteAddress           : 70.37.104.240
RemotePort              : 5672
InterfaceAlias          : vEthernet (Broadcom NetXtreme Gigabit Ethernet - Virtual Switch)
SourceAddress           : 10.10.10.98
PingSucceeded           : False
PingReplyDetails (RTT) : 0 ms
TcpTestSucceeded        : False
```

You determine that your gateway is blocked by a firewall. Which ports must be configured on the firewall for the data gateway to create an outbound connection to the Azure Service Bus? (Choose all that apply.)

A) 443

B) 7890-7899

C) 13000-13050

D) 389

E) 4201-4299

F) 80

G) 5671-5672

H) 9350-9354

Explanation

You would choose the following:

- 443 for HTTPS
- 5671-5672 for Advanced Message Queuing Protocol (AMQP)
- 9350-9354 for Listeners on Service Bus Relay over TCP.

The following graphic lists the ports that need to open on a firewall in order to create an outbound connection to the Azure Service Bus:

Domain names	Outbound ports	Description
*.analysis.windows.net	443	HTTPS
*.core.windows.net	443	HTTPS
*.frontend.clouddatahub.net	443	HTTPS
*.login.windows.net	443	HTTPS
*.microsoftonline-p.com	443	Used for authentication depending on configuration.
*.msftncsi.com	443	Used to test internet connectivity when the gateway is unreachable by the Power BI service.
*.servicebus.windows.net	443, 9350-9354	Listeners on Service Bus Relay over TCP (requires 443 for Access Control token acquisition)
*.servicebus.windows.net	5671-5672	Advanced Message Queuing Protocol (AMQP)
login.microsoftonline.com	443	HTTPS

You would not open ports 7890-7899. This range is used for the iControl Internet Cafe Suite Administration software, which is not needed here.

You would not open port 80. This is used for HTTP, and HTTPS or port 443 is required in this scenario.

You would not open port 389. This port is used for Lightweight Directory Access Protocol (LDAP), which is not needed.

You would not open ports 13000-13050 or ports 4201-4299. These ranges are used by online games and are not needed.

Objective:
Connect to and consume Azure services and third-party services

Sub-Objective:
Develop message-based solutions

References:

Microsoft Azure > Logic Apps > Install the on-premises data gateway for Azure Logic Apps

Microsoft Azure > Logic Apps > Connect to on-premises data sources from Azure Logic Apps > Connect to on-premises data

---

Question #42 of 135

Question ID: 1403600

You are the administrator of the Nutex Corporation. You have developed an event-based solution using Azure queue storage. You want to change the contents of a message in-place in your Azure storage queue. You want to update the status of a work task in the queue. You want to update the queue message with new content, and you want to set the visibility timeout to extend another 60 seconds.

Fill in the missing parts with the correct commands:

```
// Retrieve storage account from connection string.
CloudStorageAccount storageAccount = CloudStorageAccount.Parse(
    CloudConfigurationManager.GetSetting("StorageConnectionString"));

CloudQueueClient queueClient = storageAccount.CreateCloudQueueClient();
CloudQueue queue = queueClient.GetQueueReference("myqueue");
CloudQueueMessage message = queue.GetMessage();

message.[A]("Updated contents.", false);

queue.[B](message,
    TimeSpan.FromSeconds(60.0),
    [C].Content | [D].Visibility);
```

{UCMS id=5631062383263744 type=Activity}

Explanation

You would choose the following:

```
// Create the queue client.
CloudQueueClient queueClient = storageAccount.CreateCloudQueueClient();

// Retrieve a reference to a queue.
CloudQueue queue = queueClient.GetQueueReference("myqueue");

// Get the message from the queue and update the message contents.
CloudQueueMessage message = queue.GetMessage();
message.SetMessageContent2("Updated contents.", false);
queue.UpdateMessage(message,
    TimeSpan.FromSeconds(60.0),  // Make it invisible for another 60 seconds.
    MessageUpdateFields.Content | MessageUpdateFields.Visibility);
```

It is possible to change the contents of a message in place when it is in the queue. For example, you can change the status of a work task if the message respresents a work task.

The following code retrieves the message from the queue and updates the message with new content:

```
CloudQueueMessage message = queue.GetMessage();
message.SetMessageContent2("Updated contents.", false);
queue.UpdateMessage(message,
```

The following code sets the visibility timeout to extend another 60 seconds:

```
    TimeSpan.FromSeconds(60.0),
    MessageUpdateFields.Content | MessageUpdateFields.Visibility);
```

Once this action occurs, the message's state of work is saved, and the client has 60 more seconds to continue working on the message. This action is useful for tracking multi-step workflows on queue messages. You do not have to begin tracking again if a step fails because of hardware or software issues. You would need to keep a retry count variable to set the number of times a message is retried before the message is deleted. A retry count variable would protect against a message that causes an application error each time it is processed.

Objective:
Connect to and consume Azure services and third-party services

Sub-Objective:
Develop message-based solutions

References:

Microsoft Docs > Azure > Storage > Get started with Azure Queue storage using .NET

Question #43 of 135

Question ID: 1403591

You are the administrator of the Nutex Corporation. You want to use Azure Application Insights alerts to send an email when the server's response to HTTP requests average over 5 minutes and is slower than 1 second. Your application is named **NutexApp** and it is in the resource group **NutexRG**. You are the owner of the Azure subscription. You need to apply the correct values to the following PowerShell command:

```
Add-AzMetricAlertRule -Name "slow responses"
-Description A
-ResourceGroup B
-ResourceId "/subscriptions/00000000-0000-0000-0000-
000000000000/resourcegroups/NutexRG/providers/microsoft.insights/components/IceCreamWebApp"
-MetricName C
```

```
-Operator D
-Threshold 1
-WindowSize E
-SendEmailToServiceOwners
-Location "East US"
-RuleType F
```

Match the missing values or parameters in the PowerShell command to the corresponding letters.

{UCMS id=5704335380971520 type=Activity}

Explanation

You would choose the following:

```
Add-AzMetricAlertRule -Name "slow responses"
-Description "email me if the server responds slowly"
-ResourceGroup "NutexRG"
-ResourceId "/subscriptions/00000000-0000-0000-0000-
000000000000/resourcegroups/NutexRG/providers/microsoft.insights/components/IceCreamWebApp"
-MetricName "request.duration"
-Operator GreaterThan
-Threshold 1
-WindowSize 00:05:00
-SendEmailToServiceOwners ‘
-Location "East US"
-RuleType Metric
```

The **Add-AzMetricAlertRule** cmdlet adds or updates a metric-based alert rule associated with a resource group. The **description** parameter’s value is just a text name describing the rule. The **ResourceGroup** parameter specifies the value for the NutexRG resource group. The **MetricName** parameter states the metric that is being used, in this case “`request.duration`”. The **WindowSize** parameter sets the time windows for the rule. In this scenario that is 00:05:00 or 5 minutes. The **RuleType** parameter specifies the type of rule. In this scenario, it is a metric type rule.

Objective:
Monitor, troubleshoot, and optimize Azure solutions

Sub-Objective:
Instrument solutions to support monitoring and logging

References:

Microsoft Azure > Azure Monitor > Set Alerts in Application Insights

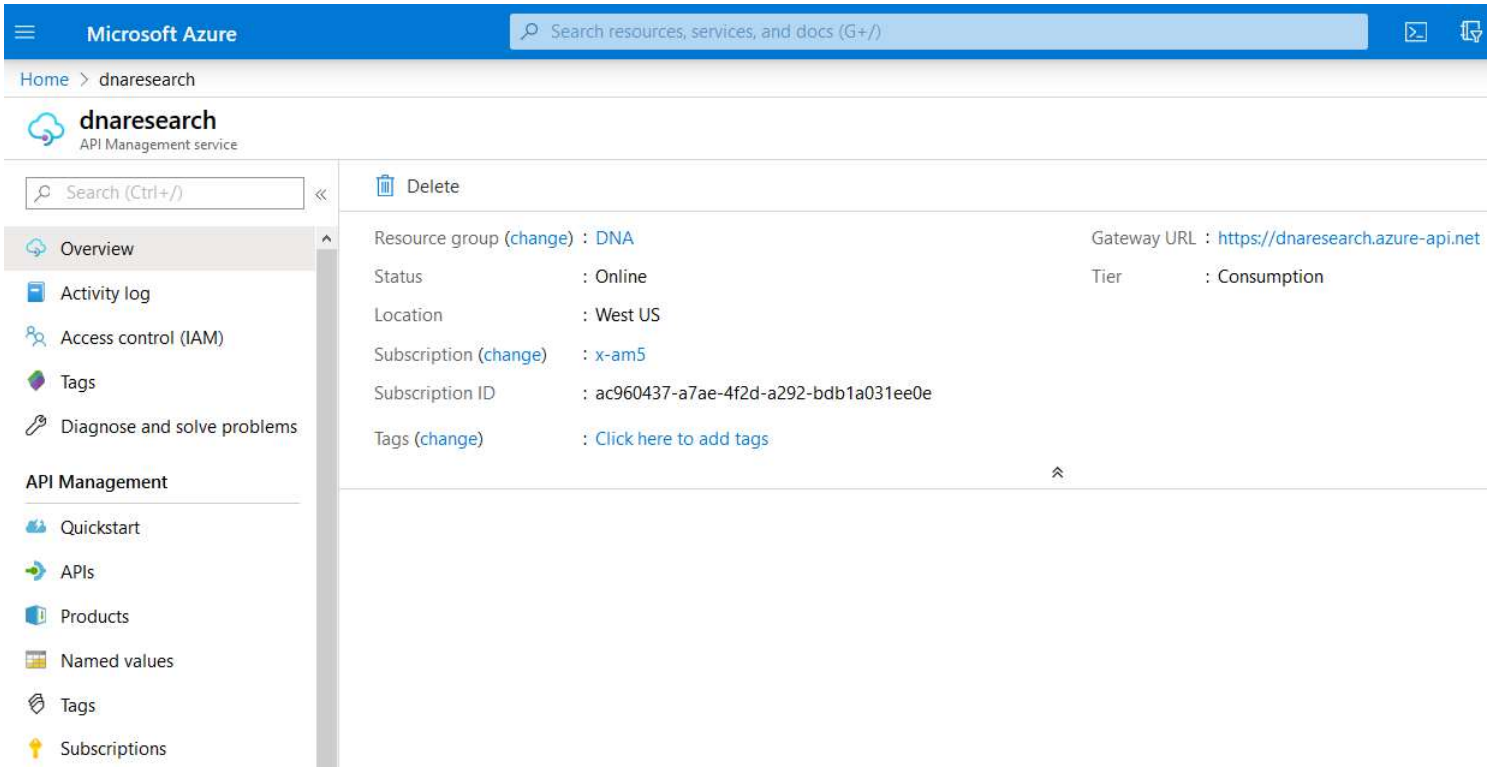
Microsoft Azure > Azure Monitor > Use PowerShell to set alerts in Application Insights

Microsoft Azure > PowerShell > Add-AzMetricAlertRule

Question #44 of 135

Question ID: 1287227

You work as an Azure developer for your company and are involved in API development. Another administrator implemented the API Management service in Azure as follows:



You need to access Azure Key Vault from the **dnaresearch** API Management service.

What should you do first to implement integration with Azure Key Vault?

A) Configure managed identities.

B) Upgrade API Management to the Premium tier.

C) Upgrade API Management to the Standard tier.

D) Create an API definition from the OpenAPI specification.

Explanation

You would configure managed identities. A system-assigned managed identity prevents you from storing credentials in code. It allows Azure resources to authenticate to cloud services such as the Azure Key Vault without stored credentials. Once a system-assigned managed identity is enabled, you can use Azure role-based-access-control (RBAC) to grant all necessary permissions.

You would not upgrade API Management to either the Premium or Standard tiers because managed identities are supported in all tiers of API Management. You would not have to change the tier from the Consumption tier.

You would not create an API definition from the OpenAPI specification as a first option. This action can be an additional step in order to import an API definition. You could also use other methods to create APIs.

Objective:
Connect to and consume Azure services and third-party services

Sub-Objective:
Implement API management

References:

Microsoft Azure > API Management > Use managed identities in Azure API Management

---

Question #45 of 135

Question ID: 1287190

You are the administrator of the Nutex Corporation. You want to implement sign-in to Microsoft through an ASP.NET MVC solution by using a traditional web browser-based application and OpenID Connect. The application needs to be able to accept sign-ins of personal accounts from outlook.com and live.com. Additionally, work and school accounts from any company or organization that are integrated with Azure AD need to be able to sign in to your app. You need to use the browser to access the ASP.NET website that prompts the user to authenticate through a sign-in button.

Place the steps in the correct order.

{UCMS id=5363418727972864 type=Activity}

Explanation

You would place the choices in the following order:

1. Add authentication components.
2. Configure the authentication pipeline.
3. Add a controller to handle sign-in and sign-out requests.
4. Create the app's home page for user sign-in.
5. Add a controller to display user's claims.
6. Create a view to display the user's claims.
7. Register your application.

You would first add authentication components. You will have to add the OWIN middleware NuGet packages through the Package Manager Console. You can do this by typing the following PowerShell cmdlets in the console window:

```
Install-Package Microsoft.Owin.Security.OpenIdConnect
Install-Package Microsoft.Owin.Security.Cookies
Install-Package Microsoft.Owin.Host.SystemWeb
```

Then you would configure the authentication pipeline because you have to create an OWIN middleware Startup class to configure OpenID Connect authentication. When your IIS process starts, this class is executed automatically.

Next you would add a controller to handle sign-in and sign-out requests because you have to create a new controller to expose sign-in and sign-out methods.

Then you would create the app's home page for user sign-in because you have to create a new view to add the sign-in button and display user information after authentication. This new view can be created in Visual Studio.

Next you would add a controller to display user's claims because you have to use the `Authorize` attribute to protect the controller. This attribute allows only authenticated users to access the controller.

Then you would create a view to display the user's claims because a new view is needed to display the user's claims in a web page.

Lastly you would register your application because you have to register the application and add your application registration information to your solution. For that you have two options: Express mode and Advanced mode.

Objective:
Implement Azure security

Sub-Objective:
Implement secure cloud solutions

References:

:

Microsoft Docs > Azure > Active Directory > Develop > Add sign-in to Microsoft to an ASP.NET web app

---

Question #46 of 135

Question ID: 1287154

You are the administrator of the Nutex Corporation. You have to query data stored in your Cosmos database using MongoDB shell. You have the following sample code:

```
{
  "id": "BartkowskiFamily",
  "parents": [
      { "familyName": "Bartkowski", "givenName": "Laura" },
      { "familyName": "Miller", "givenName": "Ben" }
  ],
  "children": [
      {
        "familyName": "Merriam",
        "givenName": "Jesse", t
        "gender": "female", "grade": 1,
        "pets": [
            { "givenName": "Goofy" },
            { "givenName": "Shadow" }
        ]
      },
      {
        "familyName": "Miller",
        "givenName": "Lisa",
        "gender": "female",
        "grade": 8 }
  ],
  "address": { "state": "GA", "county": "Fulton", "city": "Atlanta" },
  "creationDate": 1431620462,
  "isRegistered": false
}
```

Apply the relevant query results to the appropriate queries.

{UCMS id=6050255603761152 type=Activity}

Explanation

You would use `db.families.find({ id: "BartkowskiFamily"})` to get the documents where the ID matches BartkowskiFamily. The query uses `find` to match the `id` field.

You would use `db.families.find( { id: "BartkowskiFamily" }, { children: true } )` to get all children in the family.

You would use `db.families.find( { "isRegistered" : true })` to get all the families that are registered.

You would use `db.families.find( { "isRegistered" : false })` to get all the families that are not registered.

Objective:
Develop for Azure storage

Sub-Objective:
Develop solutions that use Cosmos DB storage

References:

GitHub > Azure-Docs > Query data by using Azure Cosmos DB's API for MongoDB

Microsoft Azure > Cosmos DB > Tutorial: Query data from a Cassandra API account in Azure Cosmos DB

Question #47 of 135

Question ID: 1287209

The Nutex Application Services team has several Azure VMs and need a solution to monitor the web workloads on each. You mentioned using Azure Application Insights to track VM Performance Counters over lunch with a team member. The team wants you to lead the VM monitoring project.

How should you proceed? Place the appropriate steps in order, not all steps will be used.

{UCMS id=5033161236938752 type=Activity}

Explanation

You would proceed in the following order:

1. Ensure the Sales App targets the full .Net Framework.
2. Install Application Insights Status Monitor on the VM.
3. Sign in with your Azure Credentials.
4. Restart IIS.
5. Add the requisite counters in **ApplicationInsights.config.**

Performance counters can be collected when adding Application Insights to .Net Framework targeting apps. You need to ensure the Sales App targets the full .Net Framework.

You will have to install Application Insights Status Monitor on the VM. This must be done to ensure the appropriate DLLs and application hooks are added to enable monitoring.

You will have to sign in with your Azure Credentials. During the Status Monitor install, your Azure Credentials will direct the Application Insights output to your Azure Portal.

After the Status Monitor install, you will be asked to restart IIS.

You must add the requisite counters in the **ApplicationInsights.config** file. If the Performance Counters you require are not already being monitored, you must add them to the config file.

You would not verify the Sales App targets, only the .Net Core. Performance counters cannot be collected when adding Application Insights to .Net Core developed apps.

Objective:
Monitor, troubleshoot, and optimize Azure solutions

Sub-Objective:
Instrument solutions to support monitoring and logging

References:

Microsoft Azure > Azure Monitor > Instrument web apps at runtime with Application Insights Codeless Attach -

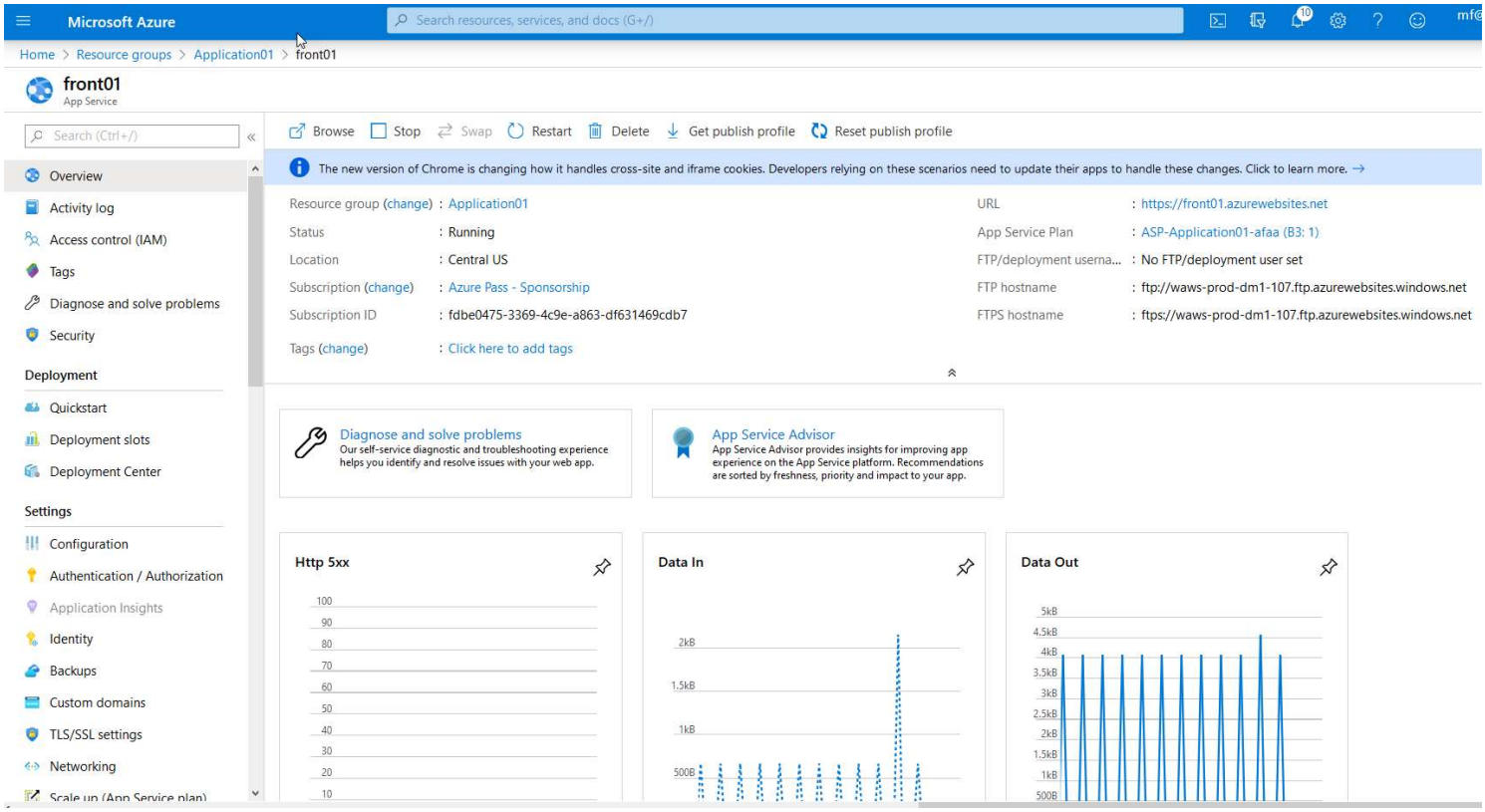
Microsoft Azure > Azure Monitor > System performance counters in Application Insights

---

Question #48 of 135

Question ID: 1403560

You are working as a web app enterprise consultant. Another administrator reports she cannot set up a backup for a Linux application named front01 in a resource group called Application01.



Your goal is to minimize Azure costs.

What should you recommend so that a backup for the **front01** application can be established?

A) Scale up the size to P2v2.

B) Scale up the size to S3.

C) Deploy Windows Server 2012 R2 Datacenter.

D) Deploy Windows Server 2019 Datacenter.

E) Scale up the size to P1v2.

F) Add the tag DailyBackup.

Explanation

You would scale up the size to P1v2. The App Service plan needs to be in the Standard or Premium tier to use the Backup and Restore feature. In this scenario, the P1v2 instance is cheaper than an S3 or P2v2 instance. The price per hour for an S3 instance and P2v2 instance are currently $0.40/hour, while the price per hour of an P1v2 instance is $0.20/hour.

INSTANCE	CORES	RAM	STORAGE	PRICES
S1	1	1.75 GB	50 GB	$0.10/hour
S2	2	3.50 GB	50 GB	$0.20/hour
S3	4	7 GB	50 GB	$0.40/hour
INSTANCE	**CORES**	**RAM**	**STORAGE**	**PRICES**
P1v2	1	3.50 GB	250 GB	$0.20/hour
P2v2	2	7 GB	250 GB	$0.40/hour
P3v2	4	14 GB	250 GB	$0.80/hour

You would not deploy Windows Server 2019 Datacenter or Windows Server 2012 R2 Datacenter because the application is a Linux application, not a Windows application. You would need a Linux operating system to deploy the Linux application.

You would not add the tag DailyBackup. A tag is just for information to organize Azure resources. You can use a tag to identify resources in a subscription or resource group. A tag is not needed for the Backup and Restore feature.

Objective:
Develop Azure compute solutions

Sub-Objective:
Create Azure App Service Web Apps

References:

Microsoft Azure > App Service > Web Apps > Back up your app in Azure

Microsoft Azure > App Service pricing

Question #49 of 135

Question ID: 1287180

You are the administrator of the Nutex Corporation. You use Razor Pages. You need to create an Azure authorization policy with C#. You need to define a collection of data parameters that your policy can use to evaluate the current user principal. The policy must handle three different requirements with permissions such as Read, Edit, and Delete.

Which components are needed in the authorization policy so that you can evaluate on an OR basis? (Choose two.)

A) Multiple authorization handlers
B) Requirements
C) Conditional access policy
D) Single authorization handler

Explanation

You would use multiple authorization handlers because, in this case, you need a one-to-many relationship in which a permission handler can handle three different types of requirements with permissions such as Read, Edit, and Delete..

You would use requirements because an authorization requirement is a collection of data parameters that a policy uses to evaluate the current user principal. If an authorization policy contains several authorization requirements, all of the requirements must pass for the policy evaluation to succeed. In other words, numerous authorization requirements added to a single authorization policy are treated on an AND basis. In cases where you want the evaluation to be on an OR basis, implement multiple handlers for a single requirement.

For example, a company may have doors that can only be opened with key cards. If you forget your key card, the receptionist prints a temporary sticker and opens the door for you. In this scenario, you would have a single requirement, `BuildingEntry`, but multiple handlers, each one examining an individual requirement.

You would not use a single authorization handler because, in this scenario, multiple requirements are needed.

A conditional access policy could allow conditions for legacy authentication or to require multifactor authentication.

Objective:
Implement Azure security

Sub-Objective:
Implement user authentication and authorization

References:

Microsoft Docs > .NET > Security and Identity > Policy-based authorization in ASP.NET Core > Requirements

Microsoft Docs > Azure > Active Directory > What is Conditional Access?

Question #50 of 135

Question ID: 1403592

You are the administrator of the Nutex Corporation. You have created an API. You want to take advantage of the scale-out features of Microsoft Azure App Service, the telemetry features of Application Insights, and the performance-testing features of Azure DevOps. You need to deploy the API to the App Service by using API Apps, and capture telemetry and metrics by using Application Insights. You have to implement a smart client that can handle network issues or other transient faults.

Which is a possible step to do that?

A) Add the Microsoft.Azure.ServiceBus package to your project.

B) Implement the IReconnectRetryPolicy interface.

C) Create a retry policy that will retry a failed HTTP request by using Polly.

D) Implement the IExtentedRetryPolicy interface.

Explanation

It would be best if you created a retry policy that will retry a failed HTTP request by using Polly. By adding retry logic using Polly, you can handle transient faults. For that, you can edit the PollyHandler class to add retry logic.

You would not add the Microsoft.Azure.ServiceBus package to your project because, in this scenario, you do not use Azure Service Bus. You can add a retry mechanism to the service bus with the RetryPolicy class.

You would not implement the IReconnectRetryPolicy interface because, with that interface, you can create a custom retry policy. You can do that for REDIS Cache by setting the options for the client before connection to the cache. In this scenario, there is no REDIS Cache, so you do not need that kind of transient fault handling.

You would not implement the IExtentedRetryPolicy interface because this kind of transient fault handling is for Azure Blob storage.

Objective:
Monitor, troubleshoot, and optimize Azure solutions

Sub-Objective:
Instrument solutions to support monitoring and logging

References:

GitHub > Lab: Monitoring services deployed to Azure:

Microsoft Azure > Architecture > Retry guidance for Azure services: HYPERLINK "https://docs.microsoft.com/en-us/azure/architecture/best-practices/retry-service-specific"

Question #51 of 135

Question ID: 1404420

You are the administrator of the Nutex Corporation. You have developed an application named NutexApp. NutexApp will use several queries to get data from Azure tables storage. You determine that some queries have slow performance. You must categorize all queries from NutexApp to improve the query performance.

Apply the relevant query type to the partitionKeyMatch and RowKeyMatch properties.

{UCMS id=5102508893536256 type=Activity}

Explanation

You should choose the following:

Query type	PartitionKey match	RowKey match	Performance rating
Point	Exact	Exact	Best
Row range scan	Exact	Partial	Better with smaller-sized partitions.
			Bad with partitions that are very large.
Partition range scan	Partial	Partial	Good with a small number of partition servers being touched.
			Worse with more servers being touched.
Full table scan	Partial, none	Partial, none	Worse with a subset of partitions being scanned.
			Worst with all partitions being scanned.

You should use the query type Point, a partition key match of Exact, and a performance rating of Best. Point queries are the best type of queries to use because they fully use the table's clustered index.

You should use the query type Row range scan with a partition key match of Exact and a performance rating of Better with smaller-sized partitions and Bad with partitions that are very large, because if the application has multiple queries, not all of the queries can be point queries. Range queries are similar to point queries in terms of performance. Range queries have two types: the row range scan and the partition range scan. Row range scans generally are more efficient than partition range scans. A row range scan specifies only one partition, occuring on a single partition server. The performance of the row range scan is determined by how selective the query is. The more selective a query is, the more efficient the query is during row range scans.

You should use the query type Partition range scan with a partition key of Partial and a performance rating of Good with a small number of partition servers being touched and Worse with more servers being touched, because a partition range scan for a table that has many large partitions might perform poorly compared to a full table scan for a table that has a few small partitions.

You should use the query type Full table scan with a partition key match of Partial, None, and the performance rating Worse with a subset of partitions being scanned and Worst with all partitions being scanned.

Objective:
Develop for Azure storage

Sub-Objective:
Develop solutions that use Cosmos DB storage

References:

Microsoft Azure > Storage Services > Design a scalable partitioning strategy for Azure Table storage

---

Question #52 of 135

Question ID: 1287140

You are the administrator of the Nutex Corporation. You have created different Azure functions. You have to decide which kind of input and output binding you have to choose for which type of function. The trigger causes the function to run. The input and output bindings to the function connect another resource to the function.

Scenario 4:

A webhook that uses Microsoft Graph to update an Excel sheet.

Apply the relevant input and output bindings.

{UCMS id=5679543554670592 type=Activity}

Explanation

Example scenario	Trigger	Input binding	Output binding
A new queue message arrives which runs a function to write to another queue.	Queue*	*None*	Queue*
A scheduled job reads Blob Storage contents and creates a new Cosmos DB document.	Timer	Blob Storage	Cosmos DB
The Event Grid is used to read an image from Blob Storage and a document from Cosmos DB to send an email.	Event Grid	Blob Storage and Cosmos DB	SendGrid
A webhook that uses Microsoft Graph to update an Excel sheet.	HTTP	*None*	Microsoft Graph

The trigger will be HTTP because a webhook is HTTP-based. There is no HTTP or webhook input trigger available. Therefore the input binding in this scenario is NONE. The output binding is Microsoft Graph because this function must write to an Excel sheet.

The function trigger is not using Timer because this function does not have to run on a schedule. The function trigger is not using Queue because this function is not based on another queue. The function trigger is not using Event Grid because it is not based on events.

The function cannot have an input binding with None because it must be based on Blob Storage content. The function cannot use Cosmos DB as input binding because it must read blob storage content and not content from Cosmos DB.

The output binding of this function is not Queue because this function does not have to write content into another queue. The output binding of this function is not Cosmos DB because this function does not have to create documents in a Cosmos DB. The output binding of this function is not SendGrid because this function does not have to send email.

Objective:
Develop Azure compute solutions

Sub-Objective:
Implement Azure functions

References:

Microsoft Azure > Functions > Azure Functions triggers and binding concepts

Microsoft Azure > Functiions > Azure Event Grid bindings for Azure Functions

Microsoft Azure > Functions > Timer trigger for Azure Functions

Microsoft Azure > Functions > Azure Blob storage bindings for Azure Functions overview

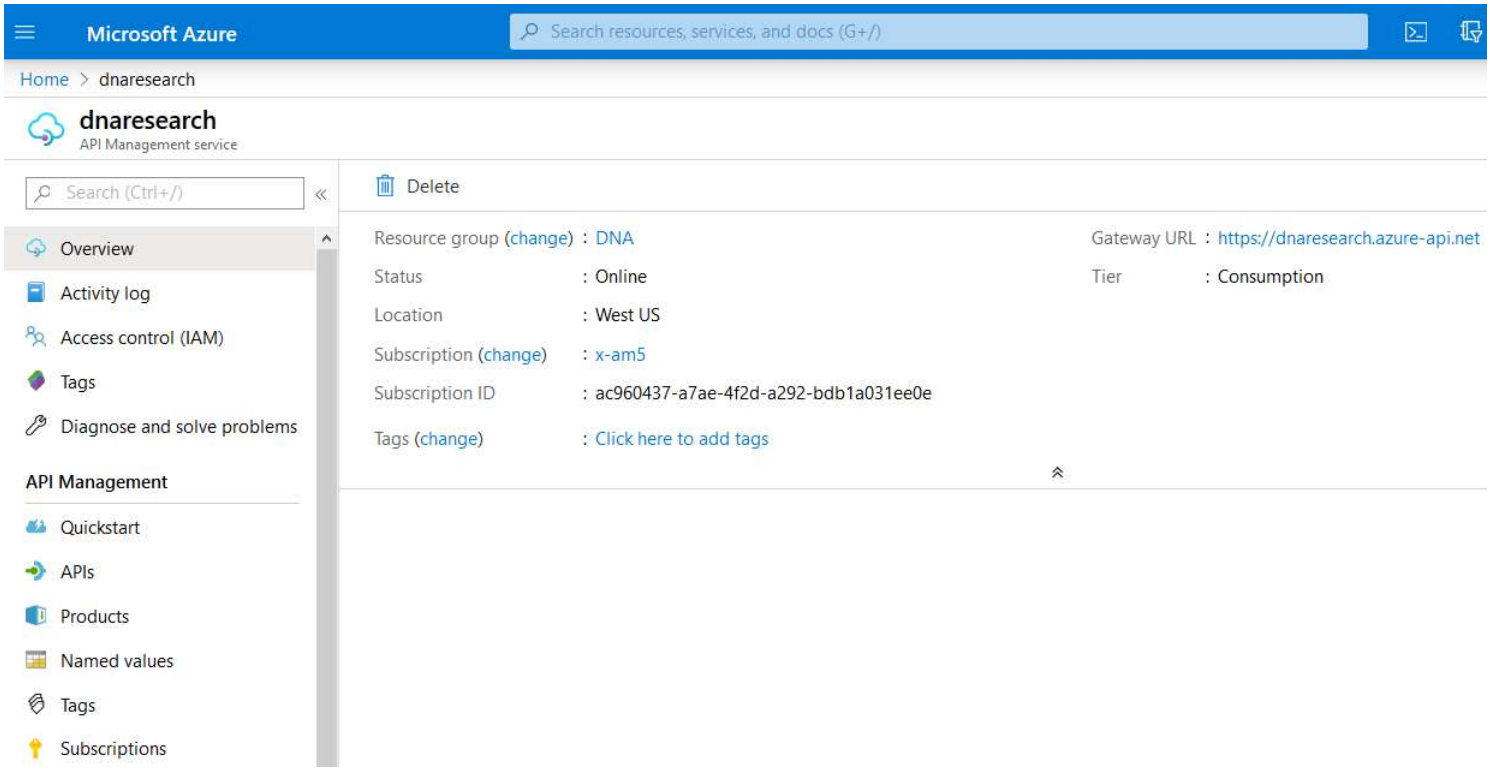
Microsoft Azure > Functions > Azure Cosmos DB bindings for Azure Functions 1.x

---

Question #53 of 135

Question ID: 1287226

You work as an Azure developer for your company and are involved in the development of a system API. Another administrator has implemented the API Management service in Azure as follows:



What should you do first to implement rate-limit-by-key in your API?

A) Create an API definition from the OpenAPI specification.

B) Create API Management.

C) Create an API definition from the WADL.

D) Create a blank API.

Explanation

You would first create API Management because the existing API Management tier is configured for **Consumption.** This tier does not support rate-limit-by-key or quota-by-key. You would have to use another tier such as the Premium tier. The rate-limit-by-key policy thwarts spikes in API usage on a per key basis by limiting the call rate to a configured number during the configured time period. The quota-by-key policy sets bandwidth quota and/or call volume on a per key basis.

You would not first create a blank API. This could be a second option to create an API.

You would not first create an API definition from the OpenAPI specification or create from the WADL specification. These options can be used to import an API definition which would be another task to be done.

Objective:
Connect to and consume Azure services and third-party services

Sub-Objective:
Implement API management

References:

Microsoft Azure > API Management > API Management access restriction policies > Limit call rate by key

---

Question #54 of 135

Question ID: 1287147

You are the administrator of the Nutex Corporation. You have created an Azure function in Visual Studio and have uploaded the function to Azure. You want to use the recommended method to monitor the execution of your function app.

Which Azure resource do you have to create after publishing the function app with Visual Studio?

A) Application Insights

B) Azure Service Bus

C) System Center Operations Manager

D) Azure Monitor

Explanation

You would create the Application Insights resource because the recommended way to monitor the execution of your functions is by integrating your function app with Azure Application Insights. Integrating your function app with Azure Application Insights is done automatically. When you create your function app during Visual Studio publishing, the integration of your function in Azure is not complete. You need to enable the Application Insights integration manually after publishing the function app.

You would not choose Azure Monitor because this is not the recommended way to monitor the execution of function apps.

You would not choose System Center Operations Manager because it is not used primarily for Azure function apps. Instead, it is an overall monitoring solution.

You would not choose Azure Service Bus because this is a messaging service and not usable for application monitoring.

Objective:
Develop Azure compute solutions

Sub-Objective:
Implement Azure functions

References:

Microsoft Azure > Functions > Develop Azure Functions using Visual Studio > Monitoring functions

Microsoft Azure > Functions > Monitor Azure Functions

Question #55 of 135

Question ID: 1403570

You are the administrator of the Nutex Corporation. You use Azure Cosmos DB storage. You have 70,000 documents in one development database with 2.5 GB data and 200 MB indexing data. The newest document is from September 27, 2019, the oldest from June 21, 2018. You want to use a simple SQL API-based solution to remove all data before November 15, 2018.

What is your preferred solution?

A) SQL query

B) Develop a microservice

C) Time to Live (TTL)

D) User-defined function

E) Cosmos DB stored procedure

Explanation

You would use Time to Live (TTL) because you can set a TTL for documents and/or containers. You can enable TTL for documents and wait for the Cosmos DB cleanup to start. After the cleanup finishes, every document in a collection stored in a Cosmos DB contains a `_ts` property representing the Unix time of the last update. The `_ts` property for June 21, 2018 is 1529539200. The `_ts` property for November 15, 2018 is 1542240000. You can choose to delete documents that have a timestamp `1529539200 <= _ts < 1542240000`.

You would not use a user-defined function. While you could use a user-defined function to accomplish this, an SQL API using the TTL feature to query and delete the documents is simpler. A user-defined function would be much more effort.

You would not use an SQL query because you cannot simply use a DELETE based on a Unix TimeStamp. You can use a query language with a SELECT statement, such as `SELECT ... from WHERE ....` However you are not able to run `DELETE * from c WHERE c._ts < unixTimeStamp`.

You would not use a Cosmos DB stored procedure because with that you have restrictions for the result length and the handling of continuation tokens.

You would not develop a microservice. While you could develop a microservice to do this, it is simpler to use an SQL API with the TTL feature to query and delete the documents. Developing a microservice is much more effort.

Objective:
Develop for Azure storage

Sub-Objective:
Develop solutions that use Cosmos DB storage

References:

Tekaris > Azure Cosmos DB bulk delete with TTL

Microsoft Azure > Cosmos DB > Time to Live (TTL) in Azure Cosmos DB

Question #56 of 135

Question ID: 1287198

The Nutex Corporation has developed an online TV station. Your consumers should have the opportunity to view video summarizations from recorded content. You have deployed an eight-node file server on-premises failover cluster named **content.nutex.com**. The cluster is distributed through two sites, West US and East US, in the **nutex.com** domain. Your application servers use a second cluster with four nodes, named **TV.nutex.com**, to host your online video streaming web application.

You want to ensure the following requirements are met:

- Your pre-recorded static videos are moved to Azure.
- Consumers can view summarizations from the recorded content.
- Consumers from all over the world will see improved performance.

Which Azure solution should you recommend?

A) Azure Table Storage with Azure Storage Analytics

B) Azure Blob Storage with Azure Storage Analytics

C) Azure Content Delivery Network (CDN) with Azure Media Analytics services

D) Azure Content Delivery Network (CDN) with Azure Storage Analytics

E) Azure File Storage with Azure Media Analytics services

Explanation

You would use the Azure Content Delivery Network (CDN) with Azure Media Analytics services. Through the Azure Content Delivery Service, you can stream your static media content quickly in different formats for different kinds of devices and with good performance worldwide. Azure Media Analytics has a feature named Video summarization. The Azure Media Video Thumbnails media processor (MP) allows you to create a summarization of your video.

You would not use Azure Table Storage with Azure Storage Analytics because the media content is not the correct kind of content for which Azure Table Storage is used. Instead, use Azure Table Storage for unstructured data not using a schema. Azure Storage Analytics can be used to log and metric data about your storage account.

You would not use Azure File Storage with Azure Media Analytics services because Azure File Storage is using SMB-protocol. The Azure CDN is made for streaming videos. If you want to use Azure Media Video Thumbnails, you have to use CDN for that, not Azure File Storage. Azure Media Analytics services can be used for Azure CDN, not for Azure File Storage.

You would not use Azure Blob Storage with Azure Storage Analytics. With Azure Blob Storage you can store static files that are frequently used by a website, including PDFs, CSS files, and images. However, Azure Blob Storage is not specifically designed for streaming media content, as opposed to CDN. Azure Storage Analytics will not provide customers with video thumbnails.

Objective:
Monitor, troubleshoot, and optimize Azure solutions

Sub-Objective:
Integrate caching and content delivery within solutions

References:

Microsoft Docs > Azure > Storage > Storage Analytics

Microsoft Azure > Media Services > Media Analytics on the Media Services platform

---

Question #57 of 135

Question ID: 1287212

You are working as a senior developer for the Nutex Corporation. Your collegue created a function with the following code, but the function from time to time does not work properly:

```
if ($req_query_computer)
{
    $Computer = $req_query_computer
    $username = $req_query_username
    $password = $req_query_password
    $command  = $req_query_command
}
$secureStringPwd = ConvertTo-SecureString $password -AsPlainText -Force
$creds= New-Object System.Management.Automation.PSCredential ($username, $secureStringPwd)
$sblock  = [Scriptblock]::Create($command)
New-SshSession -ComputerName $Computer -Credential $creds -Reconnect
$result=Get-SshSession|invoke-SSHCommand -ScriptBlock $sblock
$result=$result -replace '@{ComputerName=', '<h3>ComputerName='
$result=$result -replace '; Result=', '; Result={</h3>'
$result=$result -replace '; Error=', '<h3>Error='
$result=$result -replace '\x0a', '<br>'
get-SshSession|Remove-SshSession
$html = @"
<title>ReturnString</title>
<h1>$($command)</h1>
<h2>$(Get-Date)</h2>
"@
$html=$html+"<body>"+$result+"</body>"
@{
    headers = @{ "content-type" = "text/html" }
    body    = $html
} | ConvertTo-Json > $res
```

What is your proposal to fix the code?

A) Implement Cache-Aside pattern.

B) Implement Transient fault handling.

C) Implement Competing Consumers pattern.

D) Implement Sharding pattern.

Explanation

Since the function works sometimes but not all of the time, you would implement Transient fault handling. Transient faults could mean the temporary unavailability of a service because of a sudden loss of network connectivity to components and services, or timeouts that occur when a service is busy. Often these faults are not issues because they are mostly self-correcting, and if the action can be repeated after a short delay, the action more than likely will succeed. In this case, the connection cannot be established. The line `New-SshSession -ComputerName $Computer -Credential $creds -Reconnect` should be retried several times.

You could also use the Retry pattern, which improves the stability of an application by allowing an application to retry a failed operation when intermittent failures of connecting to a network resource or a service occur.

You would not implement the Competing Consumers pattern. This type of pattern is used for queue implementation and can be a part of a solution, but it does not resolve the problem of fixing an intermittent fault.

You would not implement the Cache-Aside pattern. The Cache-Aside pattern is used to improve performance when loading data. This pattern is for storing data in memory to speed up queries. It also keeps consistency between data in the underlying data store and data held in the cache. This pattern does not resolve the problem of fixing an intermittent fault.

You would not implement a Sharding pattern. This pattern is used for splitting data across databases, disks, files, or partitions. This pattern does not resolve the problem of fixing an intermittent fault.

Objective:
Monitor, troubleshoot, and optimize Azure solutions

Sub-Objective:
Instrument solutions to support monitoring and logging

References:

Microsoft Azure > Architecture > Best Practices > Transient fault handling

---

Question #58 of 135

Question ID: 1403578

You are the administrator of the Nutex Corporation. You use an Azure blob storage general purpose v2 account. You want to define a lifecycle management policy. The policy rule has to include the following requirements:

- Tier blob to cool tier 30 days after last modification.
- Tier blob to archive tier 90 days after last modification.
- Delete blob 7 years after last modification.
- Delete blob snapshots 90 days after snapshot creation.

Make the necessary changes in the following JSON template:

```
{
  "rules": [
    {
      "name": "ruleFoo",
      "enabled": true,
      "type": "Lifecycle",
      "definition": {
        "filters": {
          "blobTypes": [ "blockBlob" ],
          "prefixMatch": [ "container1/foo" ]
        },
        "actions": {
          "baseBlob": {
            "
```

```
": { "daysAfterModificationGreaterThan": 30 },
            "B
": { "daysAfterModificationGreaterThan": 90},
            "C
": { "daysAfterModificationGreaterThan": E

}
          },
          "snapshot": {
            "D
": { "daysAfterCreationGreaterThan": 90}
          }
        }
      }
    }
  ]
}
```

Match the appropriate code to the corresponding letter.

{UCMS id=5691057892229120 type=Activity}

Explanation

```
{
  "rules": [
    {
      "name": "ruleFoo",
      "enabled": true,
      "type": "Lifecycle",
      "definition": {
        "filters": {
          "blobTypes": [ "blockBlob" ],
          "prefixMatch": [ "container1/foo" ]
        },
        "actions": {
          "baseBlob": {
            "tierToCool": { "daysAfterModificationGreaterThan": 30 },
            "tierToArchive": { "daysAfterModificationGreaterThan": 90 },
            "delete": { "daysAfterModificationGreaterThan": 2555 }
          },
          "snapshot": {
            "delete": { "daysAfterCreationGreaterThan": 90 }
          }
        }
      }
    }
  ]
}
```

The `tierToCool` action is not used with a snapshot, but is used with a base blob. This action supports blobs currently at hot tier.

The `TierToArchive` action is not used with a snapshot, but is used with a base blob. This action supports blobs currently at either the hot or cool tier.

The `delete` supports both the base blob and the snapshot. If you define more than one action on the same blob, lifecycle management applies the least expensive action to the blob. For example, the `delete` action is cheaper than the `tierToArchive` action. The `tierToArchive` **action** is cheaper than the `tierToCool` action.

You would set the value for a blob deleted 7 years after the last modification to 2555 because this would be the number of days in 7 years. The value should be stated in days and not years.

You would not select `tierToBackup` or `tierToWarm`. These are not valid actions.

Objective:
Develop for Azure storage

Sub-Objective:
Develop solutions that use blob storage

References:

Microsoft Docs > Azure > Storage > Blobs > Manage the Azure Blob storage lifecycle

---

Question #59 of 135

Question ID: 1287225

You work as an Azure architect for your company and are involved in a system architecture review. The system provides information for laboratories all over the world about DNA Gnomon. The information is provided via an API, and the origins are located on virtual machines and web apps. You want to limit the number of queries run by laboratories and also prevent the OWASP TOP 10 security vulnerabilities.

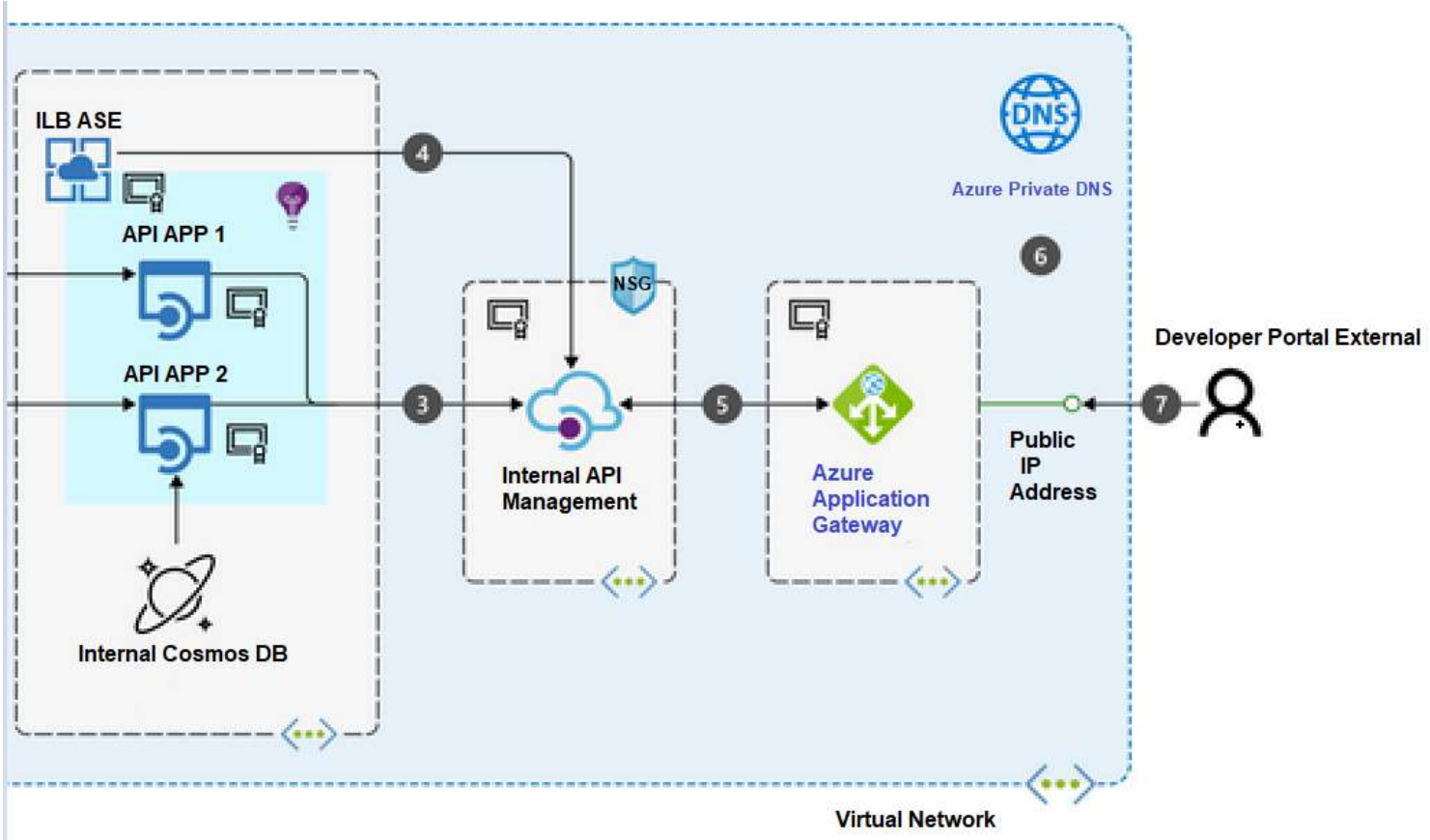
Which of the following solutions should you choose? (Choose all that apply.)

A) Use Azure SAS tokens.
B) Use Azure AD OAuth implicit grant flow to authenticate.
C) Use Azure Application Gateway.
D) Use Azure API Management.
E) Use Azure Traffic Manager.

Explanation

Azure API Management allows you to publish APIs to internal developers, external users, and partners so that they can use services and data. You can publish an API by associating the API with a product. You can have several APIs in a product.

The Azure Application Gateway is a web traffic load balancer that manages web application traffic, and is based on the Core Rule Set (CRS) 3.1 from the Open Web Application Security Project (OWASP). The Application Gateway exposes the API portal and API Management's developer. The reference architecture is as follows:



You would not use the Azure AD Oauth implicit Grant flow. This is an authentication protocol. It will not limit the number of queries run by laboratories or prevent the OWASP TOP 10 security vulnerabilities.

You would not use Azure Trafic Manager. This is a Content Delivery Network that can speed up downloads. It will not limit the number of queries run by laboratories or prevent the OWASP TOP 10 security vulnerabilities.

You would not use Azure SAS tokens. These can be used to share blobs from storage accounts. It will not limit the number of queries run by laboratories or prevent the OWASP TOP 10 security vulnerabilities.

Objective:
Connect to and consume Azure services and third-party services

Sub-Objective:
Implement API management

References:

Microsoft Azure > Architecture > Publishing internal APIs to external consumers

Microsoft Azure > Networking > Web Application Firewall > Azure Web Application Firewall on Azure Application Gateway

Microsoft Azure > API Management > Import and publish your first API

Question #60 of 135

Question ID: 1287163

You are the administrator of Nutex. You' have developed a globally distributed application. This application uses one Cosmos DB storage as the storage solution. You have the following requirements:

- Consistency level: Strong
- Cost for read operations compared to other consistency levels
- Calculate request units for item size of 1 KB.

Which of the following is true of Azure regions you can associate?

A) Azure Cosmos DB accounts cannot be associated with more than one Azure region.

B) Azure Cosmos DB accounts can be associated with any number of Azure regions.

Explanation

Azure Cosmos DB accounts cannot be associated with more than one Azure region. Azure Cosmos DB accounts that are configured to use strong consistency cannot associate more than one Azure region with their Azure Cosmos DB account. Strong consistency has a linearizability guarantee with the reads that allows you to see the most recent version of an item. Once a write is committed durably by the majority quorum of replicas, that write becomes visible. The write has to be committed durably by both the primary and the secondaries or the write is aborted. A read must be acknowledged by the majority read quorum so that a client can never see an uncommitted or partial write.

Objective:
Develop for Azure storage

Sub-Objective:
Develop solutions that use Cosmos DB storage

References:

Microsoft Azure > Cosmos DB > Consistency levels in Azure Cosmos DB

Microsoft Azure > Products > SLA for Azure Cosmos DB

Microsoft Azure > Cosmos DB > Request Units in Azure Cosmos DB

Question #61 of 135

Question ID: 1287182

You are the administrator of the Nutex Corporation. Users from the Marketing user group are configured to use Azure multi-factor authentication. Users from the Sales user group are configured to use Self-Service password reset.

You want to simplify the registration process for all users so that they can register once for Azure multi-factor authentication and Azure Self-Service password reset. Sales users need to do that through a wizard-like experience. For Marketing users, app passwords are absolutely necessary.

What should you do?

A) Enable combined security information registration with Managed mode for the Marketing users.

B) Enable combined security information registration with Managed mode for the Sales users.

C) Enable combined security information registration with Interrupt mode for the Sales users.

D) Enable combined security information registration with Interrupt mode for the Marketing users.

Explanation

You whould enable combined security information registration with Interrupt mode for the Sales users. In the past, users registered authentication methods for Azure multi-factor authentication (MFA) and Self-Service password reset (SSPR) separately. People had to register for both features. With combined security information registration, users only have to register once to get the benefits of both MFA and SSPR. You must use Interrupt mode because this will enforce a wizard-like experience being presented to users when they register or refresh their security information at sign-in.

You would not enable combined security information registration with Managed mode for the Sales users. Managed mode is part of the user profile and allows users to manage their security information. Managed mode does not present a wizard-like experience to the user.

You would not enable combined security information registration with Managed mode for the Marketing users. For Marketing users, app passwords are necessary. App passwords are available only to users who have been enforced for MFA. Users who are enabled for MFA via a Conditional Access policy will not have app passwords available. Therefore, you cannot use the combined security information registration because this will be configured through a Conditional Access policy.

You would not enable combined security information registration with Interrupt mode for the Marketing users because the combined security information registration will be configured through a Conditional Access policy.

Objective:
Implement Azure security

Sub-Objective:
Implement user authentication and authorization

References:

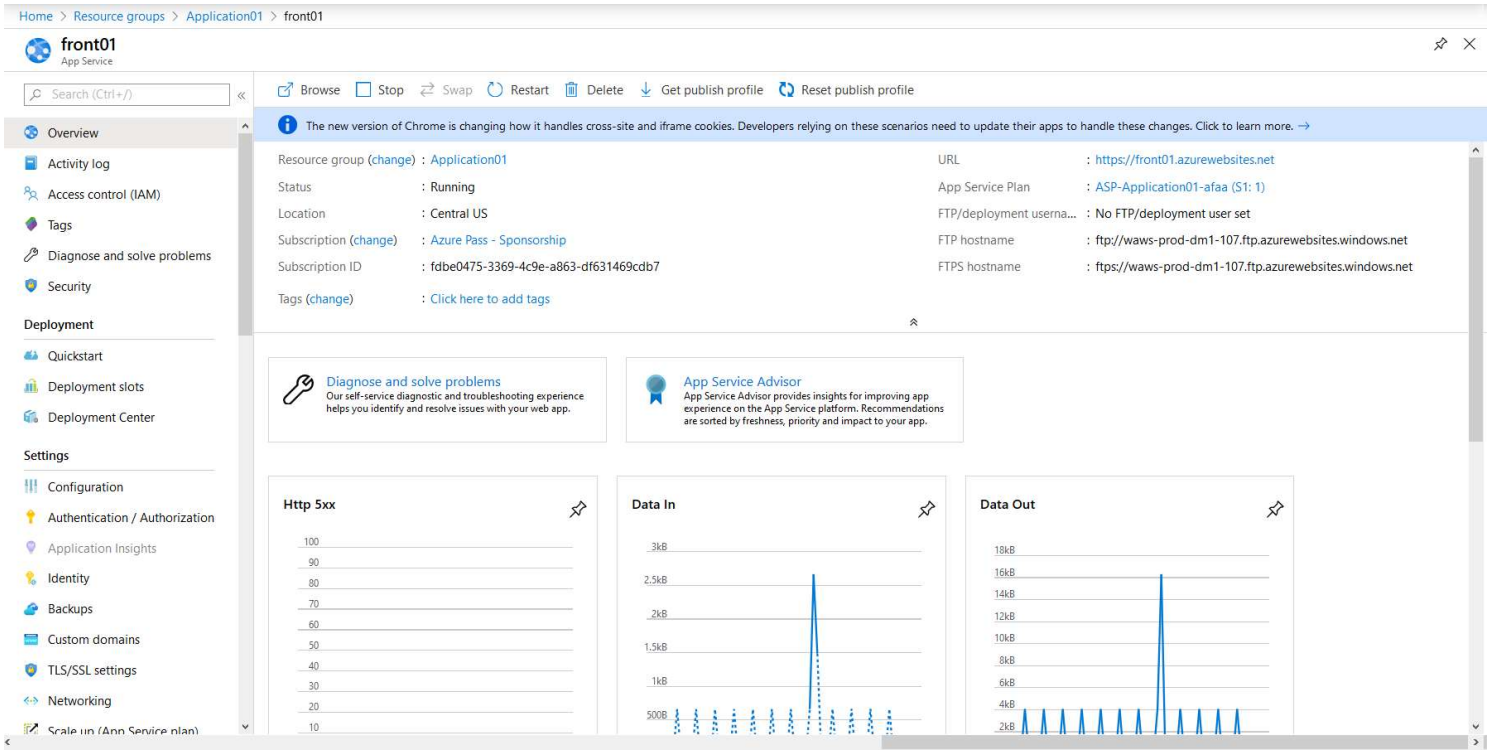
Microsoft Docs > Azure > Active Directory > Combined security information registration overview

---

Question #62 of 135

Question ID: 1287131

You are working as a developer for the Nutex Corporation. You are responsible for the application that sells company goods during Black Friday and Cyber Monday. Your application's Overview pane looks like the following:



You need to configure Automating Autoscaling based on processor utilization that allows you to run at least 19 instances.

Which action should you perform first?

A) Create Scale to a specific instance count.

B) Create Scale based on a metric.

C) Scale-up App Service plan.

D) Configure alerts and actions.

Explanation

The application Overview pane says that the application has an S1 plan that allows scale-out to a maximum of 10 instances. So first you need to scale-up an instance to the Premium service plan and use either the P1V2, P2V2, or P3V2 instance to support at least 19 instances.

You would not choose to create scale based on a metric. This action will not allow you to enter 19 instances.

You would not choose to create scale to a specific instance count. This action will not allow you to enter 19 instances. This action scales an application to a specific count that is not based on processor utilization.

You would not configure alerts and actions. This allows you to receive alerts, but not scale-out the App Service plan.

Objective:
Develop Azure compute solutions

Sub-Objective:
Create Azure App Service Web Apps

References:

Microsoft Azure > App Service pricing

Question #63 of 135

Question ID: 1404425

You are implementing a service that will be installed on a Windows Server 2016 virtual machine on AWS. The service is responsible for uploading users' generated certificates to Azure Key Vault.

What should you do to provide an identity that will be secure to achieve the goal?

Choose the four appropriate steps and place them in the correct order.

{UCMS id=4917480293138432 type=Activity}

Explanation

You should choose the following:

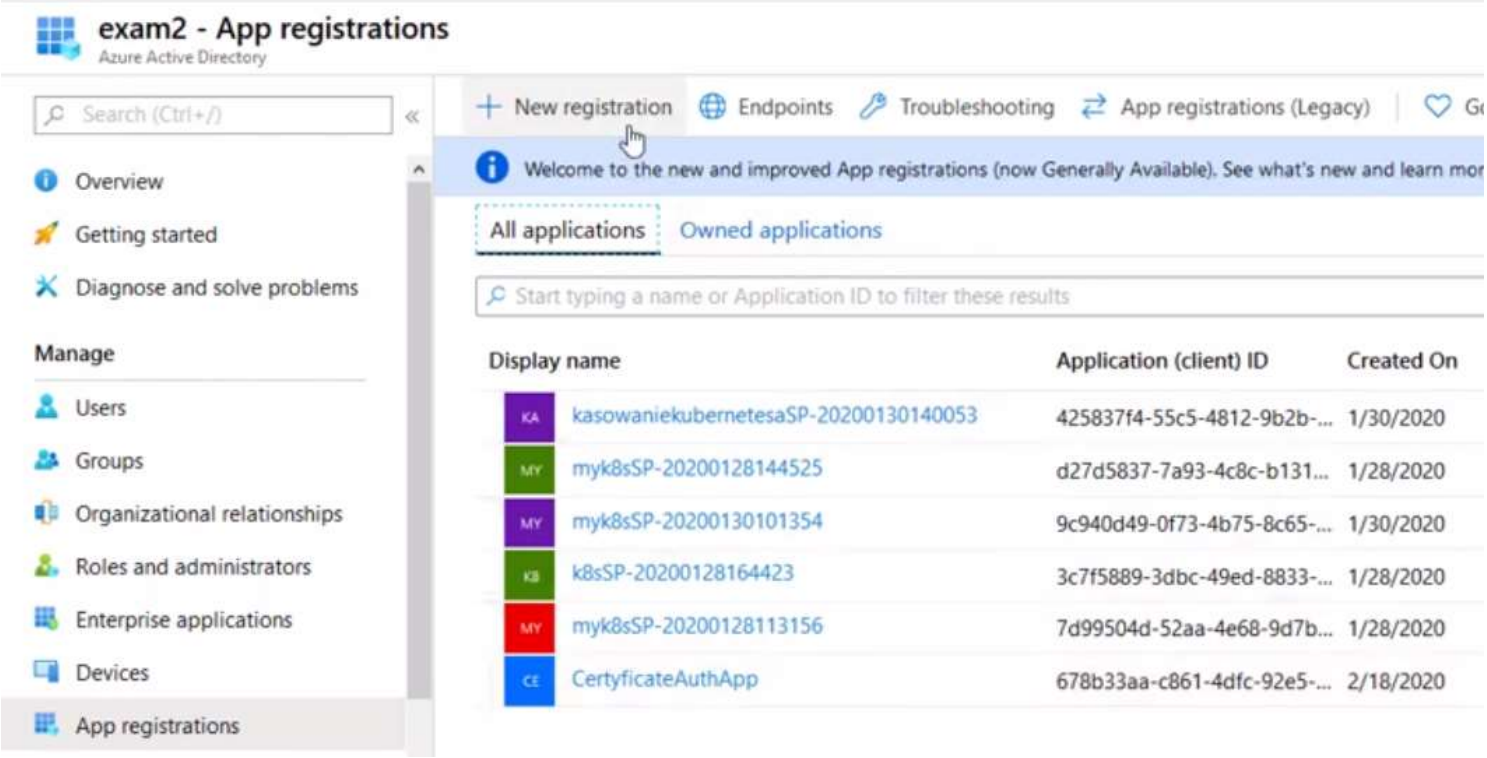
1. Login to portal.azure.com.
2. Open **Azure Active Directory.**
3. Register an application.
4. Create and upload a certificate.

You should have a certificate for the application. The certificate is the way that the application can prove its identity to an authentication service when requesting a token. A client secret or a certificate can be used as a credential. Microsoft recommends using a certificate instead of a client secret for a higher level of assurance. The following script can be used to create a certificate:

```
New-SelfSignedCertificate  -Subject "CN=MyAppCertificate" -CertStoreLocation "cert:\LocalMachine\My" -KeyExportPolicy Exportable -KeySpec Signature
```

You should export the certificate to so it can be uploaded later.

After logging into the portal, you should open **Azure Active Directory**. You need to register the application. Under **App registrations**, choose **New registration,** give the application a name, and speciy the supported account type.



It is not mandatory to create the certificate before registering the application, but typically the certificate is created before registering the application.

After registering the application, you would need to upload the certificate that you created. In the application page, you would choose **Certificates & Secrets**, and then choose **Upload Certificate** to upload the exported certificate.

|~ApplicationCertificates&Secrets.png~|

You do not have to expose an API or download the manifest. These steps use an API and download a configuration of the registered application.

You would not open Security Center. In Security Center, you can see dashboards on security hygiene, information threat protection, and your overall security score. You cannot register an application and upload a certificate to the application in Security Center.

Objective:
Implement Azure security

Sub-Objective:
Implement secure cloud solutions

References:

WIEDZA > Certificate-based authentication for an Azure

Microsoft Docs > Azure > Active Directory > Microsoft identity platform application authentication certificate credentials

---

Question #64 of 135

Question ID: 1403595

You want to create a logic app that monitors changes to a virtual machine named VM01 and sends an email to you about those changes. What should you do?

Choose the appropriate steps and place them in the correct order.

{UCMS id=5737206905831424 type=Activity}

Explanation

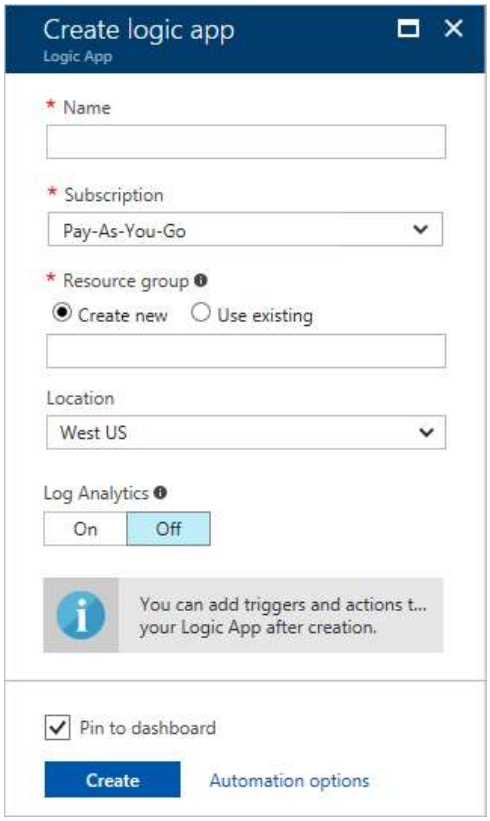
You would choose the following:

1. Create an Azure resource for your logic app.

2. Choose a logic app template to build your logic app.
3. Add an event grid trigger to create a logic app instance.
4. Subscribe your logic app to publisher events.
5. Add a condition to run your logic app workflow.

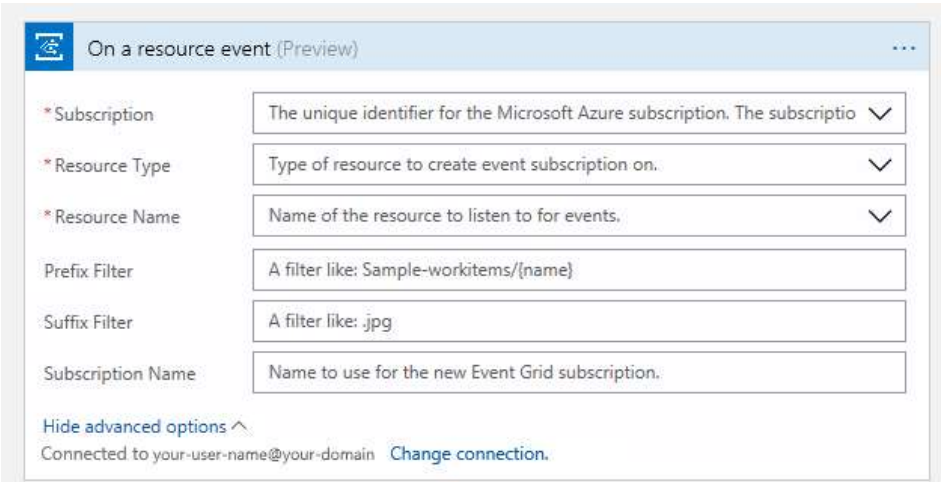
When specific events happen in an Azure resource, you can start an automated logic app workflow. The Azure resource can publish those events to an Azure event grid. The event grid can send those events to subscribers via endpoints such as queues, webhooks, or event hubs. The logic app is the subscriber and waits for those events to happen before running automated workflows which perform tasks.

You would create an Azure resource for your logic app and specify a resource group.



Choose a logic app template to build your logic app from scratch. You can choose **Blank Logic App** under **Templates** in Logic Apps Designer. You should add an event grid trigger to create a logic app instance which starts the logic app workflow. You should add **Azure Event Grid - On a resource event** as the trigger.

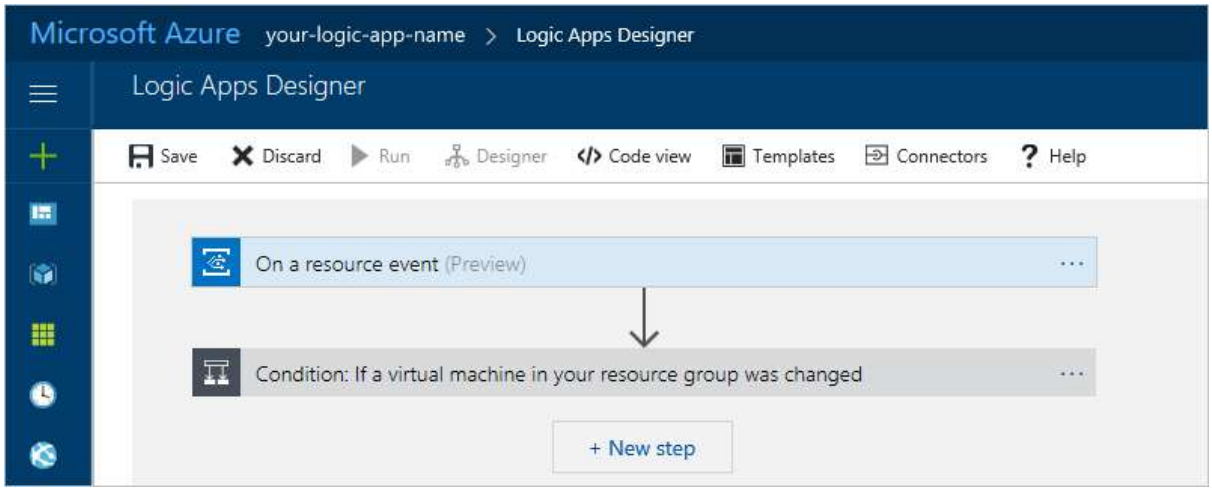
You would subscribe your logic app to publisher events.



Azure automatically creates an event subscription for your logic app to your selected resource when the logic app is saved with an event grid trigger. When the resource publishes events to the event grid, the event grid automatically pushes those events to your logic app. The event calls your logic app, then creates an

instance of the workflow and runs that instance of the workflow.

You will need to add a condition to run your logic app workflow only when a specific event occurs. In this scenario, you would define an action to send an email when something changes on the virtual machine.



Objective:
Connect to and consume Azure services and third-party services

Sub-Objective:
Develop event-based solutions

References:

Microsoft Azure > Messaging services > Event Grid > Tutorial: Monitor virtual machine changes by using Azure Event Grid and Logic Apps

---

Question #65 of 135

Question ID: 1403551

You are the administrator of the Nutex Corporation. You want to enable Azure Disk Encryption on an existing Linux virtual machine with the **Set-AzVMDiskEncryptionExtension** PowerShell cmdlet.

Which of the following is NOT an additional prerequisite for Linux IaaS VMs?

A) Azure Key Vault integration
B) persistent block device name
C) vfat module
D) dm-crypt module

Explanation

Azure Key Vault integration is a mandatory prerequisite and not an additional prerequisite for Linux IaaS VMs. Azure Disk Encryption needs the Key Vault. The Key Vault and the VMs need to be co-located in the same region.

You would not choose the dm-crypt module and the vfat module, because Azure Disk Encryption requires the dm-crypt and vfat modules to be present on the system. Thus, they are mandatory prerequisites. Removing or disabling vfat from the default image will prevent the system from reading the key volume and obtaining the key needed to unlock the disks on subsequent reboots.

You would not choose the persistent block device name, because you have to use a persistent block device name. Device names in the "`/dev/sdX`" format should not be relied upon to be associated with the same disk across reboots and especially after encryption has been applied.

Objective:
Develop Azure compute solutions

Sub-Objective:
Implement IaaS solutions

References:

Microsoft Azure > Security > Azure Disk Encryption for virtual machines and virtual machine scale sets

---

Question #66 of 135

Question ID: 1287210

The Nutex Sales team uses a variety of tools and applications to monitor a variety of moving parts. Nutex has decided to implement Azure OMS Log Analytics.

There are some specific VMs that have been identified that need a bit more watching than the others. You are going to add appropriate agents to each VM to ensure their metrics are added to the Nutex Log Analytics service.

What information is needed when installing the agents to ensure that they work properly?

A) Active Directory username and password

B) Workspace ID and Workspace (Primary) Key

C) Performance Monitor counters and destination directory

D) Azure username and password

Explanation

You need the the Workspace ID and Workspace (Primary) Key. This information must be collected from the Azure Portal Log Analytics workspace that the agent will be configured on. The Workspace ID and Workspace (Primary) Key are needed to configure the agent and ensure it can successfully communicate with Log Analytics in Azure commercial and US Government clouds.

The following are not important or unnecessary when installing the agents:

Azure username and password are not needed during the Agent install, but prior to the install these will be used to log in to the Azure Portal.

There is no need to select specific Performance Monitor counters and the destination directory. However, the destination directory will be defined during the install.

The Active Directory account credentials must be used to access the VM on which the agent is to be installed, but during the install this information is not necessary

Objective:
Monitor, troubleshoot, and optimize Azure solutions

Sub-Objective:
Instrument solutions to support monitoring and logging

References:

Microsoft Azure > Azure Monitor > Collect data from an Azure virtual machine with Azure Monitor

Microsoft Azure > Azure Monitor > Overview of log queries in Azure Monitor

Microsoft Azure > Azure Monitor > Connect Windows computers to Azure Monitor -

---

Question #67 of 135

Question ID: 1403590

You are the administrator of the Nutex Corporation. You have created an ASP.NET MVC web application in Visual Studio. You have added Application Insights Telemetry to your project.

Which of the following code lines tracks exceptions to an automatically applied code change to your **FileConfig.cs** file?

A) `instrumentationKey:"7812zdg"`

B) `"ProviderId": "Microsoft.ApplicationInsights.ConnectedService.ConnectedServiceProvider"`

C) `filters.Add(new HandleErrorAttribute());`

D) `filters.Add(new ErrorHandler.AiHandleErrorAttribute());`

Explanation

You would use `filters.Add(new ErrorHandler.AiHandleErrorAttribute());`. The `AiHandleErrorAttribute` class is in the ErrorHandler folder. Everytime an exception is made, this class attribute will log the exception. You can also use the `AiHandleErrorAttribute` class as an exception filter.

You would not use `"ProviderId": "Microsoft.ApplicationInsights.ConnectedService. ConnectedServiceProvider"`, because this change is in the **ConnectedService.json** file.

You would not use `filters.Add(new HandleErrorAttribute());` because this is the line of code used to put the HandleError attribute in its basic state. It is used before adding Application Insights telemetry to the project.

You would not use `instrumentationKey:"7812zdg"` because the instrumentation key and its value are added to the **_Layout.cshtml** file.

Objective:
Monitor, troubleshoot, and optimize Azure solutions

Sub-Objective:
Instrument solutions to support monitoring and logging

References:

YouTube > Azure Monitor - Application Insights - Intro to Monitoring ASP.NET

Microsoft Azure > Azure Monitor > Create an Application Insights resource

Microsoft Azure > Azure Monitor > Set up Application Insights for your ASP.NET website

Microsoft Azure > Azure Monitor > Instrument web apps at runtime with Application Insights Codeless Attach

---

Question #68 of 135

Question ID: 1287205

You are the administrator of the Nutex Corporation. You have a web application hosted in Azure. You have configured application insights to support exception reporting. To get diagnostic data specific to your app, you can insert code to send your own telemetry data. This data is displayed in a diagnostic search alongside the request, page view, and other automatically collected data. For that, you have several options. Apply the relevant description to the appropriate option.

{UCMS id=6594869301608448 type=Activity}

Explanation

TrackEvent() is used to count various events and is commonly used for monitoring usage patterns. The data it sends appears under Custom Events in a diagnostic search. You can use these events to filter your diagnostic searches because events are named and can carry string properties and numeric metrics.

TrackTrace() allows you to send a "breadcrumb trail" to help diagnose problems. You can use this option to send longer data, such as POST information.

TrackException() allows you to send stack traces. You can capture exceptions automatically or log exceptions explicitly.

Diagnostic Search captures logs from frameworks such as Log4Net or NLog. You can view these logs in a diagnostic search alongside request and exception data.

Objective:
Monitor, troubleshoot, and optimize Azure solutions

Sub-Objective:
Instrument solutions to support monitoring and logging

References:

Microsoft Azure > Azure Monitor > Diagnose exceptions in your web apps with Application Insights

---

Question #69 of 135

Question ID: 1287112

You are the administrator of the Nutex Corporation. You want to build images based on Linux and Windows for your Azure solutions.

Which Azure services can you use? (Choose all that apply.)

A) ImageX
B) Azure Kubernetes Service
C) Azure Pipelines
D) Azure Container Registry tasks

Explanation

You can use Azure Container Registry tasks and Azure Pipelines.

Azure Container Registry tasks allows you to build on-demand docker container images in the cloud.

Azure Pipelines allow you to implement a pipeline for building, testing, and deploying an app. The Azure Pipelines service allows you to build images for any repository containing a dockerfile.

You would not choose the Azure Kubernetes Service, because this service is there to manage container images for solutions and not to build images.

You would not choose the ImageX utility, because this is not an Azure service and cannot be used to create container images. ImageX allows you to capture an image of a hard drive in a Windows Imaging Format (WIM) file.

Objective:
Develop Azure compute solutions

Sub-Objective:
Implement IaaS solutions

References:

Microsoft Docs > Azure DevOps > Azure Pipelines > Build an image

Microsoft Azure > Container Registry > Azure Container Registry Documentation

---

Question #70 of 135

Question ID: 1287200

You are working as a developer for the Nutex Corporation. You are responsible for an online e-store system using PHP 7.4 with Azure CDN that uses default settings, which has been in place for more than ten months. You are preparing for Black Friday and Cyber Monday, and during this period you want some of the pictures in the store to be cached for 24 hours and the rest cached for 48 hours.

How can you achieve this? (Choose all that apply. Each answer is a complete solution.)

A) Use headers in your e-store system.
B) Add the PHP_EXTENSIONS key in the **Application Settings** section of the configuration blade.
C) Add PHP_INI_SCAN_DIR to App Settings.
D) Add php.ini to the wwwroot directory.

E) Enable Composer automation in Azure.

F) Use caching rules in CDN.

Explanation

You can do either of the following:

- Use caching rules in CDN.
- Use headers in your e-store system.

Azure Content Delivery Network (CDN) allows files from publicly accessible origin web servers to be cached for as long as their time to live (TTL) allows. The `Cache-Control` header determines the time of the TTL in the HTTP response from the origin server.

The expiration of web content in Azure CDN can be done in the following ways:

- Setting Cache-Control headers by using CDN caching rules.
- Setting Cache-Control headers by using configuration files.

Using caching rules is the recommended method for setting a web server's `Cache-Control` header.

If you have static content such as images and style sheets, you can modify the **applicationHost.config** or **Web.config** configuration files of your web application to control the update frequency. You can use the `<system.webServer>/<staticContent>/<clientCache>` element in either the **applicationHost.config** or **Web.config** file to set the `Cache-Control` header for your content.

You would not add PHP_INI_SCAN_DIR to App Settings. This addition can be used for the configuration of PHP, but not for headers.

You would not add the PHP_EXTENSIONS key in the Application Settings section of the Configuration blade. This addition can be used for loading extensions for a PHP interpreter, but not for headers.

You would not enable Composer automation in Azure. Composer automation allows you to add Git add, Git commit, and Git push commands to your app. Composer automation will not add a custom .dll extension to PHP.

You would not add the php.ini file to the wwwroot directory. A php.ini file does not work in the web app.

Objective:
Monitor, troubleshoot, and optimize Azure solutions

Sub-Objective:
Integrate caching and content delivery within solutions

References:

Microsoft Azure > Networking > CDN > Manage expiration of web content in Azure CDN

Question #71 of 135

Question ID: 1287124

You need to monitor containers with Log Analytics. You need to know which log types can display the information that you need.

Match the appropriate log type with its description. All choices can only be used once.

{UCMS id=5722624954990592 type=Activity}

Explanation

You can have the following log types in Log Analytics:

- **ContainerImageInventory** – This can be used to locate information organized by image and to view image information such as sizes or image IDs.
- **ContainerInventory** – This shows information about the container location, the image names, and what images are running.
- **ContainerLog** – This can be used to locate specific error log information and entries.
- **ContainerNodeInventory_CL** – This can be used to find information about the host/node where containers are residing. It also shows you the Docker version, orchestration type, storage, and network information.

- **ContainerProcess_CL** – This shows you the process running within the container.
- **ContainerServiceLog** – This can be used to locate audit trail information for the Docker daemon, such as start, stop, delete, or pull commands.
- **KubeEvents_CL** – This can be used to find the Kubernetes events.
- **KubePodInventory_CL** – This can be used to find the cluster hierarchy information.

Objective:
Develop Azure compute solutions

Sub-Objective:
Implement IaaS solutions

References:

Microsoft Azure > Azure Monitor > Container Monitoring solution in Azure Monitor

---

Question #72 of 135

Question ID: 1403596

You are the administrator of the Nutex Corporation. You use the Event Grid service to route events to subscribers. You have an application that sends events in the following format:

```
[
  {
    "myEventTypeField":"Created",
    "resource":"Users/example/Messages/1000",
    "resourceData":{"someDataField1":"SomeDataFieldValue"}
  }
]
```

You want to create a custom topic. The delivered event must have the following format:

```
{
  "id": "aa5b8e2a-1235-4032-be8f-5223395b9eae",
  "eventTime": "2018-11-07T23:59:14.7997564Z",
  "eventType": "Created",
  "dataVersion": "1.0",
  "metadataVersion": "1",
  "topic": "/subscriptions/<subscription-id>/resourceGroups/myResourceGroup/providers/Microsoft.EventGrid/topics/demotopic",
  "subject": "DefaultSubject",
  "data": {
    "myEventTypeField": "Created",
    "resource": "Users/example/Messages/1000",
    "resourceData": {
    "someDataField1": "SomeDataFieldValue"
    }
  }
}
```

When subscribing to the custom topic, you must specify the schema that you would like to use for receiving the events.

Which schema you should you use?

A) Event Grid schema

B) CloudEvents schema

C) Custom events schema

Explanation

You would use the Event Grid schema because these fields contain the mappings from the custom topic. The **myEventTypeField** is mapped to **EventType**. The default values for DataVersion and Subject are used. The Data object contains the original event schema fields.

You would not use the CloudEvents schema. Azure Event Grid natively supports events in the JSON implementation of CloudEvents v1.0 and HTTP protocol binding, in addition to its default event schema. CloudEvents is an open specification for describing event data. CloudEvents simplifies interoperability by providing a common event schema for consuming and publishing cloud-based events. This provides a schema for standard ways of routing and handling events, uniform tooling, and universal ways of deserializing the outer event schema. You can more easily integrate work across platforms with a common schema.

You would not use a Custom events schema because these are used only when creating a custom mapping between your schema and the event grid schema.

Objective:
Connect to and consume Azure services and third-party services

Sub-Objective:
Develop event-based solutions

References:

Microsoft Azure > Messaging services > Event Grid > Map custom fields to Event Grid schema

GitHub > What is the difference between Event Grid Schema & Cloud Event Schema?

Microsoft Azure > Messaging services > Event Grid > Use CloudEvents v1.0 schema with Event Grid

---

Question #73 of 135

Question ID: 1403564

You are the administrator of the Nutex Corporation. You have enabled diagnostic logging for failed request traces on your Azure web app named **NutexWebApp**. You want to view the logged information in an easy manner. What should you do?

A) Use Log Parser.
B) Open the CSV file in blob storage.
C) Stream logging information with Azure CLI.
D) Open the freb.xsl file.

Explanation

You would open the freb.xsl file because failed request traces are stored in XML files named fr####.xml in the **/LogFiles/W3SVC#########/** directory. To make it easier to view the logged information, an XSL stylesheet named **freb.xsl** is provided in the same directory as the XML files.

You would not stream logging information with Azure CLI. By streaming logging information through Azure CLI, you can only stream information from .TXT, .LOG, or .HTM files, not .XML. With the command `az webapp log tail` you can stream logging information.

You would not open the CSV file in blob storage because failed request trace logging information is not stored in CSV-format in blob storage.

You would not use Log Parser because with the Log Parser utility you view web server logs and not failed request trace log information.

Objective:
Develop Azure compute solutions

Sub-Objective:
Create Azure App Service Web Apps

References:

Microsoft Azure > App Service > Web Apps > Enable diagnostics logging for apps in Azure App Service

Question #74 of 135

Question ID: 1287148

When the Nutex Sales application experiences an internal error, it creates a new error report file in an Azure Storage blob account with all the details of the error.

You want the IT Department to be notified whenever this happens, so you have decided to capture Blob storage events. You already have an Azure Automation Runbook that will copy the file and send a message to the appropriate Nutex IT Microsoft Teams channel.

What must you do to capture the storage events and ensure that your Runbook is called? (Choose all that apply.)

A) Create and name a webhook in the Runbook.

B) Target the URL of the Runbook webhook in the event Subscription.

C) Create a subscription for the BlobCreated event.

D) Create a subscription for the FileCreated event.

E) Target the URL of the Microsoft Teams webhook in the event Subscription.

Explanation

You would do the following:

- Create and name a webhook in the Runbook.
- Create a subscription for the BlobCreated event.
- Target the URL of the Runbook webhook in the event Subscription.

You would create and name a webhook in the Runbook. This action grants you the ability to call the Runbook from other locations such as Event Grid subscriptions.

You would create a subscription for the BlobCreated event. This will allow Event Grid to alert you when a blob is created using the PutBlob, PutBlockList, or CopyBlob operations.

You would target the URL of the Runbook webhook in the event subscription. This action will be the target of the alert and cause the Runbook to fire when the event happens.

You would not create a subscription for the FileCreated event. This is not going to fire in Blob Storage as indicated by the scenario.

You would not target the URL of the Microsoft Teams webhook in the event subscription. This could work if all you wanted was a message sent to the Microsoft Teams channel. However, since we need the file copied and the Microsoft Teams notified, a Runbook with the file that needs to be copied and the URL of the Microsoft Teams webhook should be the target. Do not be fooled, though, there is a webhook for Microsoft Teams involved, but it is being used in the Runbook.

Objective:
Develop Azure compute solutions

Sub-Objective:
Implement Azure functions

References:

Microsoft Docs > Azure > Storage > Reacting to Blob storage events

Microsoft Docs > Azure > Storage > Quickstart: Route storage events to web endpoint with Azure CLI

Microsoft Azure > Messaging services > Tutorial: Integrate Azure Automation with Event Grid and Microsoft Teams

Question #75 of 135

Question ID: 1287155

You are the administrator of the Nutex Corporation. You have a hotel multi-tenant application that manages reservations and payments for the hotel rooms. Each room is identified by a Cosmos DB storage document where the room's information is located. The hotel is identified by a value in the **hotelid** field and

the room by the value in the **roomid** field. Your document contains six hotel rooms with three different **hotelid** distinct values.

You need to decide which partitioning scheme is the best for your application. You want to improve the query performance when you query different hotels. You have determined a proper partition key, but you are afraid of hitting the 10 GB limit per logical partition.

What is the best solution for the partitioning scheme?

A) Use two different partition key JSON properties.

B) Use the **hotelid** values.

C) Find a mandatory value that can have at least two distinct values for a hotel.

D) Use three different partition key JSON properties.

Explanation

You would find a mandatory value that can have at least two distinct values for a hotel. Using this partitioning scheme allows you to divide the documents across partitions. In this case, queries related to the same hotel will be spread across more logical partitions, which will improve the query performance because of more physical resources in the background.

You would not use the **hotelid** values because documents from the same hotel will be placed on a distinct logical partition. Each hotel can have documents up to 10 GB. Queries across the same hotel will perform well since they will not span multiple logical partitions. However, the 10 GB limit may be reached when the room count grows.

You would not use two or three different partition key JSON properties because CosmosDB supports only one JSON property for the partition key. A JSON property can have multiple values, but you can only have one JSON property for the partition key. For example, if you estimate that each hotel may generate 15 GB of documents, the documents will be spread over two logical containers because of the 10 GB limit. If **hotelid** only has a single distinct value per hotel then it is not a good partition key. Also, each hotel can have multiple rooms so there would be multiple room IDs. You could create a single JSON property that had multiple values. You could create a property called PartitionKey with two values: Hotel1 if the **roomid** is odd and Hotel2 if the **roomid** is even.

Objective:
Develop for Azure storage

Sub-Objective:
Develop solutions that use Cosmos DB storage

References:

BuildWindows > Understanding Azure Cosmos DB Partitioning and Partition Key

Microsoft Azure > Cosmos DB > Partitioning in Azure Cosmos DB

Question #76 of 135

Question ID: 1403558

You have an application named **MyApp** deployed in Kubernetes. The application needs to be updated. It needs to keep running during the update and should prove a rollback mechanism if a deployment failure occurs. What actions should you perform to the update?

Place the appropriate choices in the correct order.

{UCMS id=5629526170140672 type=Activity}

Explanation

You would choose the following:

1. Change the application code in the **config_file.cfg** file.
2. Use the **docker-compose up --build** command to re-create the application image.
3. Tag the image with the *loginServer* of the container registry.
4. Use the **docker push** command to push the image to the registry.

You would first make the change in the application by opening the **config_file.cfg** file with any code or text editor and making the appropriate changes to the code.

Once the application has been updated, you would re-create the application image and run the updated application. You can use the **docker-compose** command with the `--build` parameter to re-create the application image. The `-d` parameter should not be used because it runs containers in the background, and does not recreate the image.

```
docker-compose up -build
```

After you have recreated the image and tested the application, you would tag the image with the *loginServer* of the container registry. You can use the **docker tag** command to tag the image with the loginServer of the container registry. The following tags the azure-MyApp image with the loginServer of the container registry named **acrNutex**, and, adds :**v2** to the end of the image name:

```
docker tag azure-Myapp acrNutex/azure-Myapp:v2
```

Once the image has been tagged, you would push the image to the registry with the **docker push** command. The following pushes the image to the acrNutex loginServer:

```
docker push azure-Myapp acrNutex/azure-Myapp:v2
```

You should ensure that multiple instances of the application pod are running to ensure maximum uptime. You would type the **kubectl scale** command to scale the resources. You can use the `--replicas` parameter to set the number of pods. The following command ensures that three pods are running:

```
kubectl scale --replicas=3 deployment/MyApp-front
```

You would not edit the **config.sys** file. The config.sys file was used to configure the MS-DOS and Windows 3.X operating systems.

Objective:
Develop Azure compute solutions

Sub-Objective:
Implement IaaS solutions

References:

Microsoft Azure > AKS > Tutorial: Update an application in Azure Kubernetes Service (AKS)

Question #77 of 135

Question ID: 1403579

Your application depends on Azure storage. You use the Azure storage diagnostics to capture metrics and log data. This data can later be used to analyze the storage service usage and diagnose issues with requests made against the storage account.

You need to use a cmdlet to change the retention period of captured log data for the blob service. Which cmdlet can help you accomplish the task?

A) You can only use the management portal to set the retention period.

B) **`Set-AzureStorageServiceMetricsProperty`**

C) **`Set-AzureStorageAccount`**

D) **`Set-AzureStorageServiceLoggingProperty`**

Explanation

You would use **`Set-AzureStorageServiceLoggingProperty`**. With this cmdlet, you can modify the retention policy for log settings for Blob, Table, or Queue service. The following example turns on logging for read, write, and delete requests in the Queue service in your default storage account with retention set to three days:

```
Set-AzureStorageServiceLoggingProperty -ServiceType Queue -LoggingOperations read,write,delete -RetentionDays 3
```

You would not use **`Set-AzureStorageServiceMetricsProperty`**. This cmdlet is similar to the one above, but it modifies the retention policy for the metric settings for Blob, Table, or Queue service instead of the log settings.

You would not use **`Set-AzureStorageAccount`**. This cmdlet is used to modify the label and type of a storage account.

You would not select the option that the retention period can only be set using the management portal. You can depend on PowerShell commands to set almost anything in Azure. In this scenario, you can use **`Set-AzureStorageServiceLoggingProperty`** to set the retention period for log settings for the blob.

Objective:
Develop for Azure storage

Sub-Objective:
Develop solutions that use blob storage

References:

Microsoft Docs > Azure > Storage > Azure Storage analytics logging

Microsoft Docs > Blog Archive > Change the retention days of the logs from the Management Portal for a Cloud Service (PAAS)

Microsoft Azure > PowerShell > Set-AzureStorageServiceLoggingProperty

Microsoft Azure > PowerShell > Set-AzureStorageServiceMetricsProperty

---

Question #78 of 135

Question ID: 1287165

You are the administrator of Nutex. You have developed a globally distributed application. This application uses one Cosmos DB storage as the storage solution. You have the following requirements:

- Consistency level: Strong
- Cost for read operations compared to other consistency levels
- Calculate request units for item size of 1 KB.

How you can calculate the request units/s?

A) (Reads/second*1.3) + (Writes/second*7)

B) (Reads/second*1) + (Writes/second*5)

C) (Reads/second*10) + (Writes/second*48)

Explanation

You would use the formula (Reads/second*1) + (Writes/second*5) because a request unit is a normalized measure of request processing cost. A single request unit represents the processing capacity required to read (via self-link or id) a single 1 KB item consisting of 10 unique property values (excluding system properties). A request to create (insert), replace, or delete the same item will consume more processing from the service and thereby consume more request units. The formula for an item size of 1 KB is: (Reads/second*1) + (Writes/second*5).

All the other answers are incorrect.

Objective:
Develop for Azure storage

Sub-Objective:
Develop solutions that use Cosmos DB storage

References:

Microsoft Azure > Cosmos DB > Consistency levels in Azure Cosmos DB

Microsoft Azure > Products > SLA for Azure Cosmos DB

Microsoft Azure > Cosmos DB > Request Units in Azure Cosmos DB

Question #79 of 135

Question ID: 1403549

You are the administrator of the Nutex Corporation. You want to create a new Azure Windows VM named **VMNutex** in a resource group named **RG1** using Visual Studio and C#.

The virtual machine needs to be a member of an availability set and needs to be accessible through the network.

Which steps should you perform? Select the necessary steps and put them in the correct order.

{UCMS id=6751722077683712 type=Activity}

Explanation

You would choose the following:

1. Create a Visual Studio project.
2. Type `Install-Package Microsoft.Azure.Management.Fluent` in the Package Manager Console.
3. Create the `azureauth.properties` file.
4. Create the management client.
5. Add this code to the `Main` method:

```
var groupName = "RG1"; var vmName = "VMNutex"; var location = Region.USWest; Console.WriteLine("Creating resource group...");
var resourceGroup = azure.ResourceGroups.Define(groupName).WithRegion(location).Create();
```

1. Add this code to the `Main` method:

```
Console.WriteLine("Creating availability set...");
var availabilitySet = azure.AvailabilitySets.Define("myAVSet").WithRegion(location)
.WithExistingResourceGroup(groupName).WithSku(AvailabilitySetSkuTypes.Managed).Create();
```

1. Add the code to create the public IP address, the virtual network, and the network interface.
2. Add this code:

```
“azure.VirtualMachines.Define(vmName).WithRegion(location)
.WithExistingResourceGroup(groupName).WithExistingPrimaryNetworkInterface(networkInterface)
.WithLatestWindowsImage("MicrosoftWindowsServer", "WindowsServer", "2012-R2-Datacenter")
.WithAdminUsername("AtlFalcon").WithAdminPassword("Ih8DaN0S8ntZ")
.WithComputerName(vmName).WithExistingAvailabilitySet(availabilitySet)
.WithSize(VirtualMachineSizeTypes.StandardDS1).Create();
```

1. Run the application.

First, you need to create a Visual Studio project. You will then install the NuGet package so that you can add the additional libraries that you need in Visual Studio. You would choose **Tools > Nuget Package Manager.** From the Package Manager Console, you would type `Install-Package Microsoft.Azure.Management.Fluent`.

You would then create the `azureauth.properties` file. This file ensures that you have access to an AD service principal and you can do that through the authorization properties in the `azureauth.properties` file.

You would then create the management client. This can be done by opening the `Program.cs` file of the project and adding the following statements to the top of the file:

```
using Microsoft.Azure.Management.Compute.Fluent;
using Microsoft.Azure.Management.Compute.Fluent.Models;
using Microsoft.Azure.Management.Fluent;
using Microsoft.Azure.Management.ResourceManager.Fluent;
using Microsoft.Azure.Management.ResourceManager.Fluent.Core;
```

To complete the management client creation, you would add the following code to the Main method:

```
var credentials = SdkContext.AzureCredentialsFactory
    .FromFile(Environment.GetEnvironmentVariable("AZURE_AUTH_LOCATION"));

var azure = Azure
    .Configure()
    .WithLogLevel(HttpLoggingDelegatingHandler.Level.Basic)
    .Authenticate(credentials)
    .WithDefaultSubscription();
```

Then you need to create the resource group since all resources must be contained in the resource group. You can add the following code to the Main method to create the resource group:

```
“var groupName = "RG1"; var vmName = "VMNutex"; var location = Region.USWest; Console.WriteLine("Creating resource group...");
var resourceGroup = azure.ResourceGroups.Define(groupName).WithRegion(location).Create();
```

You will then need to create an availability set because an availability set allows you to maintain virtual machines that are used by your applications. You can create the availability set by adding the following code to the Main method:

```
Console.WriteLine("Creating availability set..."); var availabilitySet =
azure.AvailabilitySets.Define("myAVSet").WithRegion(location)
.WithExistingResourceGroup(groupName).WithSku(AvailabilitySetSkuTypes.Managed).Create();
```

Then you need to add the code to create the public IP address, the virtual network, and the network interface. The virtual machine needs a public IP to communicate with the virtual machine. A virtual machine must be in a subnet of the virtual network and has to have a network interface to communicate on the virtual network.

You will then create the virtual machine. You can create the virtual machine by adding the following code to the Main method:

```
azure.VirtualMachines.Define(vmName).WithRegion(location)
.WithExistingResourceGroup(groupName).WithExistingPrimaryNetworkInterface(networkInterface)
.WithLatestWindowsImage("MicrosoftWindowsServer", "WindowsServer", "2012-R2-Datacenter")
.WithAdminUsername("AtlFalcon").WithAdminPassword("Ih8DaN0S8ntZ")
.WithComputerName(vmName).WithExistingAvailabilitySet(availabilitySet)
.WithSize(VirtualMachineSizeTypes.StandardDS1).Create();
```

Then you will run the application. To run the code in Visual Studio, you have to run the application.

Objective:
Develop Azure compute solutions

Sub-Objective:
Implement IaaS solutions

References:

Microsoft Azure > Virtual Machines > Windows > Create and manage Windows VMs in Azure using C#

Question #80 of 135

Question ID: 1403550

You are the administrator of the Nutex Corporation. You want to deploy some virtual machines through an ARM template. You need a virtual network named **VNET1** with a subnet named **Subnet1**, which has to be defined as a child resource. For that you have to define the corresponding JSON template.

Choose one of the following possibilities to complete the following ARM template.

A) `originHostHeader`

B) `dependsOn`

C) `parametersLink`

D) `location`

Explanation

You would use the `dependsOn` element because the child resource, which is the subnet that is marked as dependent on the parent, is the VNet resource. The parent resource must exist before the child resource can be deployed.

You would not use the `originHostHeader` element, because this element is used as a reference function to enable an expression. This expression derives its value from another JSON name or runtime resources.

You would not use the `parametersLink` element, because you use this element to link an external parameter file.

You would not use the `location` element, because this element defines the geographical location.

Objective:
Develop Azure compute solutions

Sub-Objective:
Implement IaaS solutions

References:

Microsoft Azure > Resource Manager > Define the order for deploying resources in ARM Templates

Microsoft Azure > Resource Manager > Using linked and nested templates when deploying Azure resources

Microsoft Azure > Resource Manager > Resource iteration in ARM templates

Question #81 of 135

Question ID: 1403588

You are the administrator of the Nutex Corporation. You use different CDN solutions. You want your users always to obtain the latest copy of your assets. You want to purge cached content from all edge nodes and force them all to retrieve newly updated assets. You use Azure CDN from Microsoft, Azure CDN from Verizon, and Azure CDN from Akami.

On which caching service is the purge request processing the fastest?

A) Azure CDN from Microsoft

B) Azure CDN from Akamai

C) Azure CDN from Verizon

Explanation

You would use Azure CDN from Akamai because it is faster than Azure CDN from Microsoft or Azure CDN from Verizon. Purge requests take approximately 10 seconds with Azure CDN from Akamai, approximately 10 minutes to process with Azure CDN from Microsoft, and approximately two minutes with Azure CDN from Verizon.

You would not use Azure CDN from Microsoft because it has a limit of 50 concurrent purge requests at any given time at the profile level.

You would not use Azure CDN from Verizon because it also has a limit of 50 concurrent purge requests at any given time at the profile level.

Objective:
Monitor, troubleshoot, and optimize Azure solutions

Sub-Objective:
Integrate caching and content delivery within solutions

References:

Microsoft Azure > Networking > CDN > Purge an Azure CDN endpoint

Microsoft Azure > CDN > Endpoints – Purge Content:

Question #82 of 135

Question ID: 1287176

You are working as an Azure architect for your company and are involved in an application review for a corporate system implemented around the globe. The system is installed on medical equipment looking for new vaccines and automatically interacts with blob storage sending DNA data. Every branch which uses the system uploads data. Five thousand such devices are currently operating worldwide. Uploaded data from the medical device is going to the nearest Azure region. Once a day, you copy data to the central Azure storage account using an asynchronous copy. You notice that sometimes the copy operation fails with HTTP status code 412 (Precondition Failed).

Which actions should you perform to resolve the issue? (Choose all that apply. Each answer is a complete solution.)

A) Use SAS tokens.

B) Create a snapshot and copy the snapshot.

C) Use CloudBlob.StartCopyAsync.

D) Use CopyBlob (synchronous).

E) Use Lease Blob.

F) Use CloudBlob.StartCopy.

Explanation

You could use either of the following:

- Use Lease Blob.

- Create a snapshot and copy the snapshot.

HTTP status code 412 (Precondition Failed) occurs when the source blob is modified when the copy operation is pending in an asynchronous copy. The Lease Blob operation creates and manages a temporary lock from 15 to 60 seconds or a permanent lock on a blob for write and delete operations.

You can also create a blob snapshot and copy that snapshot. A snapshot is useful for backing up blobs because, by its nature, a snapshot is a read-only version of the blob at the time the snapshot was taken.

You would not use SAS tokens. SAS tokens are used for permissions only. They cannot be used to make a copy of a blob or place a temporary lock on a blob.

You would not use CopyBlob (synchronous) or use CloudBlob.StartCopy. Both allow you to copy blobs between storage accounts. However, if there are any changes being made to the source while the copy is in progress using either method, the copy will fail.

You would not use CloudBlob.StartCopyAsync. CloudBlob.StartCopyAsync allows you to complete the operation asynchronously and returns a response if the copy operation has completed, and also returns a successful response when the copy is accepted (HTTP status code 202). However, an asynchronous copy of blob does not prevent HTTP status code 412 when any source access condition does not match.

Objective:
Develop for Azure storage

Sub-Objective:
Develop solutions that use blob storage

References:

Microsoft Azure > Storage Services > Lease Blob

Microsoft Azure > Storage Services > Copy Blob

Microsoft Docs > Blog Archive > Introducing Asynchronous Cross-Account Copy Blob

Microsoft Docs > Azure > Storage > Blobs > Create and manage a blob snapshot in .NET

Question #83 of 135

Question ID: 1422639

You are working as a developer for the Nutex Corporation. You are responsible for developing a new online e-store system using ASP.NET Core 3.1 and ASP .NET V3.5. You deployed a .NET Core 3.1 LTS web app to the resource group name Application01 using the below parameters successfully:

|~WebAppReview&Create1.png~|

However, you cannot deploy the ASP.NET web app to the Application01 resource group. You receive the error that states: "`The template deployment 'Microsoft.Web-WebApp-Portal-9bbde857-8bb3' is not valid according to the validation procedure. The tracking id is 'e00d1db1-9a52-4ed7-b305-061ded6246b3'. See inner errors for details.`"

What should you do to resolve the problem?

A) Choose Runtime stack ASP .NET V4.7.
B) Deploy the application to a new resource group.
C) Deploy the application using the same App Service plan.
D) Choose Runtime stack ASP .NET V3.5.

Explanation

You would deploy the application to a new resource group. Net Core 3.1 (LTS) uses the Linux operating system, but .NET V3.5 needs the Windows operating system. You cannot use both the Windows and Linux operating systems for a web app in the same resource group and region.

You would not deploy the application using the same App Service plan because the App Service Plan can be either Linux or Windows operating system.

You would not choose Runtime stack ASP .NET V4.7 or Runtime stack ASP .NET V3.5. Choosing either one of these stacks does not resolve the problem because those stacks need the Windows operating system, which cannot be deployed in the same resource group.

Objective:
Develop Azure compute solutions

Sub-Objective:
Create Azure App Service Web Apps

References:

Microsoft Azure > App Service > Web Apps > Introduction to Azure App Service on Linux > Limitations

---

Question #84 of 135

Question ID: 1287175

Your application is deployed to Azure and you have data in Azure blob storage. You are concerned about reliability. You have the following conditions:

- Three copies within a single facility
- Three copies in a second facility in a separate region
- Read access to a second facility
- Writes go to the primary facility.

Which replication option for redundancy meets all of the conditions?

A) Geographically redundant storage

B) Locally redundant storage

C) Zone redundant storage

D) Read-access geographically redundant storage

Explanation

You would select read-access geographically redundant storage. With this redundancy type, you get the following:

- Three copies within a single facility
- Three copies in a second facility in a separate region
- Read access to the second facility
- All writes going to the primary facility.

You would not select locally redundant storage because with this you only get three copies within the single facility.

You would not select zone redundant storage. With this redundancy, you only get three copies within multiple facilities in a region.

You would not select geographically redundant storage. Although you get three copies within a single facility and three copies in second facility in a separate region, you are not meeting all of the conditions stated above. You still need read access to a second facility and all writes going to the primary facility.

Objective:
Develop for Azure storage

Sub-Objective:
Develop solutions that use blob storage

References:

Microsoft MSDN Blogs > Windows Azure Storage Redundancy Options and Read Access Geo Redundant Storage

Microsoft Docs > Azure > Storage > Introduction to the core Azure Storage services

James Serra Blog > Redundancy Options in Azure Blob Storage

Question #85 of 135

Question ID: 1287196

You want to create a Node.js console application which will use CDN. You have created a resource group. You have configured Azure Active Directory to provide authentication for the application. You have applied permissions to the resource group so that only authorized users from your Azure AD tenant can interact with the CDN profile. You have created a folder to store your application. The project will be initialized with a packages.json file.

You use ms-rest-azure and azure-arm-cd. In the app.js file, you add the necessary “requires” for your NPM packages. You define the constants.

What is the next step?

A) Instantiate the CDN management client.

B) Create a CDN profile.

C) Assign the Reader role to the application.

D) Create CDN endpoints.

Explanation

You would instantiate the CDN management client. With the code “`var cdnClient = new cdnManagementClient(credentials, subscriptionId);`”, you instantiate the CDN client variable.

Once you have added the "requires" for your NPM packages at the top of the app.js file and you have defined some contants for the method, you would instantiate the CDN management client by supplying credentials similar to the following:

```
var credentials = new msRestAzure.ApplicationTokenCredentials(clientId, tenantId, clientSecret);
var cdnClient = new cdnManagementClient(credentials, subscriptionId);
```

You would not create a CDN profile. You need to instantiate the CDN client before you can create a CDN profile.

You would not create CDN endpoints. You need to create the CDN profile before you can create CDN endpoints.

You would not assign the Reader role to the application. You would assign the CDN Profile Contributor role to the service principal.

Objective:
Monitor, troubleshoot, and optimize Azure solutions

Sub-Objective:
Integrate caching and content delivery within solutions

References:

Microsoft Azure > Networking > CDN > Get started with Azure CDN development:

Question #86 of 135

Question ID: 1287230

You are the administrator of the Nutex Corporation. You want to configure your Azure API Management instance to protect an API by using Oauth 2.0 protocol with Azure AD. You must pre-authorize your requests in API Management by validating the access tokens of each incoming request. If a request does not have a valid token, API Management has to block it.

What must you do?

A) In API Management, select Authorization code as the Authorization grant type.

B) Add an authorization header to the request.

C) Configure a JWT validation policy.

D) Register the client application in Azure AD.

Explanation

You would configure a JWT validation policy. The JWT validation policy pre-authorizes requests in API Management by validating the access tokens of each incoming request. API Management blocks the incoming request if the request does not have a valid token.

You would not register the client application in Azure AD. This solution will not block a request if there is no valid token. You can register an application (backend-app) in Azure AD to represent the API and also the client application, which needs to call the API, but with that, you do not block an invalid token.

You would not add an authorization header to the request because with this step you configure a call to the API from the developer portal.

You would not select Authorization code as the Authorization grant type in API Management because that action enables Oauth 2.0 user authorization in the Developer Console.

Objective:
Connect to and consume Azure services and third-party services

Sub-Objective:
Implement API management

References:

Microsoft Azure > API Management > Protect an API by using OAuth 2.0 with Azure Active Directory and API Management

---

Question #87 of 135

Question ID: 1403563

You are the administrator of the Nutex Corporation. You have enabled diagnostic logging for your Azure web app named **NutexWebApp**. You want to download diagnostic information and save it to the app fie system using FTP. You want to download log information as a ZIP archive using Azure CLI. You only want to download deployment log information.

Where can you find the relevant logs? (Choose all that apply.)

A) /LogFiles/W3SVC#########/
B) /LogFiles/Git
C) /LogFiles/Application/
D) /LogFiles/http/RawLogs
E) /LogFiles/DetailedErrors/
F) D:\home\site\deployments

Explanation

You would use **/LogFiles/Git** and **D:\home\site\deployments** because you can download deployment log information to these locations. The **/LogFiles/Git** and **D:\home\site\deployments** folders contain logs generated for Git deployments and logs generated by internal deployment processes. The easiest way to get the logs stored in the App Service file system is to download them as a ZIP file in the browser.

You would not use **/LogFiles/Application/** because this directory contains one or more text files containing information produced by application logging.

You would not use **/LogFiles/W3SVC#########/**, because in this directory you can find information about failed request traces.

You would not use **/LogFiles/DetailedErrors/** because in this directory you can find one or more .htm files that provides extensive information for any HTTP errors that have occurred.

You would not use **/LogFiles/http/RawLogs** because in this directory you can find the web server logs.

Objective:
Develop Azure compute solutions

Sub-Objective:
Create Azure App Service Web Apps

References:

Microsoft Azure > App Service > Web Apps > Enable diagnostics logging for apps in Azure App Service

Question #88 of 135

Question ID: 1287243

You are the administrator of the Nutex Corporation. You have developed an event-based solution that uses Azure Service Bus. Because of reaching subscription spending limits, the system has suspended entities. You want to reactivate the system-disabled entities.

What is a possible solution for that?

A) Use the ReceiveEnabled field.

B) Restore the system-disabled entity.

C) Use the SendEnabled field.

D) Reactivate the queue as a user.

Explanation

You would restore the system-disabled entities because system-disabled entities cannot be reactivated by the user. However, system-disabled entities are restored when the cause of the suspension has been addressed.

You would not use the ReceiveEnabled or the SendEnabled fields because these fields are not available. There are fields named ReceiveDisabled and SendDisabled, but they are available when the queue has been suspended. The SendDisabled field represents the state of the queue when it is partially suspended, but can still receive. The ReceiveDisabled field represents the state of the queue when it is partially suspended, but can still send.

You would not use Reactivate the queue as a user because system-disabled entities cannot be reactivated by the user.

Objective:
Connect to and consume Azure services and third-party services

Sub-Objective:
Develop message-based solutions

References:

Microsoft Azure > Messaging services > Service Bus Messaging > Suspend and reactivate messaging entities (disable)

Question #89 of 135

Question ID: 1287164

You are the administrator of Nutex. You' have developed a globally distributed application. This application uses one Cosmos DB storage as the storage solution. You have the following requirements:

- Consistency level: Strong
- Cost for read operations compared to other consistency levels
- Calculate request units for item size of 1 KB.

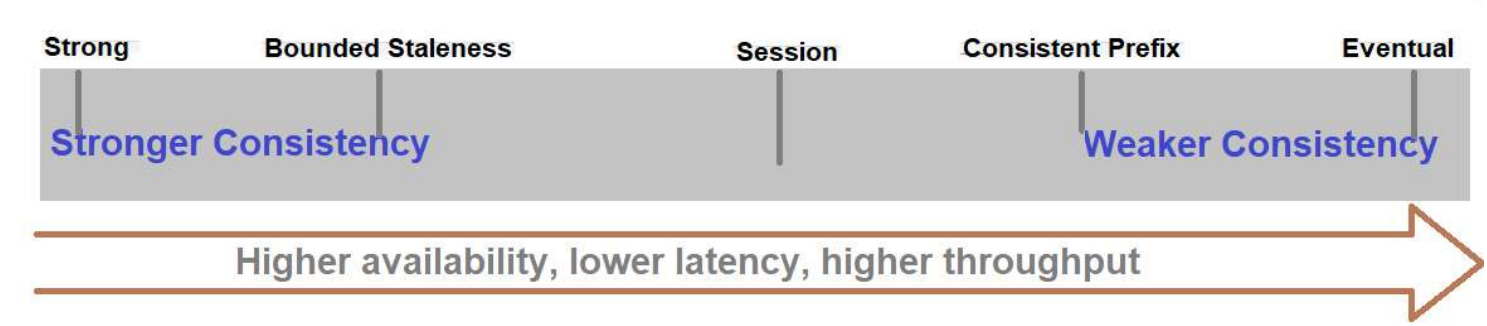
Which statement about the cost for read operations is true?

A) The cost of a read operation (in terms of request units consumed) with strong consistency is higher than session and eventual, but the same as bounded staleness.

B) The cost of a read operation (in terms of request units consumed) with strong consistency is lower than session and eventual, but the same as bounded staleness.

Explanation

The cost of a read operation (in terms of request units consumed) with **strong** consistency is higher than **session** and **eventual**, but is similar to **bounded staleness.**



The cost of a read operation (in terms of request units consumed) with **bounded staleness** is higher than **session** and **eventual** consistency, but is similar to **strong** consistency**.** The cost of a read operation (in terms of request units consumed) with **session** consistency level is less than **strong** and **bounded staleness**, but more than **eventual consistency.**

Objective:
Develop for Azure storage

Sub-Objective:
Develop solutions that use Cosmos DB storage

References:

Microsoft Azure > Cosmos DB > Consistency levels in Azure Cosmos DB

Microsoft Azure > Products > SLA for Azure Cosmos DB

Microsoft Azure > Cosmos DB > Request Units in Azure Cosmos DB

Question #90 of 135

Question ID: 1403571

You are the administrator of the Nutex Corporation. You have created an Azure SQL database. Now you want to query some product data from that database using C# code. You need to fill in the missing parts of the code. Apply the relevant code snippets.

```
using System;
using System.Data.SqlClient;
using System.Text;

namespace sqltest
{
    class Program
    {
        static void Main(string[] args)
        {
            try
            {
                SqlConnectionStringBuilder builder = new
```

A

```
                builder.DataSource = "<your_server.database.windows.net>";
                builder.UserID = "<your_username>";
                builder.Password = "<your_password>";
                builder.InitialCatalog = "<your_database>";
```

```
            using (SqlConnection connection = new
```

B

```
            {
                Console.WriteLine("\nQuery data example:");

Console.WriteLine("==========================================\n");
                connection.Open();
                StringBuilder sb = new StringBuilder();
```

C

```
                String sql = sb.ToString();

                using (SqlCommand command = new SqlCommand(sql, connection))
                {
                    using (
```

D

```
)
                    {
                        while (reader.Read())
                        {
                            Console.WriteLine("{0} {1}", reader.GetString(0), reader.GetString(1));
                        }
                    }
                }
            }
            catch (SqlException e)
            {
                Console.WriteLine(e.ToString());
            }
            Console.WriteLine("\nDone. Press enter.");
            Console.ReadLine();
        }
    }
}
```

Match the missing code to the appropriate letter.

{UCMS id=4724806583844864 type=Activity}

Explanation

You would use `SqlConnectionStringBuilder();` for code fragment A. The `SqlConnectionStringBuilder` class is used to create the connection string and pass the `ConnectionString` property of the `SqlConnectionStringBuilder` instance to the constructor of the connection class.

You would use `SqlConnection(builder.ConnectionString);` for code fragment B. This code passes the connection string to the `SqlConnection` object. The `SqlConnection` object is a unique session to a SQL Server data source.

You would specify the following for code fragment C:

```
sb.Append('SELECT TOP 20 pc.Name as CategoryName, p.name as ProductName ');
sb.Append('FROM [SalesLT].[ProductCategory] pc ');
```

```
sb.Append('JOIN [SalesLT].[Product] p ');
sb.Append('ON pc.productcategoryid = p.productcategoryid;');
```

The above code specifies a query that returns a list of products, which is required by the scenario.

You would specify `SqlDataReader reader = command.ExecuteReader()` for code fragment D. This code sends a Transact-SQL statement, table name, or stored procedure to execute at the data source to the Connection and builds an SqlDataReader.

Objective:
Develop for Azure storage

Sub-Objective:
Develop solutions that use Cosmos DB storage

References:

Microsoft Azure > SQL Database > Quickstart: Use .NET and C# in Visual Studio to connect to and query an Azure SQL database

Microsoft Docs > .NET > SqlConnectionStringBuilder Class

Microsoft Docs > .NET > SqlCommand.CommandText Property

Question #91 of 135

Question ID: 1287194

You are the administrator of the Nutex Corporation. You have created a resource group for your CDN profile, and you have given Azure AD application permission to manage CDN profiles and endpoints within that group. Now you want to create your project. For authentication, you use ADAL to retrieve a token.

Which directive do you NOT need?

A) Microsoft.Rest
B) Microsoft.Azure.Management.Resources
C) Microsoft.Azure.Management.Redis.Fluent
D) Microsoft.Azure.Management.Resources.Models
E) System.Collections.Generic
F) System
G) Microsoft.IdentityModel.Clients.ActiveDirectory
H) Microsoft.Azure.Management.Cdn.Models
I) Microsoft.Azure.Management.Cdn

Explanation

Directives are used by the Cache-Control general header field. Directives specify behavior intended to stop caches from obstructing the request or response. These directives are designed to override the default caching algorithms. You can add directives in the Program.cs tab. You replace the `using` directives at the top of the Program.cs tab with the following:

```
using System;
using System.Collections.Generic;
using Microsoft.Azure.Management.Cdn;
using Microsoft.Azure.Management.Cdn.Models;
using Microsoft.Azure.Management.Resources;
using Microsoft.Azure.Management.Resources.Models;
using Microsoft.IdentityModel.Clients.ActiveDirectory;
using Microsoft.Rest;
```

`Microsoft.Azure.Management.Redis.Fluent` is not a directive which can be used for CDN.

Objective:
Monitor, troubleshoot, and optimize Azure solutions

Sub-Objective:
Integrate caching and content delivery within solutions

References:

Microsoft Azure > Networking > CDN > Get started with Azure CDN development

Cloud Academy > Managing Your Cloud Content Assets Using Azure CDN and .Net Client Library

---

Question #92 of 135

Question ID: 1292131

Lara must edit an Azure Resource Manager template to add a variable for the available storage to be used later in her template.

Which syntax should she use to accomplish this?

A)
```
variables: {  "storageName": "[concat(toLower(parameters('storageNamePrefix')),
uniqueString(resourceGroup().id))]" }
```

B)
```
"variables": [  "storageName": "[concat(toLower(parameters('storageNamePrefix')),
uniqueString(resourceGroup().id))]" ]
```

C)
```
"variables": {  "storageName"= "[concat(toLower(parameters('storageNamePrefix')),
uniqueString(resourceGroup().id))]" }
```

D)
```
"variables": {  "storageName": "[concat(toLower(parameters('storageNamePrefix')),
uniqueString(resourceGroup().id))]" }
```

Explanation

JSON syntax requires Lara to add the following to her Azure RM template:

```
"variables": {  "storageName": "[concat(toLower(parameters('storageNamePrefix')), uniqueString(resourceGroup().id))]" }
```

The other options are incorrect because they have syntax choices that will cause them problems.

```
variables: {  "storageName": "[concat(toLower(parameters('storageNamePrefix')), uniqueString(resourceGroup().id))]" }
```

Each element of the Azure RM Template must be in quotes, for example, `"variables"`.

```
"variables": [  "storageName": "[concat(toLower(parameters('storageNamePrefix')), uniqueString(resourceGroup().id))]" ]
```

This option incorrectly uses the square brackets ([]) instead of the French brackets ({}).

```
"variables": {  "storageName"= "[concat(toLower(parameters('storageNamePrefix')), uniqueString(resourceGroup().id))]" }
```

In this example, the application of value was introduced using the equals (=) instead of the colon (:), making it syntactically incorrect.

Objective:
Develop Azure compute solutions

Sub-Objective:
Implement IaaS solutions

References:

Microsoft Azure > Resource Manager > Quickstart: Create and deploy ARM templates by using the Azure portal

Microsoft Azure > Resource Manager > Understand the structure and syntax of ARM templates

Microsoft Azure > Resource Manager > Variables in Azure Resource Manager template

Question #93 of 135

Question ID: 1287115

You have been using the Dev-NutexSalesApp-VM in Azure DevTest Labs. After completing your assigned development tasks, what must you do to make the VM available to another developer who is responsible for the next part of the solution?

A) Generate artifacts containing your changes and provide them to the developer.

B) Generate a VM formula from Dev-NutexSalesApp-VM and let the developer use it.

C) Save the VM as an image and provide it to the developer to create a new VM.

D) Unclaim the VM and allow the developer to claim it and take over.

Explanation

You would unclaim the VM and allow the developer to claim it and take over. Unclaiming the VM frees it up so that the developer can see it in the claimable VMs list, claim it, and continue with the next part of the solution.

You would not save the VM as an image and provide it to the developer to create a new VM. There is no need to save another image and spawn another VM from it. This action adds cost and unnecessary resource usage.

You would not generate artifacts containing your changes and provide them to the developer. Artifacts are a way to load specific sets of tools, perform actions, or install applications onto a fresh VM. This course of action is a little overkill for just transferring your work to the developer to take over.

You would not generate a VM Formula from Dev-NutexSalesApp-VM and let the developer use it. A formula is a set of properties to be used when provisioning a new VM and is intended to be reusable. This will not just transfer your work over to the developer and should be avoided.

Objective:
Develop Azure compute solutions

Sub-Objective:
Implement IaaS solutions

References:

Microsoft Azure > Lab Services > DevTest Labs concepts

Microsoft Azure > Lab Services > Create and manage claimable VMs in Azure DevTest Labs

Question #94 of 135

Question ID: 1287232

You are the administrator of the Nutex Corporation. You must configure policies for your API's using API Management service and API gateways.

Which of the following policies are NOT access restriction policies? (Choose all that apply.)

A) Set usage quota by key

B) Check HTTP header

C) Restrict caller IPs

D) Authentication-certificate policy

E) Cross-domain policy

F) Limit call rate by subscription

G) Authentication-basic policy

Explanation

You would use an Authentication-basic policy because this kind of policy is an API Management authentication policy and not an access restriction policy. With this policy, you authenticate with a backend service using Basic authentication.

You would use an Authentication-certificate policy because this kind of policy is an API Management authentication policy and not an access restriction policy. With this policy, you authenticate with a backend service using a client certificate.

You would use a cross-domain policy. With this kind of policy, you make the API accessible from Adobe Flash and Microsoft Silverlight browser-based clients.

You would not use a check-header policy because this is an access restriction policy. You can use the check-header policy to enforce a request that has a specified HTTP header. You can optionally check to see if the header has a specific value or check for a range of allowed values. If the check fails, the policy terminates request processing and returns the HTTP status code and error message specified by the policy.

You would not use a limit call rate by subscription policy because this is an access restriction policy. The rate-limit policy prevents API usage spikes on a per subscription basis by limiting the call rate to a specified number in a specified time period. When this policy is triggered, the caller receives a 429 Too Many Requests response status code.

You would not use a restrict caller IPs policy because this is an access restriction policy. The IP-filter policy filters (allows/denies) calls from specific IP addresses or address ranges.

You would not use a set usage quota-by-key policy because the quota-by-key policy enforces a renewable or lifetime call volume and/or bandwidth quota on a per key basis. The key can have an arbitrary string value and is typically provided using a policy expression. Optional increment conditions can be added to specify which requests should be counted towards the quota. If multiple policies would increment the same key value, it is incremented only once per request. When the call limit is reached, the caller receives a 403 Forbidden response status code.

Objective:
Connect to and consume Azure services and third-party services

Sub-Objective:
Implement API management

References:

Microsoft Azure > API Management > API Management access restriction policies

Microsoft Azure > API Management > API Management authentication policies

Microsoft Azure > API Management > API Management cross domain policies

---

Question #95 of 135

Question ID: 1287170

You are the administrator of the Nutex Corporation. You try to acquire a lease on a blob at the same time you create it. You use the following code to acquire the lease:

```
lease = blockBlob.AcquireLease(_leaseTimeOut, null);
blockBlob.UploadFromByteArrayAsync(contentBytes, 0, contentBytes.Length).Wait();
```

You get a 404 error.

What is NOT a possible solution for that error?

A) Create the blob. Write at least a single character. Acquire the lease.
B) Exclude access to the blob until you have leased it.
C) Use an SAS to write to the blob.
D) Wait one minute and try again.

Explanation

Waiting one minute and trying again will not solve the problem. There is no way to lease a blob at the same time that you create it. After one minute, the blob does not exist, and thus the lease cannot be acquired.

The other options could be possible reasons for the 404 error.

If you exclude access to the blob until you have leased it then you can solve the error. You can exclude access to the blob by ensuring that the container is private until you have leased the blob (assuming other clients are not using the account key for access).

If you create the blob, write at least a single character, and acquire the lease, it will work. After you are able to write to the blob, you can acquire the lease.

You can use an SAS to write to the blob. You could write your application so that users must have an SAS in order to write to the blob. This will ensure that the SAS grants access to the blob only when and if the blob is available for other clients to write to.

Objective:
Develop for Azure storage

Sub-Objective:
Develop solutions that use blob storage

References:

StackOverflow > Trying to acquire a lease on a new blockblob gets me a 404

Microsoft Docs > Azure > Storage > Managing Concurrency in Microsoft Azure Storage

---

Question #96 of 135

Question ID: 1287157

You are the administrator of the Nutex Corporation. You use Azure Cosmos DB storage for your application data. You need to define the consistency level.

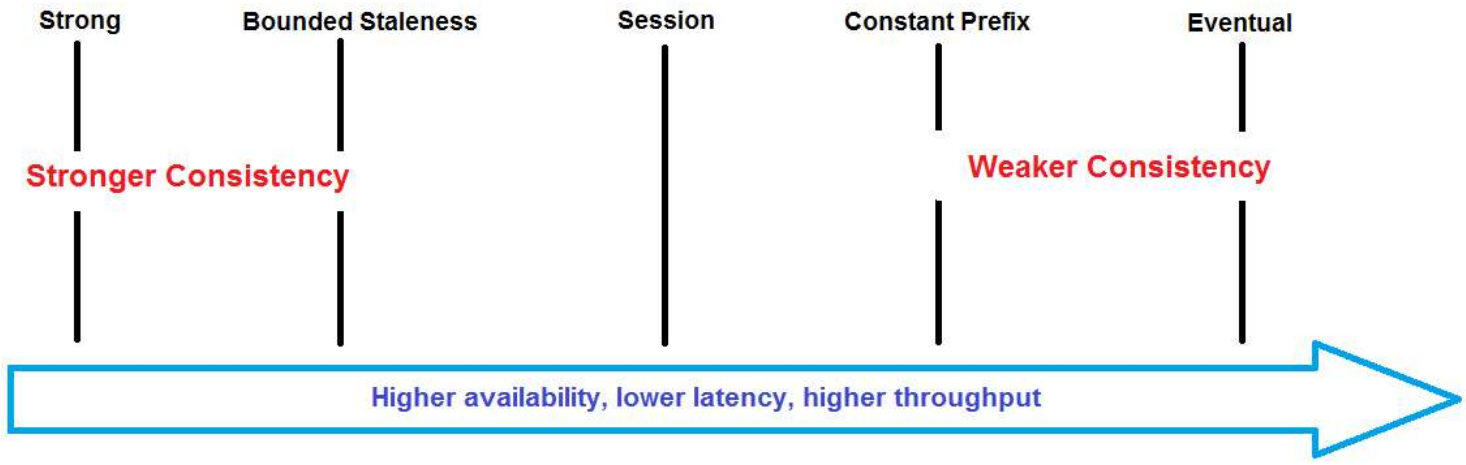
Which explanation describes the relevant consistency level?

Apply the relevant explanation to the appropriate consistency level.

{UCMS id=5107901996728320 type=Activity}

Explanation

There are five well-defined consistency models on the consistency spectrum:



Strong offers a guarantee of serving requests concurrently. Reads guarantee the most recent committed version of an item. Users are always guaranteed the latest committed write, and a client never sees a partial or uncommitted write.

Bounded Staleness guarantees that reads never see out of order writes, which means reads are guaranteed to honor the consistent-prefix guarantee, but reads might lag behind writes at most versions of an item (updates) or by time interval. Staleness can be configured by the number of versions (K) of the item or the time interval (T) by which the reads might lag behind the writes.

Session ensures reads are guaranteed to honor the consistent-prefix within a single client session. Single client session reads are guaranteed to honor the consistent-prefix, monotonic reads, monotonic writes, read-your-writes, and write-follows-reads guarantees. Eventual consistency will be seen by clients

outside of the session performing writes.

Consistent prefix ensures reads never see out-of-order writes. There is some prefix for updates that are returned, but there are no gaps.

Eventual allows for no ordering guarantee for reads. The replicas eventually converge if there are no further writes.

Objective:
Develop for Azure storage

Sub-Objective:
Develop solutions that use Cosmos DB storage

References:

Microsoft Azure > Cosmos DB > Consistency levels in Azure Cosmos DB

Question #97 of 135

Question ID: 1403557

You have a Kubernetes cluster in AKS and you deployed an app called **MyApp**. You run the following command to list all pods in a namespace:

```
kubectl get pods
```

The output of the command is as follows:

NAME	READY	STATUS	RESTARTS	AGE
myapp-back-2549686872-4d2r5	1/1	Running	0	31m
myapp-front-848767080-tf34m	1/1	Running	0	31m

You need to change the number of pods in the myapp-front deployment to 5. You type the following command:

[ ] `--replicas=5 deployment/azure-vote-front`

In the space above, type the command.

Explanation

Acceptable answer(s) for field 1:

- kubectl scale

You would type the **kubectl scale** command to scale the resources. You can use the `--replicas` parameter to set the number of pods.

Objective:
Develop Azure compute solutions

Sub-Objective:
Implement IaaS solutions

References:

Microsoft Azure > AKS > Tutorial: Scale applications in Azure Kubernetes Service (AKS)

Kubernetes > kubectl Cheat Sheet

Question #98 of 135

Question ID: 1403574

You are the administrator of the Nutex Corporation. You want to use AzCopy to copy blobs between two Azure storage accounts. Your network bandwidth in your company is poor. You want to increase the throughput when transferring small files.

Which task or command should you use on your Windows 10 client?

A) Use the `cap-mbps` flag.

B) Increase network bandwidth.

C) Run `export AZCOPY_CONCURRENCY_VALUE`.

D) Run `set AZCOPY_CONCURRENCY_VALUE`.

Explanation

You would set the `AZCOPY_CONCURRENCY_VALUE` environment variable with the `set AZCOPY_CONCURRENCY_VALUE` command. This environment variable can increase the throughput when transferring small files and specifies the number of concurrent requests that can occur. The default value for this environment variable is equal to 16 multiplied by the number of CPUs. If your device has less than 5 CPUs then the value of this environment variable is set to 32.

You would not run the `export AZCOPY_CONCURRENCY_VALUE` command. This command sets the value on a Linux or MacOS device. In this scenario, you are using a Windows 10 client, not a Linux or MacOS device.

You would not increase network bandwidth. Although this may be helpful, it could be expensive, and you should try setting the `AZCOPY_CONCURRENCY_VALUE` environment variable first. AzCopy uses server-to-server APIs, so data is copied directly between storage servers. These copy operations do not use the network bandwidth of your computer.

You would not use the `cap-mbps` flag. This flag places a ceiling on the throughput data rate, which would restrict the bandwidth.

Objective:
Develop for Azure storage

Sub-Objective:
Develop solutions that use blob storage

References:

Microsoft Docs > Azure > Storage > Configure, optimize and troubleshoot AzCopy: HYPERLINK "https://docs.microsoft.com/en-us/azure/storage/common/storage-use-azcopy-configure" \\l "optimize-throughput"

Microsoft Docs > Azure > Storage > Transfer data with AzCopy and Blob storage

---

Question #99 of 135

Question ID: 1287127

You are the administrator of Nutex. You want to run containers in Azure. You have to decide between the following Azure services:

- Azure Container Instance
- Azure Kubernetes Service.

Apply the following service benefits from the left to the relevant service on the right. (Use each option only once.)

{UCMS id=5741632474316800 type=Activity}

Explanation

Azure Container Instances (ACI) is the service that allows you deploy a container on Azure cloud without having to manage the underlying infrastructure. ACI allows you launch containers quickly. With ACI, you incur costs only when running the container. The billing is on a per-second instead of a per-minute billing. You can isolate an application in a container like a VM environment. You can specify custom sizes for an Azure Container by specifying exact values for CPU cores and memory. With ACI, you can mount Azure files for persistent storage. The shared files are part of the container and are in a persistant state. You can have scheduled Linux containers as well as Windows containers with the same API.

The Azure Kubernetes Service (AKS) manages a Kubernetes environment in Azure. AKS provides full container orchestration because you deploy and manage containerized applications without container orchestration expertise. AKS is scalable to meet growing demands by designs because it includes built-in application autoscaling.

Microsoft recommends AKS instead of ACI when you need service discovery across multiple containers, coordinated application upgrades, and automatic scaling.

Objective:
Develop Azure compute solutions

Sub-Objective:
Implement IaaS solutions

References:

Microsoft Docs > Learn > Exercise - Run Azure Container Instances:

Medium > The best choice between ACI or AKS or Web App for containers:

Question #100 of 135

Question ID: 1287177

You work as an Azure architect for your company and are involved in a code review for a corporate system implemented around the globe. The system is installed on medical equipment that is looking for new vaccines and automatically interacts with blob storage by sending and receiving sensitive DNA data to multiple branches. Every branch that has the medical equipment is uploading and downloading data. Currently, five thousand such devices are operating worldwide. Your company does not want to change the infrastructure. Permission for downloaded data depends on the location and is often changed. The audited code is as follows:

```
public async Task ConnectionStringAsync()
    {
        string connectionString = ConnectionString;
        BlobServiceClient service = new BlobServiceClient(connectionString);
        await service.GetPropertiesAsync();
    }
```

What changes should you implement in the code to support authentication?

A) Use Active Directory Federation Services to authenticate.

B) Use SAS tokens.

C) Use Azure AD-managed identities.

D) Use Azure AD OAuth2 Implicit grant flow to authenticate.

E) Use a third party solution such as KeyCloak or Ping.ID.

F) Use a token credential that can use an Azure Active Directory application to authenticate.

G) Use Key Vault to store credentials in the storage account.

Explanation

You would use a token credential that can use an Azure Active Directory application to authenticate. Azure Storage provides integration with Azure Active Directory for identity-based authentication of requests to the Blob. With Azure AD, you can use role-based access control (RBAC) to grant access to your Azure Storage resources.

You would not use SAS tokens because, in this scenario, permission for downloaded data depends on the location and is often changed. SAS tokens cannot provide RBAC.

You would not use the Azure AD Oauth2 Implicit grant flow. A suitable scenario for the OAuth2 Implicit grant flow is to enable user-agent applications, such as JavaScript applications executing within a browser. Azure AD Oauth2 Implicit grant flow will not integrate with Azure Active Directory for identity-based authentication of requests to a Blob.

Using Active Directory Federation Services (ADFS) is not a complete solution and needs more changes. You would need to implement ADFS as two additional virtual machines and integrate it with Active Directory. The question asks what changes you should implement in the code, not to build a new infrastructure.

Using a third-party solution such as KeyCloak or Ping.ID is not a complete solution. It is not the best answer because you need to implement KeyCloak or PingID on additional virtual machines and integrate it with Azure Active Directory. The question asks what changes you should implement in the code, not to build a new infrastructure.

You would not use Azure AD-managed identities. Azure AD-managed identities only work on a workload running on Azure AD. A managed identity works only when both parties are in Azure. It could work if the medical equipment will be running on Azure, but in this scenario it is a physical device that is not running on Azure but just sending data to Azure.

You would not use Key Vault to store credentials in a storage account. A Key Vault can store secrets and certificates but cannot provide RBAC.

Objective:
Develop for Azure storage

Sub-Objective:
Develop solutions that use blob storage

References:

GitHub > Azure > azure-sdk-for-net

Question #101 of 135

Question ID: 1287214

You are working as a developer for the Nutex Corporation. You are responsible for an online e-store system using PHP 7.4. You are preparing for the Black Friday and Cyber Monday period. Your CEO is afraid that during these periods, MySQL DB will be overloaded and will not respond fast enough.

Which cloud design pattern do you propose to mitigate MySQL potential problems?

A) Implement Competing Consumers pattern.
B) Implement Retry pattern.
C) Implement Cache-Aside pattern.
D) Implement Sharding pattern.

Explanation

You would implement the Cache-Aside pattern. The Cache-Aside pattern is used to improve performance when loading data. This pattern is for storing data in memory to speed up MySQL queries. It also keeps consistency between data in the underlying data store and data held in the cache.

You would not implement the Competing Consumers pattern. This type of pattern is used for queue implementation and can be a part of a solution, but it does not resolve database problems.

You would not implement the Retry pattern. The Retry pattern improves the stability of an application by allowing an application to retry a failed operation when intermittent failures of connecting to a network resource or a service occur. However, this pattern will not resolve database problems, although it could resolve connection problems.

You would not implement the Sharding pattern. This pattern is used for splitting data across databases, disks, files, or partitions. This pattern can resolve database issues for SQL and NoSQL, but not MySQL.

Objective:
Monitor, troubleshoot, and optimize Azure solutions

Sub-Objective:
Instrument solutions to support monitoring and logging

References:

Microsoft Azure > Architecture > Cloud Design Patterns > Cache-Aside pattern

---

Question #102 of 135

Question ID: 1403555

You create a manifest file to create all objects needed to run your application. The manifest includes a Kubernetes deployment for the application and another Kubernetes deployment for the Redis instance. You create a file named **MyApp.yaml** that has the following code:

```
apiVersion: apps/v1beta1
kind: Deployment
metadata:
  name: MyApp
spec:
  replicas: 1
  template:
    metadata:
      labels:
        app: MyApp
    spec:
      containers:
      - name: MyApp
        image: redis
        ports:
        - containerPort: 6379
          name: redis
---
apiVersion: v1
kind: Service
metadata:
  name: MyApp
spec:
  ports:
  -  port: 6379
  selector:
    app: MyApp
---
apiVersion: apps/v1beta1
kind: Deployment
metadata:
  name: MyApp-front
spec:
  replicas: 1
  template:
    metadata:
      labels:
        app: MyApp-front
    spec:
      containers:
      - name: MyApp-front
        image: microsoft/MyApp-front:v1
        ports:
        - containerPort: 80
        env:
        - name: REDIS
          value: "MyApp-back"
---
apiVersion: v1
```

```
kind: Service
metadata:
  name: MyApp-front
spec:
  type: LoadBalancer
  ports:
  - port: 80
  selector:
    app: MyApp-front
```

You type the following command to run the application:

[ ] **-f MyApp.yaml**

In the space provided above, type the missing part of the command.

Explanation

Acceptable answer(s) for field 1:

- kubectly apply

You would use **kubectly apply** to run the application. This command is used to apply a configuration to a resource by specifying the file name. You can use either JSON or YAML formats.

Objective:
Develop Azure compute solutions

Sub-Objective:
Implement IaaS solutions

References:

Microsoft Azure > AKS > Quickstart: Deploy an Azure Kubernetes Service cluster using the Azure CLI

Question #103 of 135

Question ID: 1292141

You are the administrator of the Nutex Corporation. You have established an API Gateway through the use of API management services. You want to secure access to your API's using client certificates. You do not want to check the certificate against the CRL. You also want to protect against client certificate deadlocks.

Which steps do you NOT have to perform? (Choose all that apply.)

A) On the endpoint, enable **Negotiate client certificate**.

B) Turn on Request client certificate on the **Custom domains** blade.

C) Create a policy to check the issuer and subject of a client certificate.

D) Use `context.Request.Certificate.Verify()` in the policy.

E) Disable the default SSL binding on the endpoint.

Explanation

You do not have to disable the default SSL binding on the endpoint of the API gateway. If you disable it, the certificate is not bound to an SSL port and cannot be used.

You do not have to use `context.Request.Certificate.Verify()` in the policy to verify the certificate. You should use `context.Request.Certificate.VerifyNoRevocation()` to disable verifying the certificate in the CRL.

You would select Turn on Request client certificate on the **Custom domains** blade because you need to set this setting to YES to receive and verify client certificates in the Consumption tier.

You would create a policy to check the issuer and subject of a client certificate because you have to create a policy to check the issuer and subject of a client certificate.

You would enable **Negotiate client certificate** on the endpoint because, with that setting, you can prevent a client certificate deadlock issue.

Objective:
Connect to and consume Azure services and third-party services

Sub-Objective:
Implement API management

References:

Microsoft Azure > Architecture > Using API gateways in microservices

Microsoft Azure > API Management policy samples

Microsoft Azure > API Management > How to secure APIs using client certificate authentication in API Management

---

Question #104 of 135

Question ID: 1287192

You work as an Azure architect for your company and are involved in an application review for a corporate system implemented around the globe, which encompasses multiple regions in Azure. The system is installed on VMs and uses Azure AD-managed identities. The system is looking for new vaccines and automatically interacts with an Amazon Aurora database on AWS. Security is the primary goal, and all secrets must be rotated every four days. You do not want to make changes to infrastructure.

What solution should you propose to store secrets?

A) Use a token credential that can use an Azure Active Directory application to authenticate.
B) Use Azure AD-managed identities.
C) Use SAS tokens.
D) Use a third party solution such as KeyCloak or Ping.ID.
E) Use Active Directory Federation Services to authenticate.
F) Use Key Vault to store credentials in the storage account.
G) Use Azure AD OAuth2 Implicit grant flow to authenticate.

Explanation

You would use Key Vault to store credentials in the Amazon Aurora database. Securing the credentials is an important task. Azure Key Vault securely stores credentials, and your code has to authenticate to Key Vault to retrieve them.

You would not use a managed identity for Azure. You can use the **identity** to authenticate to any service that supports **Azure** AD authentication. Aurora is not an Azure resource but is part of the AWS cloud.

You would not use SAS tokens. SAS tokens work with resources in the Azure cloud, but not with resources in the AWS cloud such as Aurora.

You would not use the Azure AD Oauth2 Implicit grant flow. A suitable scenario for the OAuth2 Implicit grant flow is to enable user-agent applications, such as JavaScript applications executing within a browser. Azure AD Oauth2 Implicit grant flow will not integrate with resources in the AWS cloud such as Aurora.

Using Active Directory Federation Services (ADFS) is not a complete solution and needs more changes. You need to implement ADFS as two additional virtual machines, and integrate it with Active Directory. The question asks what changes you should implement in the code, not to build new infrastructure.

Using a third-party solution such as KeyCloak or Ping.ID is not a complete solution. It is not the best answer because you need to implement KeyCloak or PingID on additional virtual machines and integrate it with Azure Active Directory. The question asks what changes you should implement in the code, not to build new infrastructure.

You would not use a token credential that can use an Azure Active Directory application to authenticate. This solution still needs to store the secret in the code, in a variable, or in a config file.

Objective:
Implement Azure security

Sub-Objective:
Implement secure cloud solutions

References:

Microsoft Docs > Azure > Active Directory > What are managed identities for Azure resources?

Question #105 of 135

Question ID: 1287141

You are the administrator of the Nutex Corporation. You create some Azure functions, triggers, and bindings. You must resolve to values from various sources. You use Azure functions version 2.x runtime bindings.

Which kind of bindings should you NOT have to register? (Choose all that apply.)

A) HTTP
B) Twilio
C) IoT Hub
D) Table storage
E) Queue storage
F) Timer

Explanation

You do not have to register HTTP and timer bindings as they are supported by default and do not require a binding extension.

All other bindings, including table storage, blob storage, Cosmos DB, queue storage, Twilio, Microsoft Graph, SendGrid, and IoT Hub require a binding extention in Azure functions version 2.x. With Azure functions version 2.x, all bindings except HTTP and Timer must be registered.

Objective:
Develop Azure compute solutions

Sub-Objective:
Implement Azure functions

References:

Microsoft Azure > Functions > Register Azure Functions binding extensions:

Microsoft Azure > Functions > Azure Functions triggers and binding concepts

Microsoft Azure > Functions > Azure Functions binding expression patterns:

Question #106 of 135

Question ID: 1287203

You are working as an internal system developer that is creating an HR system for the Nutex Corporation, which uses a hybrid configuration of Office 365 and an on-premises Exchange email subsystem. The application uses PHP on your Apache/Ubuntu 18.04 LTS, but for legal purposes the system must be deployed in the on-premises server. Security is the main goal, so users must use MFA authentication.

What is the best method to provide secure authentication for the HR system?

A) Use Key Vault to store credentials in the storage account.

B) Use Active Directory Federation Services to authenticate.

C) Use SAS tokens.

D) Use OpenID/OAuth against Azure Active Directory.

Explanation

You would use OpenID/OAuth against Azure Active Directory. OpenID Connect is a simple identity layer built on top of the OAuth 2.0 protocol, and it allows developers to build applications that sign in using all Microsoft identities.

You would not use SAS tokens because they can be used to share access to blobs. It does not use MFA.

Using Active Directory Federation Services (ADFS) is not a complete solution. You would need to implement ADFS with at least two additional virtual machines and integrate it with Active Directory. Moreover, providing MFA can be a further process, not a standard procedure.

Using Key Vault to store credentials is incorrect because it can be used to store secrets but not for authentication and authorization.

Objective:
Monitor, troubleshoot, and optimize Azure solutions

Sub-Objective:
Integrate caching and content delivery within solutions

References:

Microsoft Docs > Azure > Active Directory > Azure AD for Developers > Authorize access to web applications using OpenID Connect and Azure Active Directory

Microsoft Docs > Azure > Active Directory > Develop > Microsoft identity platform and OAuth 2.0 authorization code flow

---

Question #107 of 135

Question ID: 1403576

You are the administrator of the Nutex Corporation. You want to retrieve Azure blob storage container property metadata. Which C# code content can you apply to the missing section? (Choose all that apply.)

```
public static async Task ReadContainerMetadataAsync(CloudBlobContainer container)
{
    try
    {
        // Fetch container attributes in order to populate the container's properties and metadata.

        await container. MISSING ();

        // Enumerate the container's metadata.
        Console.WriteLine("Container metadata:");
        foreach (var metadataItem in container.Metadata)
        {
            Console.WriteLine("\tKey: {0}", metadataItem.Key);
            Console.WriteLine("\tValue: {0}", metadataItem.Value);
        }
    }
```

```
    catch (StorageException e)
    {
        Console.WriteLine("
HTTP error code {0}: {1}",
                           e.RequestInformation.
httpStatusCode,
                           e.RequestInformation.ErrorCode);
        Console.WriteLine(e.Message);
        Console.ReadLine();
    }
}
```

A) `GetAttributesAsync`

B) `FetchPropertiesAsync`

C) `FetchAttributesAsync`

D) `FetchAttributes`

Explanation

You would use the `FetchAttributesAsync` or `FetchAttributes` method. Either one of these methods fetch or retrieve a container's properties.

You would not use the `FetchPropertiesAsync` method. This method is used in previous versions of Azure and could be used to populate a blob's properties or metadata.

There is no `GetAttributesAsync` method in Azure for .NET. This method can work with Amazon's AWS and retrieves the attributes for the queue identified by the queue URL asynchronously. It is used with the **AWSSDK.Core.dll** assembly.

Objective:
Develop for Azure storage

Sub-Objective:
Develop solutions that use blob storage

References:

:

Microsoft Docs > Azure > Storage > Manage container properties and metadata with .NET

Microsoft Azure > .NET > API Reference > CloudBlobContainer.FetchAttributesAsync Method

Microsoft Azure > .NET > API Reference > CloudBlobContainer.FetchAttributes(AccessCondition, BlobRequestOptions, OperationContext) Method

---

Question #108 of 135

Question ID: 1403566

You are an administrator for the Nutex Corporation. You want to use an Azure function to trigger an issue-based event-driven GitHub webhook. You have created the function app based on C# GitHub Webhook template.

You must configure the GitHub webhook trigger. Place all of the following tasks in the correct order:

{UCMS id=5749647504048128 type=Activity}

Explanation

You would perform the following steps:

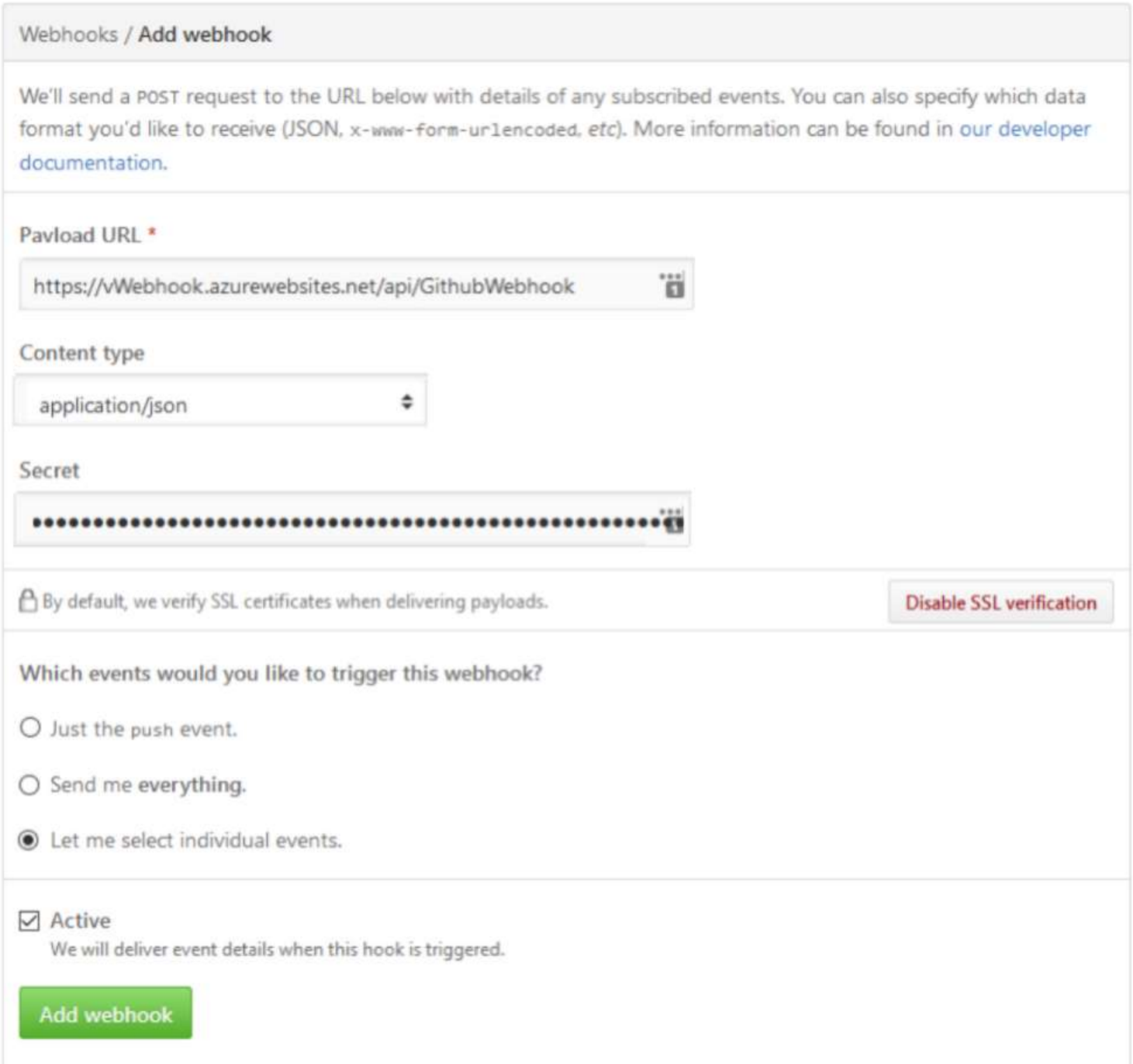
1. Select the function URL.
2. Select the GitHub secret.

3. Add the webhook to the repository.
4. Select “issues”.

First, you would select the function URL. An HTTP request must be sent to a URL that is a combination of the function app URL and the function name to trigger a function.

Second, you must select the GitHub secret. You must have an API key included with an HTTP request to trigger a webHook function or HTTP function. The API key values are stored in the **D:\home\data\Functions\secrets** folder in the file system of the function app.

Third, you must add the webhook to the repository and configure which events are triggered by the webhook.



Lastly, you should select “Issues” to fire the trigger if open, edit, close, reopen, assign, unassign, labeled, unlabeled, milestoned, or demilestoned issues occur in the GitHub repository.

Click the **Add webhook** button to complete the task.

Objective:
Develop Azure compute solutions

Sub-Objective:
Implement Azure functions

References:

Visual Studio Magazine > Serverless C# with Azure Functions: Implementing Webhooks

GitHub > Azure Functions > HTTP and webhook bindings

GitHub Docs > Developers > Webhooks and events > Webhooks > Creating webhooks

---

Question #109 of 135

Question ID: 1287113

You are the administrator of the Nutex Corporation. You want to create and deploy a container image to the Azure Kubernetes service. You want to use Azure Pipelines for that.

Which service does Azure Pipelines use to build and push docker images to your container registry using a Docker registry service connection?

A) Kubernetes manifest task
B) Docker swarm clusters on Azure
C) Docker task
D) Azure Image Builder

Explanation

You would use Docker task to build or release a pipeline to build and push Docker images to any container registry using the Docker registry service connection. You can easily integrate with a Docker registry service connection and you can add metadata to the image.

You would not use a Kubernetes manifest task, because you would use this type of task in a build or release pipeline to bake and deploy manifests to Kubernetes clusters. The key benefits of using this task are: artifact substitution, manifest stability, traceability annotations, secret handling, and bake manifests. You would not use this type of task to build and push Docker images to your container registry using a Docker registry service connection.

You would not use Azure Image Builder because with this service you can create custom images based on Windows and Linux virtual machines.

You would not use Docker swarm clusters on Azure because with this service you cannot build and push Docker images to your container registry using Docker registry service connection. Instead you use Docker swarm clusters to create a collection/cluster of virtual machines (VMs) running the Docker engine, which includes other resources such as Load Balancers, VM Scale Sets or Availability Sets, Storage, and Network. A Docker Swarm on Azure Container Service is made up of the Swarm Master and the Swarm Agent nodes (VMs). A Swarm Master may be directly connected for using an SSH RSA key. A Swarm Agent is not directly connectable by using a SSH RSA key.

Objective:
Develop Azure compute solutions

Sub-Objective:
Implement IaaS solutions

References:

Microsoft Docs > Azure DevOps > Azure Pipelines > Build and deploy to Azure Kubernetes Service

Microsoft Docs > Azure DevOps > Azure Pipelines > Docker task

Microsoft Azure > Virtual Machines > Preview: Azure Image Builder overview

Microsoft Azure > Container Service > Azure Container Service with DC/OS and Swarm Documentation

---

Question #110 of 135

Question ID: 1287239

You are the administrator of the Nutex Corporation. You develop an event-based solution that will use Azure Event Hub. You want to automatically deliver the streaming data in Event Hub to Azure Data Lake Store.

Which Azure event hub features can you use for that? (Choose all that apply.)

A) Idempotent producer
B) Event Hub Capture
C) Kafka streams
D) Dedicated event hub cluster

Explanation

You would use Event Hub Capture because Azure Event Hubs enable you to automatically capture the streaming data in Event Hubs in Azure Blob storage or Azure Data Lake Storage account.

You would use the dedicated event hub cluster because, with the Dedicated offering, you also get the Event Hubs Capture feature for free, which allows you to batch and log data streams to Azure Blob Storage or Azure Data Lake Storage Gen 1.

You would not use Idempotent producer because this is an Apache Kafka feature. The Idempotent producer feature ensures that messages always get delivered, in the right order, and without duplicates.

You would not use Kafka streams, because Kafka Streams is a client library for building applications and microservices, where the input and output data are stored in Kafka clusters.

Objective:
Connect to and consume Azure services and third-party services

Sub-Objective:
Develop event-based solutions

References:

Microsoft Azure > Messaging services > Event Hubs > Enable capturing of events streaming through Azure Event Hubs:

Cloudkarafka > Apache Kafka Idempotent Producer - Avoiding message duplication

Apache Kafka > Kafka Streams

Question #111 of 135

Question ID: 1287144

You are the administrator of the Nutex Corporation. You have to develop functions for your serverless applications. You want to simplify your development process with Azure durable functions.

Which application patterns can benefit from durable functions? (Choose all that apply.)

A) Fan-out/fan-in
B) Function chaining
C) Monitoring
D) Cache-aside
E) Federated Identity
F) Aggregator
G) Sharding
H) Gatekeeper

I) Valet Key

Explanation

The following application patterns can benefit from durable functions:

- Function chaining
- Monitoring
- Fan-out/fan-in
- Aggregator.

With the function chaining pattern, you can use the context parameter DurableOrchestrationContext and the context.df object to invoke other functions by name, pass parameters, and return function output. A sequence of functions executes in a specific order. In this pattern, the output of one function is applied to the input of another function. You can implement control flow by using normal imperative coding constructs. Code executes from the top down. The code can involve existing language control flow semantics, such as conditionals and loops. You can include error handling logic in try/catch/finally blocks.

With the monitoring pattern, you can use durable functions to create flexible recurrence intervals, manage task lifetimes, and create multiple monitor processes from a single orchestration. In a few lines of code, you can use durable functions to create multiple monitors that observe arbitrary endpoints. The monitors can end execution when a condition is met, or another function can use the durable orchestration client to terminate the monitors. You can change a monitor's wait interval based on a specific condition (for example, exponential backoff).

With the fan-out/fan-in pattern, multiple functions can execute in parallel. You can use the function to send multiple messages to a queue. This is referred to as fan out. In the fan in part, you can write code to track when the queue-triggered functions end and the function outputs are stored. With the durable functions extension, you can handle the fan-out/fan-in pattern with relatively simple code.

With the aggregator pattern, the data being aggregated could be received from multiple sources, sent in batches, or may be scattered over long periods of time. Sometimes the aggregator needs to take action on data when it is received, and clients need to query the aggregated data. Durable functions can use a single function to have multiple threads modifying the same data at the same time and ensure that the aggregator only runs on a single VM at a time.

The Federated Identity, Gatekeeper, Valet Key, Sharding, and Cache-aside patterns cannot benefit from durable functions.

Objective:
Develop Azure compute solutions

Sub-Objective:
Implement Azure functions

References:

Microsoft Azure > Functions > What are Durable Functions?

Microsoft Azure > Cloud Design Patterns > Federated Identity pattern

---

Question #112 of 135

Question ID: 1292134

You are the Azure administrator of the Nutex Corporation. You are designing a plan for testing an Azure Web application service. The service runs in the development fabric but fails on Azure. You need to recommend an approach for identifying errors that occur when the service runs on Azure. You have to select an easy way with the least administrative effort.

Which two tasks should you recommend?

A) Use Azure website log browser to analyze the Azure web app logs.

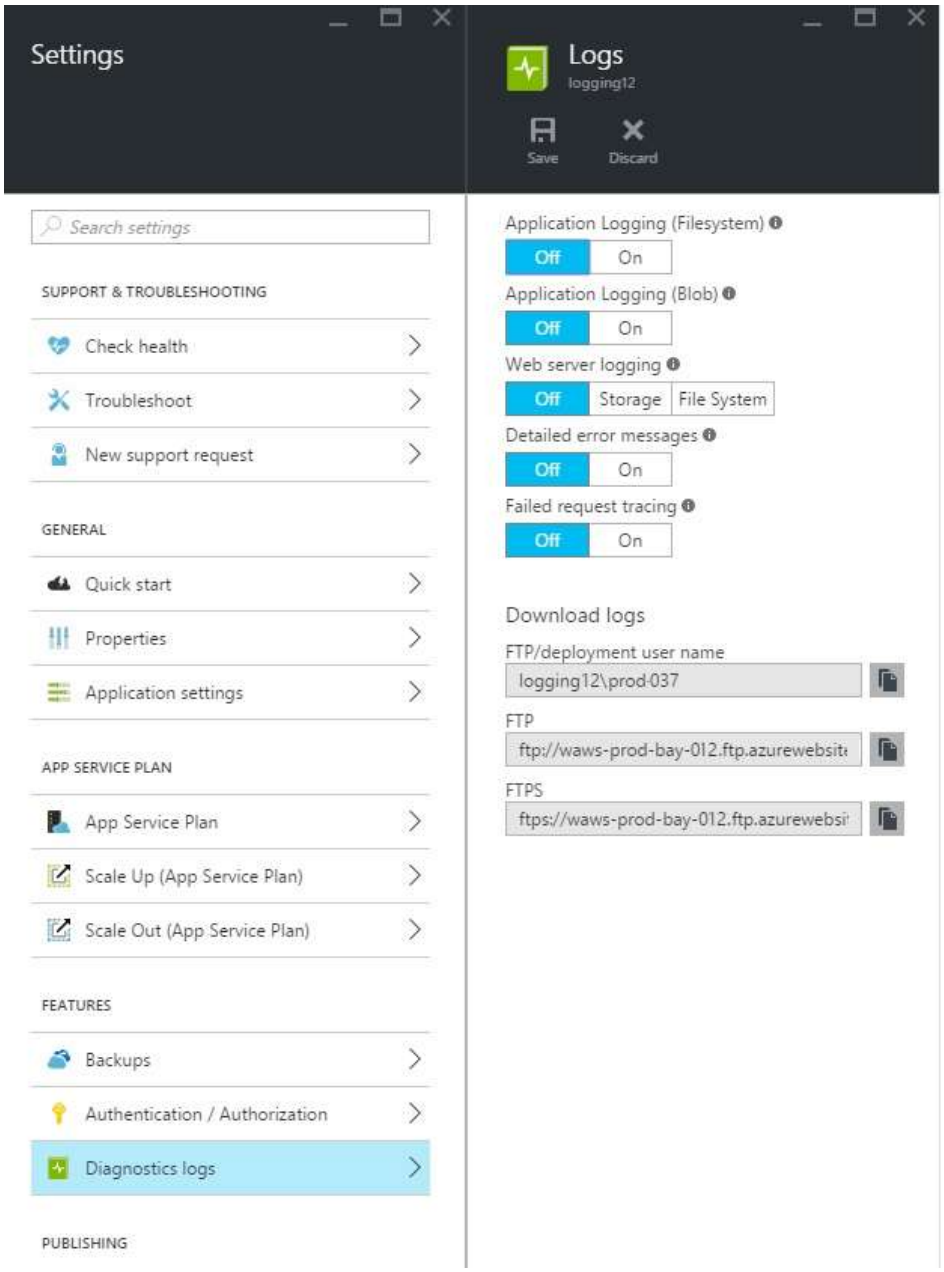
B) Analyze debugging information with Azure Web server and application diagnostics.

C) Log extensive debugging information with IntelliTrace.

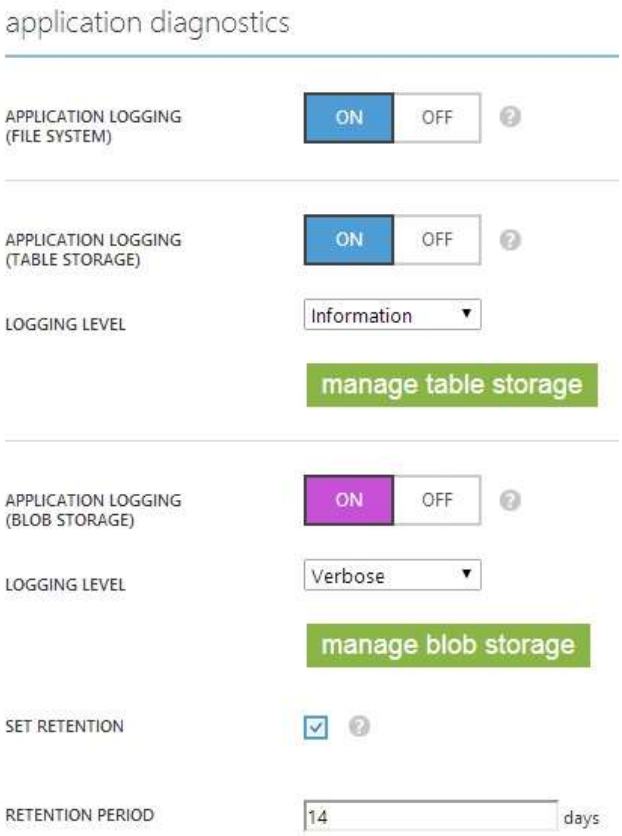
D) Attach a debugger in Visual Studio to the Azure role instance.

Explanation

You would use the Azure website log browser to analyze the Azure Web app logs because this utility is part of the gallery of Azure extensions. This is a useful utility to easily analyze web app logs. To analyze web app logs, in the Azure Portal go to the blade of the web app and click **Settings** > **Diagnostics** logs.



You would analyze debugging information captured by Azure Web Server diagnostics and Azure Application diagnostics because the service runs in Azure and is a built-in feature. Information captured by Azure Web Server diagnostics and Azure Application diagnostics is an easy way to analyze debugging information. You can use any combination of file system, table storage, or blob storage (also at the same time) to store log information.



You would not attach a debugger in Visual Studio to the Azure role instance because you explicitly have to enable that when you deploy the cloud service. If you did not enable remote debugging when you published the service, you have to republish the service with remote debugging enabled. This would be too much administrative effort.

You would not log extensive debugging information with IntelliTrace because with IntelliTrace you log extensive debugging information for a role instance when it runs in Azure. If you need to find the cause of a problem, you can use the IntelliTrace logs to step through your code from Visual Studio as if it were running in Azure. You must enable IntelliTrace before publishing the application to Azure. If you publish the application without configuring IntelliTrace, you will have to republish the application again from Visual Studio. This is too much administrative effort.

Objective:
Develop Azure compute solutions

Sub-Objective:
Create Azure App Service Web Apps

References:

Microsoft Azure > App Service > Web Apps > Enable diagnostics logging for apps in Azure App Service

Microsoft Docs > Visual Studio > Azure Development > Debugging an Azure cloud service or virtual machine in Visual Studio

Microsoft Docs > Visual Studio > Azure Development > Debugging a published Azure cloud service with Visual Studio and IntelliTrace

Blog.Amit > Azure Web App (Website) Logging - Tips and Tools

Question #113 of 135

Question ID: 1287238

You are the administrator of the Nutex Corporation. You want to develop an event-based solution that will use Azure event hub. Your application sends events to the event hub with one protocol and consumes them with a different protocol. The various parts and values of the events have to be translated and correctly interpreted by the consumer application. You have to translate Event Body information from AMQP to Kafka.

Which two classes can you use to achieve the same state in a Kafka producer or consumer?

A) AmqpSerializer

B) ByteArrayDeserializer

C) AmqpDeserializer

D) ByteArraySerializer

Explanation

You would use ByteArrayDeserializer and ByteArraySerializer because all of the Microsoft AMQP clients represent the event body as a stream of bytes.

The producing application passes the set of bytes to the client and a consuming application receives that same set of bytes from the client. The interpretation of a set of bytes happens within the application code. When sending an event via HTTPS, the event body is the POSTed content, which is also treated as uninterpreted bytes. The same state in a Kafka producer or a Kafka consumer is easy to achieve by using the ByteArraySerializer and ByteArrayDeserializer.

You would not use AmqpSerializer and AmqpDeserializer because these classes are used for event user properties. Kafka consumers use the AmqpDeserializer class when they receive properties from AMQP or HTTPS producers. The AmqpDeserializer class is modeled after the other deserializers in the Kafka ecosystem. The AmqpDeserializer reads the type of information in the AMQP-encoded byte sequences to deserialize the data bytes into a Java type.

You have to include a property in messages sent via AMQP or HTTPS. The properties in the messages are used by the Kafka consumer to determine whether header values need AMQP deserialization. The value of the property is not relevant. It just needs a well-known name so that the Kafka consumer can locate it in the list of headers and adjust its behavior accordingly.

Objective:
Connect to and consume Azure services and third-party services

Sub-Objective:
Develop event-based solutions

References:

Microsoft Azure > Messaging services > Event Hubs > Exchange events between consumers and producers that use different protocols: AMQP, Kafka, and HTTPS

GitHub > API Documentation > Class AmqpSerializer

Question #114 of 135

Question ID: 1287117

Laney currently manages the Nutex Azure cloud strategy, which involves resources found in multiple subscriptions across multiple regions using the Enterprise Pay-As-You-Go subscription. To conserve fiscal resources, she has been looking into Reserved Instance billing.

What scope should Laney select when configuring the Reserved Instance request?

A) She should select a shared scope to have the Reserved Instances spread across multiple subscriptions.

B) Laney should select one of the subscriptions to configure the Reserved Instance allocations to.

C) She should match up the Reserved Instances to the regions and machine types currently being used.

D) She cannot configure Reserved Instances because Pay-As-You-Go subscriptions are ineligible.

Explanation

Laney would select a shared scope to have the Reserved Instances spread across multiple subscriptions. Shared scope allows the application of Reserved Instances to multiple subscriptions.

She would not match up the Reserved Instances to the regions and machine types currently being used. This would be fine for resources in a single subscription, but ineffective if you have resources spread across multiple subscriptions like Nutex currently has.

Laney would not select one of the subscriptions to configure the Reserved Instance allocations to. This is possible, but leaves multiple other virtual machines uncovered by the possible discounts.

Pay-As-You-Go subscriptions are eligible. Pay-As-You-Go subscription types are certainly covered, especially for large enterprises. Laney must be the "Owner" to buy the reserved instances.

Objective:
Develop Azure compute solutions

Sub-Objective:
Implement IaaS solutions

References:

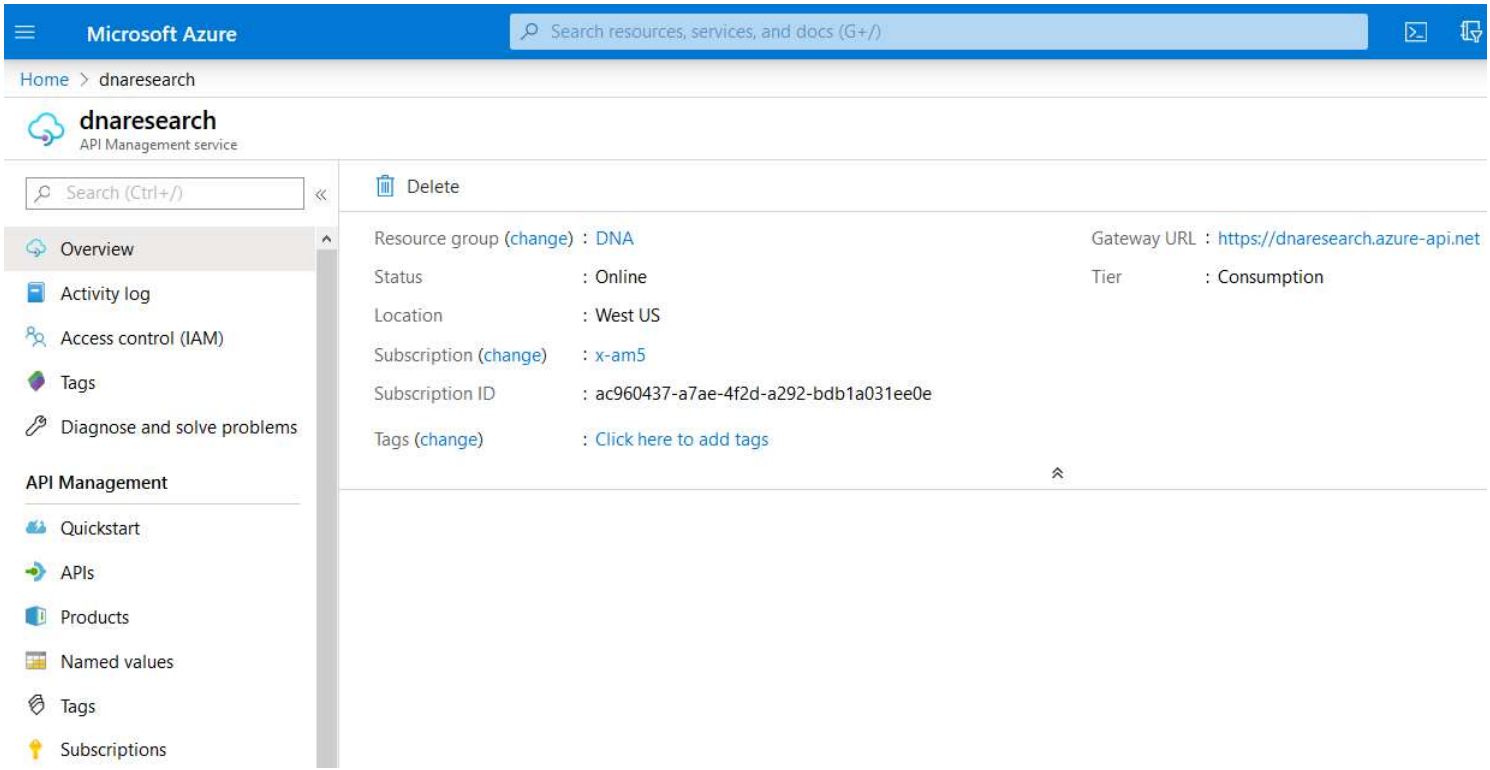
Microsoft Azure > Products > Azure Reserved VM Instances

Microsoft Azure > Cost Management and Billing > What are Azure Reservations?

Question #115 of 135

Question ID: 1287224

You work as an Azure developer for your company and are involved in the development of a system API. Another administrator implements the API Management service in Azure as follows:



Your origin API is deployed on a VM, and you need to protect the origin so that it only receives a connection from the **dnaresearch** API Management service. The IP address of the service must be the same for the lifetime of the service.

What should you do first to implement rules that allow a connection only from the **dnaresearch** API Management service?

A) Configure a firewall on the VM's operating system.

B) Create API Management.

C) Configure a network security group (NSG) on the VM.

D) Configure a firewall on the VM.

Explanation

You would create API Management because the existing API Management tier is Consumption, which does not include a static IP or integration with a VNET. Every API Management service instance in Developer, Basic, Standard, or Premium tier has public IP addresses, which are exclusive only to that service instance (they are not shared with other resources). These public IP addresses are static for the lifetime of the service.

You would not configure a network security group (NSG) on the VM, configure a firewall on the VM, or configure a firewall on the VM's operating system. All these tasks can be additional options. At this moment, we do not have a dedicated IP address of the API Management service because the Consumption tier service does not have a deterministic IP address.

Objective:
Connect to and consume Azure services and third-party services

Sub-Objective:
Implement API management

References:

Microsoft Azure > API Management > IP addresses of Azure API Management

---

Question #116 of 135

Question ID: 1287138

You are the administrator of the Nutex Corporation. You have created different Azure functions. You have to decide which kind of input and output binding you have to choose for which type of function. The trigger causes the function to run. The input and output bindings to the function connect another resource to the function.

Scenario 2:

A scheduled job reads Blob Storage contents and creates a new Cosmos DB document.

Apply the relevant input and output bindings.

{UCMS id=5661871542632448 type=Activity}

Explanation

Example scenario	Trigger	Input binding	Output binding
A new queue message arrives which runs a function to write to another queue.	Queue*	*None*	Queue*
A scheduled job reads Blob Storage contents and creates a new Cosmos DB document.	Timer	Blob Storage	Cosmos DB
The Event Grid is used to read an image from Blob Storage and a document from Cosmos DB to send an email.	Event Grid	Blob Storage and Cosmos DB	SendGrid
A webhook that uses Microsoft Graph to update an Excel sheet.	HTTP	*None*	Microsoft Graph

Because a scheduled job reads Blob Storage contents and creates a new document, your scheduled job is time-based. Therefore, you need a Timer trigger. To make it possible to read from a blob storage, you need the blob storage input binding, and to create a new Cosmos DB document you need the Cosmos DB outbound binding.

The function trigger is not HTTP because, in this scenario, no HTTP request has been received. The function trigger is not Event Grid because this function does not have to respond to an event sent to an event grid topic. The function trigger is not Queue because this function is not based on another queue.

The function cannot have an input binding with None because it must be based on Blob Storage content. The function cannot use Cosmos DB as the input binding because it must read blob storage content and not content from Cosmos DB.

The function cannot have an output binding with Queue because it must create a new Cosmos DB document. The function cannot have an output binding with SendGrid because it cannot send an email. The function cannot have an output binding with Microsoft Graph because in this scenario you do not want to have an Excel spreadsheet, OneDrive, or Outlook as output.

Objective:
Develop Azure compute solutions

Sub-Objective:
Implement Azure functions

References:

Microsoft Azure > Functions > Azure Functions triggers and binding concepts

Microsoft Azure > Functiions > Azure Event Grid bindings for Azure Functions

Microsoft Azure > Functions > Timer trigger for Azure Functions

Microsoft Azure > Functions > Azure Blob storage bindings for Azure Functions overview

Microsoft Azure > Functions > Azure Cosmos DB bindings for Azure Functions 1.x

---

Question #117 of 135

Question ID: 1403559

You need to build a development cluster named NutexAKSCluster for the resource group NutexResourceGroup.

At the prompt, type the appropriate Azure CLI command:

Type the correct response in the textbox provided.

Explanation

Acceptable answer(s) for field 1:

- az aks create --name NutexAKSCluster --resource-group NutexResourceGroup
- az aks create --resource-group NutexResourceGroup --name NutexAKSCluster

You would use the **az aks create** command to create an AKS cluster. You would use the `--resource-group` parameter to specify the resource group and the `--name` parameter to specify the name of the cluster.

Objective:
Develop Azure compute solutions

Sub-Objective:
Implement IaaS solutions

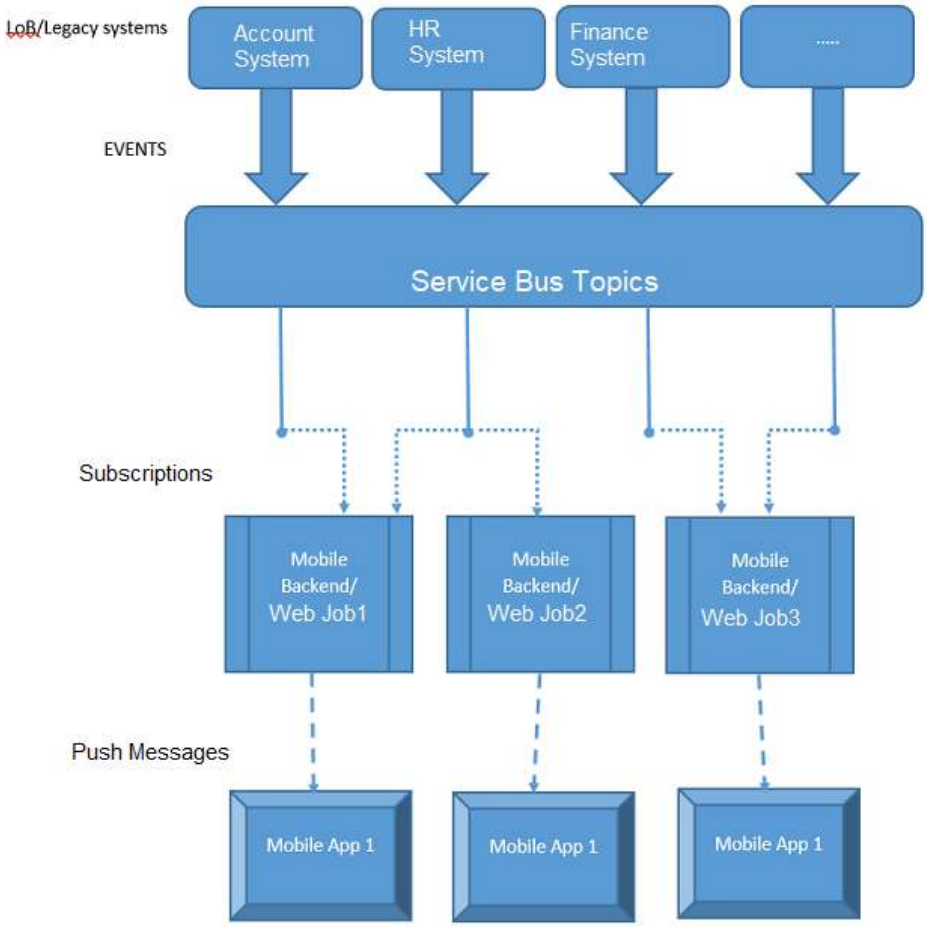
References:

Microsoft Azure > CLI > Reference > az aks create

Question #118 of 135

Question ID: 1404431

You are the administrator of the Nutex Corporation. You develop an event-based solution that will use Azure Notification Hubs. The app is for bank consumers who have the banking application on their device. They want to be notified when a debit is made above a certain amount from the account. An employee from the finance department also has a budget approval app on her phone and wants to be notified when the approved request is received. You plan the following architecture:



The accounting system, HR system, or Finance system will initiate messages that are sent as push notification messages. A mobile backend can subscribe to one or more topics. Notification hubs deliver messages to mobile apps.

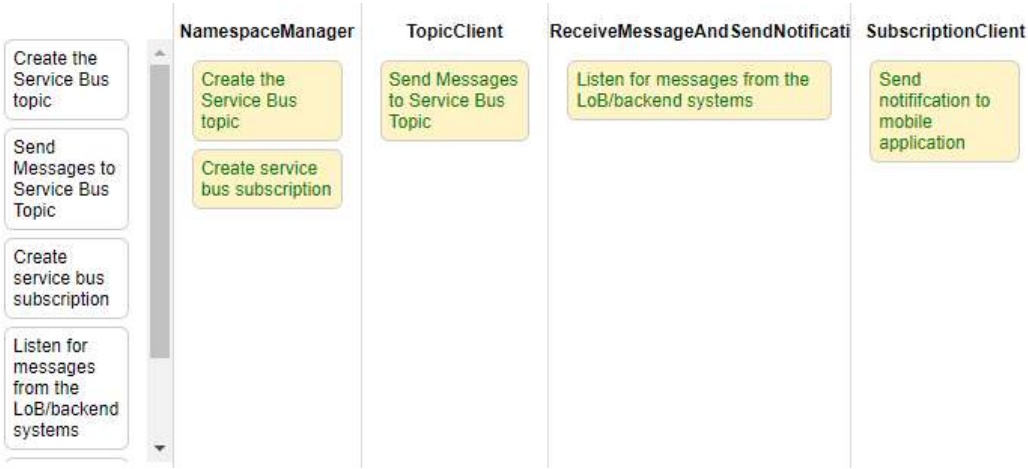
Which code parts do you have to use for which component?

Match the code parts to the appropriate component.

{UCMS id=5638704874913792 type=Activity}

Explanation

You should choose the following:



The Azure Service Bus has a topics/subscriptions programming model. The mobile backend is the receiver in this case. The mobile backend is typically the Azure Mobile Service, which initiates a push to mobile apps. The receiver receives messages directly from an intermediate abstraction layer provided by Azure Service Bus, not from the backend systems. The Azure Service Bus allows the mobile backend to receive messages from one or more backend systems.

A Service Bus Topic needs to be created for each of the backend systems. For example, Accounting, HR, Finance, are basically "topics" of interest, which initiate messages to be sent as push notifications. The backend systems send messages to these topics. A mobile backend can subscribe to a single or several such topics by creating a Service Bus subscription. It allows the mobile backend to receive a notification from the corresponding backend system. The mobile backend continues to listen for messages on their subscriptions, and when a message arrives, it sends the message as a notification to the notification hub.

You would use NamespaceManager to create the Service Bus topic and subscription. You can do that with the following code:

```
public static void CreateTopic(string connectionString)
{var namespaceManager =
        NamespaceManager.CreateFromConnectionString(connectionString);
if (!namespaceManager.TopicExists(sampleTopic))
{
    namespaceManager.CreateTopic(sampleTopic);}}

static void CreateSubscription(string connectionString)
{
var namespaceManager =
    NamespaceManager.CreateFromConnectionString(connectionString);
if (!namespaceManager.SubscriptionExists(sampleTopic, sampleSubscription))
{
    namespaceManager.CreateSubscription(sampleTopic, sampleSubscription);}}
```

You should use TopicClient to send Messages to Service Bus Topic. This code simply sends a set of random messages to the topic periodically for the purpose of the sample. Normally there is a backend system, which sends messages when an event occurs:

```
public static void SendMessage(string connectionString)
{TopicClient client =
   TopicClient.CreateFromConnectionString(connectionString, sampleTopic);
string[] messages =
{
   "Employee Id '{0}' has joined.",
   "Employee Id '{0}' has left.",
    "Employee Id '{0}' has switched to a different team."};
while (true)
   {Random rnd = new Random();
   string employeeId = rnd.Next(10000, 99999).ToString();
   string notification = String.Format(messages[rnd.Next(0,messages.Length)], employeeId);

  BrokeredMessage message = new BrokeredMessage(notification);
  client.Send(message);

  Console.WriteLine("{0} Message sent - '{1}'", DateTime.Now, notification);
  System.Threading.Thread.Sleep(new TimeSpan(0, 0, 10));}}
```

You would use ReceiveMessageandSendNotification to listen for messages from the LoB/Backend system. The following console app can run as a WebJob since it must run continuously to listen for messages from the LoB/backend systems. This application is part of your mobile backend:

```
static void Main(string[] args){string connectionString =
CloudConfigurationManager.GetSetting("Microsoft.ServiceBus.ConnectionString");
CreateSubscription(connectionString);ReceiveMessageAndSendNotification(connectionString);}
```

You would use the Subscription client to send notifications to the mobile app.

Objective:
Connect to and consume Azure services and third-party services

Sub-Objective:
Develop event-based solutions

References:

Enterprise push architectural guidance:

Microsoft Azure > Notification Hubs > Enterprise push architectural guidance

---

Question #119 of 135

Question ID: 1403572

You manage a Cosmos DB at Nutex Corporation. Every once in a while there is a storage problem that needs attention.

The Nutex cloud services team wants you to generate an alert to monitor the Cosmos DB storage and trigger when available space gets below a specified threshold.

What options are available for you to create the desired alert? (Choose all that apply.)

A) Use an Azure PowerShell Script to execute **Add-AzMetricAlertRule**.

B) In the Azure CLI, execute the command `az monitor alert create`.

C) Using a Windows Server cmd.exe session, execute `az monitor alert create`.

D) In the Azure Portal, under Azure CosmosDB properties, add an Alert Rule.

E) In Visual Studio, use the .NET SDK, to call the DocumentClient.ReadDocumentCollectionAsync method.

Explanation

The following options are possible:

- Use an Azure PowerShell Script to execute **Add-AzMetricAlertRule**.
- In the Azure CLI, execute the command `az monitor alert create`.
- In the Azure Portal, under Azure CosmosDB properties, add an Alert Rule.

You can execute the **Add-AzMetricAlertRule** cmdlet with the appropriate options and arguments to successfully create an alert as desired. The following creates a metric alert rule for a website:

```
Add-AzMetricAlertRule -Name "MyMetricRule" -Location "East US" -ResourceGroup "Default-Web-EastUS" -Operator GreaterThan -Threshold 2 -WindowSize 00:05:00 -MetricName "Requests" -Description "Pura Vida" -TimeAggregationOperator Total
```

You can execute the command `az monitor alert create` in the Cloud Shell or from a local machine to create an alert. The following creates a high CPU usage alert on a VM with no actions:

```
az monitor alert create -n rule1 -g {ResourceGroup} --target {VirtualMachineID} --condition "Percentage CPU > 90 avg 5m"
```

In the Azure Portal, under Azure CosmosDB properties, you can add an Alert Rule. Using the Web User Interface, you can click your way to successfully creating an alert to monitor Azure Cosmos DB.

You cannot use the .NET SDK in Visual Studio to call the DocumentClient.ReadDocumentCollectionAsync method. While you can use the .NET SDK to interact with Azure and create alerts, the specified method will not succeed in doing so.

You cannot use a Windows Server cmd.exe session to execute `az monitor alert create`. There currently are no plans to support cmd.exe interaction with Azure and therefore this would fail.

Objective:
Develop for Azure storage

Sub-Objective:
Develop solutions that use Cosmos DB storage

References:

Microsoft Azure > Cosmos DB > Monitoring Azure Cosmos DB

Microsoft Azure > CLI > Reference > az monitor alert create

Microsoft Azure > Azure Monitor > Azure Monitor PowerShell quick start samples

---

Question #120 of 135

Question ID: 1403575

You are the administrator of the Nutex Corporation. You want to set metadata on a blob container with C#. You want to set the value “textDocuments” for the `doctype` container property and the value “guidance” for the `category` container property.

How can you configure these values? (Choose all that apply.)

A) `PUT` method

B) `EDIT` method

C) `ADD` method

D) implicit key/value

Explanation

You would begin with the `ADD` method. The `ADD` method allows you to set metadata on a container. You can use this method to add metadata to a blob container using `container.Metadata.Add()`. The following code sets the value “textDocuments” to the `doctype` container property:

```
container.Metadata.Add("docType", "textDocuments");
```

Then you would use implicit key/value to set the value “guidance” to the `category` container property. The following code shows the syntax:

```
container.Metadata["category"] = "guidance";
```

You would not use the `PUT` method. The `PUT` method is not used with C#. You can use the `PUT` method with HTTP protocol to set container properties.

There is no `EDIT` method available for `container.metadata` that you can use in C#. You can use the `EDIT` method in Java.

Objective:
Develop for Azure storage

Sub-Objective:
Develop solutions that use blob storage

References:

Microsoft Docs > Azure > Storage > Manage container properties and metadata with .NET

Microsoft Azure > Storage Services > Set Container Metadata

Question #121 of 135

Question ID: 1287156

You are the administrator of the Nutex Corporation. You have created a Cosmos DB storage database. You want to run parallel write operations across partitions. You also want to avoid a single hot partition key.

Which of the following synthetic partition key options is the best?

A) Use a partition key with pre-calculated suffixes.

B) Manually concatenate multiple properties for an item.

C) Use a partition key with a random prefix.

D) Use a partition key with a random suffix.

Explanation

You would use a partition key with pre-calculated suffixes. With this strategy, the writes are evenly spread across the partition key values and across the partitions. A pre-calculated suffix, unlike a random suffix, is easy to read. Say that you are storing automotive data where each automobile is represented by a unique Vehicle Identification Number (VIN). If you want to run queries to find automobiles, in addition to the date, using a pre-calculated suffix allows the application to write the item to a container and calculate a hash suffix based on the VIN and append it to the partition key date.

You can easily read a particular item and date because you can calculate the partition key value for a specific VIN. The benefit of this method is that you can avoid creating a single hot partition key that takes all the workload.

You would not manually concatenate multiple properties for an item because, in real-time scenarios, you can have thousands of items in a database. Instead of adding the synthetic key manually, define client-side logic to concatenate values and insert the synthetic key into the items in your Cosmos containers.

You would not use a partition key with a random suffix because with that you cannot avoid a single hot partition key. Nevertheless, this method is good for better parallelism and overall higher throughput.

You would not use a partition key with a random prefix. You should have a suffix instead of a prefix. A suffix appends the value to the end, which makes it easier to read. A pre-calculated suffix key is easier to read than a random prefix key.

Objective:
Develop for Azure storage

Sub-Objective:
Develop solutions that use Cosmos DB storage

References:

Microsoft Azure > Cosmos DB > Create a synthetic partition key

---

Question #122 of 135

Question ID: 1403568

You are working as a developer for the Nutex Corporation. You are developing the monitor pattern to observe an arbitrary endpoint with the following code:

```
[FunctionName("AzureFunc-JobStatusMonitoring")]
public static async Task Run(
    [OrchestrationTrigger] IDurableOrchestrationContext context)
{
    int jobId = context.GetInput<int>();
    int pollingInterval = GetPollingInterval();
    DateTime expiryTime = GetExpiryTime();
    while (context.CurrentUtcDateTime < expiryTime)
    {
        var jobStatus = await context.CallActivityAsync<string>("GetJobStatus", jobId);
        if (jobStatus == "Completed")
        {
            // Code...
            await context.CallActivityAsync("SendAlert", machineId);
            break;
        }
        var nextCheck = context.CurrentUtcDateTime.AddSeconds(pollingInterval);
        await context.CreateTimer(nextCheck, CancellationToken.None);
    }

  // Code...
}
```

You notice that the code does not work for more than seven days.

How should you easily resolve the problem? (Choose two, each answer is a complete solution.)

A) redesign the solution to use Azure Batch.

B) redesign the function to use a Durable Function.

C) use the `while` loop for simulating a timer API.

D) use the `for` loop for simulating a timer API.

Explanation

Durable timers are limited to seven days. The workaround is to simulate using the timer API in a loop, such as a `while` loop or a `for` loop.

You would not redesign the function to use a Durable Function. The `"AzureFunc-JobStatusMonitoring"` function is already a Durable Function. In line number 3, the function uses `IdurableOrchestrationContext,` which means it is already a Durable Function (2.x).

You would not redesign the solution to use Azure Batch. Although this action could work since Azure Batch schedules jobs to run on nodes, we have no information about which nodes the application runs on. Using timer APIs in a loop is less complicated.

Objective:
Develop Azure compute solutions

Sub-Objective:
Implement Azure functions

References:

Microsoft Azure > Functions > Timers in Durable Functions (Azure Functions)

Question #123 of 135

Question ID: 1287179

You are the administrator of the Nutex Corporation. You use RBAC authentication for an ASP.NET MVC application. You have defined an action for creating customers. People from the sales department should be able to create customers through that action. Later, you also add the marketing people to that action. After some time, you realize that some of the marketing people must not be able to create customers. You cannot assign a different role for those people. You want only authenticated users to use the create customers action.

What is the first step the developer must do?

A) Build and register a policy

B) Use the `Policy` property on the `AuthorizeAtribute` attribute

C) Apply the `AllowAnonymousAttribute` attribute

D) add `[Authorize(Roles=”Sales,”Marketing”)]` to the code

Explanation

You would build and register a policy because claim-based authorization checks are declarative. A developer can add authorization checks within their code, against a controller or an action within a controller, specifying claims which the current user must possess, and optionally the value the claim must hold to access the requested resource. Claims requirements are policy based. The developer must build and register a policy expressing the claims requirements.

For example, in this case the EmployeeOnly policy checks for the presence of an EmployeeNumber claim on the current identity:

```
public void ConfigureServices(IServiceCollection services)
{services.AddMvc();
services.AddAuthorization(options =>
{options.AddPolicy("EmployeeOnly", policy => policy.RequireClaim("EmployeeNumber"));});
```

You would not add `[Authorize(Roles="Sales,"Marketing")]` to the code because with that you implement the RBAC authentication for both sales and marketing people. In this scenario, some of the marketing people must not be able to create customers.

You would not use the `Policy` property on the `AuthorizeAtribute` attribute because with that you can apply the policy. This action is the second step after creating the policy.

You would not apply the `AllowAnonymousAttribute` attribute because if you have a controller that is protected by the `AuthorizeAttribute` attribute but want to allow anonymous access to particular actions, you should apply the `AllowAnonymousAttribute` attribute. In this case, you want only authenticated users using the create customers action.

Objective:
Implement Azure security

Sub-Objective:
Implement user authentication and authorization

References:

Microsoft Docs > Protocols > 1.1.1.11 Claim-Based Access Control (CBAC) Model

Stackoverflow > Role-based access control (RBAC) vs. Claims-based access control (CBAC) in ASP.NET MVC

Microsoft Docs > .NET > Security and Identity > Claims-based authorization in ASP.NET Core

---

Question #124 of 135

Question ID: 1287213

You are working as a developer for the Nutex Corporation. You are responsible for an online e-store system using PHP 7.4. You are preparing for the Black Friday and Cyber Monday period. After a user buys a digital item (e.g., e-book), the monolithic application generates a personal version in .pdf format and sends it using email. Your CEO is afraid that during the Black Friday and Cyber Monday period, the application will hang with the time limit.

Which cloud design pattern do you propose to mitigate the time limit?

A) Implement Cache-Aside pattern.
B) Implement Sharding pattern.
C) Implement Competing Consumers pattern.
D) Implement Retry pattern.

Explanation

You would implement the Competing Consumers cloud design pattern. This pattern allows multiple consumers to process messages received simultaneously on the same messaging channel. You can have a queue and other subsystems receiving a message via the queue to generate digital content and send it via email.

You would not implement the Retry pattern. The Retry pattern improves the stability of an application by allowing an application to retry a failed operation when intermittent failures of connecting to a network resource or a service occur. This pattern will not resolve the time-limit problem.

You would not implement the Cache-Aside pattern. The Cache-Aside pattern is used to improve performance when loading data. This pattern is for storing data in memory to speed up queries. It also keeps consistency between data in the underlying data store and data held in the cache. This pattern will not resolve the time-limit problem.

You would not implement the Sharding pattern. This pattern is used for splitting data across databases, disks, files, or partitions. This pattern will not resolve the time-limit problem.

Objective:
Monitor, troubleshoot, and optimize Azure solutions

Sub-Objective:
Instrument solutions to support monitoring and logging

References:

Microsoft Azure > Architecture > Cloud Design Patterns > Competing Consumers pattern

---

Question #125 of 135

Question ID: 1287135

You are the administrator of Nutex. You have to design a solution for your web application named **NutexApp** in the West US region. The application uses the following Azure features: Azure Websites, Storage, and SQL Database services.

You want to ensure that when the user submits a new task, the user will immediately get a success message from the application independent of the availability of the SQL database. You also want to have an SLA of more than 99.8 percent for your solution.

Which of the following is the best solution for the requirements?

A) Create two queues in region West US. Designate one queue as the primary queue and the other as secondary.

B) Create two queues in two different regions. Designate one queue as the primary queue and the other as secondary.

C) Use two Azure SQL databases with locally redundant replication (LRS).

D) Use two Azure SQL databases with geo-redundant replication (GRS).

Explanation

You would create two queues in two different regions and designate one queue as the primary queue and the other as secondary. In this scenario, you want to ensure that when the user submits a new task, the user will immediately get a success message from the application independent of the availability of the SQL database. You have to prepare the application so that it failovers to the second queue if the primary queue is not available.

You would not use two Azure SQL databases with locally redundant replication (LRS) because this will not fulfill the requirements. The user has to get a success message from a queue immediately. In this scenario you need to make the queue highly available. The solution is not to make the SQL databases more highly available with LRS. It may be a good idea to make the SQL database highly available too, but it is not the solution for the queues.

You would not use two queues in the region West US and designate one queue as the primary queue and the other as secondary. If the region West US is going down then both queues are not working and the user cannot be informed about the processing of their task.

You would not use two Azure SQL databases with geo-redundant replication (GRS) because this will not fulfill the requirements. The user has to get a success message from a queue immediately. In this scenario you need to make the queue highly available. The solution is not to make the SQL databases more highly available via GRS. It may be a good idea to make the SQL databases highly available through different continents with GRS, but it is not the solution for the queues.

Objective:
Develop Azure compute solutions

Sub-Objective:
Create Azure App Service Web Apps

References:

Microsoft Docs > ASP.NET 4x > Web Development Best Practices > Queue-Centric Work Pattern (Building Real-World Cloud Apps with Azure)

StackOverflow > Failure handling for Queue Centric work pattern

---

Question #126 of 135

Question ID: 1287202

You are working as a developer for the Nutex Corporation. You developed an internal vacation HR planning application for a Chinese subsidiary of the Nutex Corporation in PHP 7.4 with custom libraries. The application was developed in (US) East US 2 region and registered in Azure Active Directory, and has been tested successfully by the US team. After moving the application to Azure China, you received information that the US team was not able to log in to the application. You must write a report to the CEO.

What could be the reason why the US team is not able to log in to the application?

A) The application is behind the Great Firewall.

B) The network security groups (NSGs) were not set correctly.

C) Azure Active Directory in (US) East US 2 and Azure China are independently operated.

D) Azure China does not support custom libraries.

Explanation

Services located in China are independently operated by Shanghai Blue Cloud Technology Co., Ltd (21 Vianet Blue Cloud). National clouds are unique and are separate environments from Azure global. You must register the application in Azure China Active Directory.

All of the other answers are incorrect.

The Great Firewall of China is the term used to describe the combination of technologies and legislative actions used by the Chinese government to regulate the Internet domestically. The Great Firewall can be used to filter egress connections from China, not from outside China.

NSGs contain security rules that allow or deny network traffic. They can block connections to a workload, but do not allow you to register an application in a different cloud.

Custom libraries are not connected with authentication, so that would not be a reason why you could not connect to the application.

Objective:
Monitor, troubleshoot, and optimize Azure solutions

Sub-Objective:
Integrate caching and content delivery within solutions

References:

Microsoft Docs > Azure > Active Directory > Develop > National clouds

---

Question #127 of 135

Question ID: 1403584

You are the administrator of the Nutex Corporation. You do not want to put a secure value such as a password directly in your ARM template or parameter file. You want to retrieve the value from an Azure Key Vault during deployment. You are not the owner of the key vault. You need to set the permission for secrets to set, delete, get, and list.

Which PowerShell cmdlets must you use to perform for a key vault secret to pass a secure parameter value during deployment?

Place the cmdlets in the correct order.

{UCMS id=5688444605956096 type=Activity}

Explanation

You would choose the following:

1. **New-AzKeyVault** with the `EnabledForTemplateDeployment` parameter set
2. **ConvertTo-SecureString**
3. **Set-AzKeyVaultPolicy**
4. **Set-AzKeyVaultSecret**

First you would use the **New-AzKeyVault** cmdlet to create the Azure Key Vault. You have to define the VaultName, the resource group, and the location. The following creates an Azure Key Vault in a resource group:

```
New-AzResourceGroup -Name $resourceGroupName -Location $location
New-AzKeyVault ‘
  -VaultName $keyVaultName ‘
  -resourceGroupName $resourceGroupName ‘
  -Location $location ‘
  -EnabledForTemplateDeployment
$secretvalue = ConvertTo-SecureString 'N0S8ntz$uk' -AsPlainText –Force
$secret = Set-AzKeyVaultSecret -VaultName $keyVaultName -Name 'ExamplePassword' -SecretValue $secretvalue
```

You would set the `EnabledForTemplateDeployment` parameter, instead of the `EnabledForDeployment` parameter, of the **New-AzKeyVault** cmdlet to true so that you can access the key vault during template deployment. The `EnabledForDeployment` parameter allows the resource provider to access the vault when the key vault is referenced in resource creation, not during deployment.

Then you would create a variable with the password as content. With the **ConvertTo-SecureString** cmdlet, you can create an encrypted password.

You would then use the **Set-AzKeyVaultPolicy** cmdlet to give access to create secrets. The following gives permissions for set, delete, get, and list:

```
Set-AzKeyVaulPolicy -Vaultname -userPrincipalName -PermissionsToSecrets set, delete, get, list
```

Then you would use the **Set-AzKeyVaultSecret** cmdlet to create the secret itself in the key vault.

Objective:
Implement Azure security

Sub-Objective:
Implement secure cloud solutions

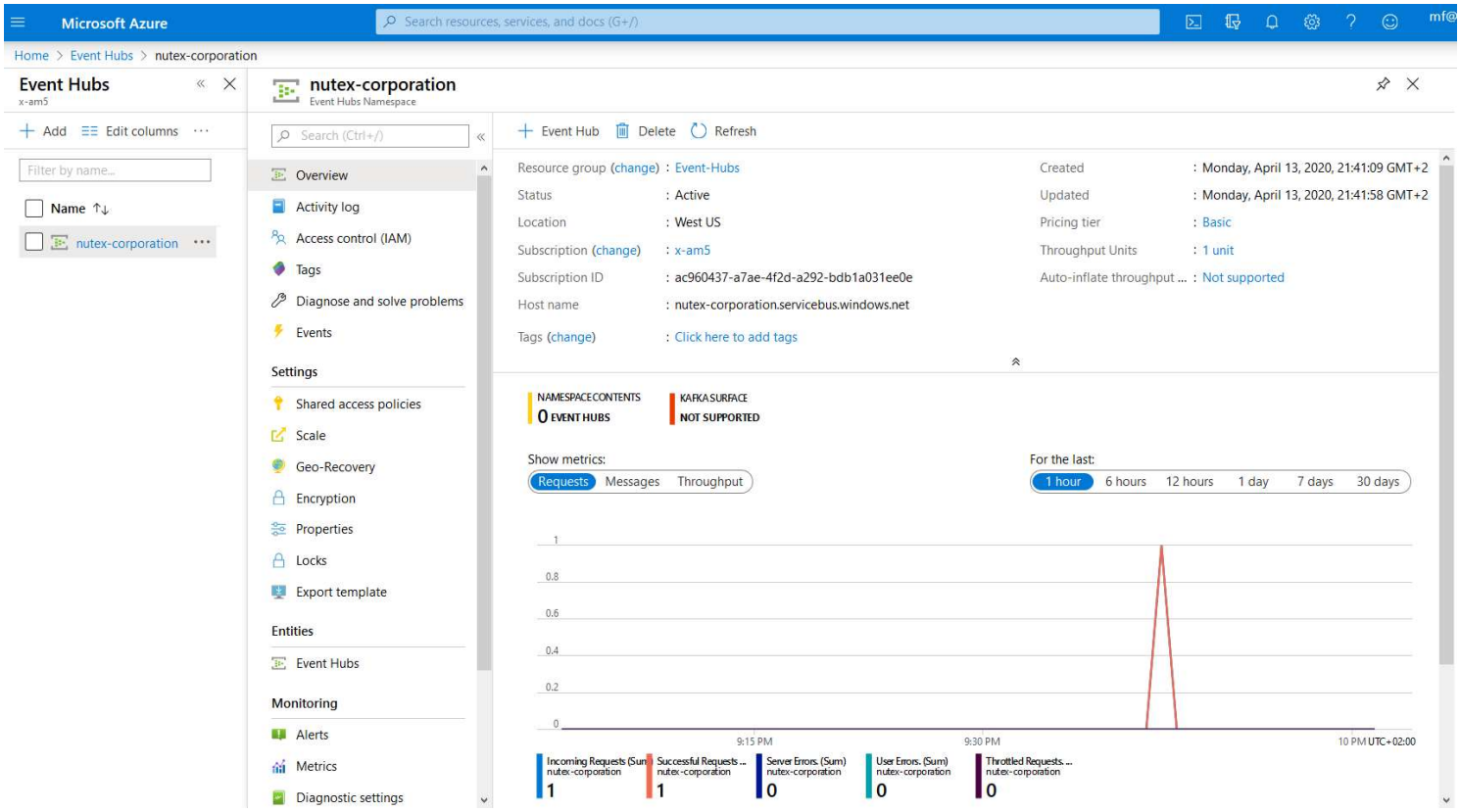
References:

Microsoft Azure > Resource Manager > Use Azure Key Vault to pass secure parameter value during deployment: HYPERLINK "https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-manager-keyvault-parameter"

Question #128 of 135

Question ID: 1287241

You are working as a developer for the Nutex Corporation. You are implementing a solution that sends Azure Events to an external security information and event management (SIEM) system. The external SIEM solution accepts only Kafka standard messages. Your main administrator created an Event Hub for this, but you notice that it is not working. The Event Hubs looks like the following graphic:



Which step should you perform first to integrate with an external SIEM solution?

A) Add Azure Active Directory to the Event Hub.

B) Configure Azure Monitor to send relevant security logs.

C) Generate sample events and check on the destination services.

D) Upgrade to Standard Tier.

Explanation

In this scenario, you are using the Basic tier. You would need to upgrade to Standard Tier. The Standard Tier plan and above supports Kafka messages in Event Hub. The Basic tier does not.

You would not configure Azure Monitor as the first step. This would be the second step in sending logs. You will need to support Kafka messages in Event Hub first.

You would not add Azure Active Directory to the Event Hub. This is an optional step. You would only perform this step if you want to include logs from Azure Active Directory in SIEM.

You would not generate sample events and check on destination services. This action will not reach the destination SIEM because the basic Plan does not support Kafka.

Objective:
Connect to and consume Azure services and third-party services

Sub-Objective:
Develop event-based solutions

References:

Microsoft Azure > Products > Event Hubs pricing

Rapid 7 > Microsoft Azure

Question #129 of 135

Question ID: 1403597

You are the administrator of the Nutex Corporation. You want to use Firebase Cloud Messaging together with Azure Notification Hub to push notifications to all registrations and to registered devices.

Which task or code snippet would you NOT use for that?

A) In the build.gradle file, add: `apply plugin: 'com.google.gms.google-services'`

B) In the build.gradle file, add: `implementation 'com.google.firebase:firebase-core:16.0.8'; implementation 'com.google.firebase:firebase-messaging:17.3.4`

C) In the build.gradle file, add: `classpath 'com.google.gms:google-services:4.0.1'`

D) Use `Config.MessageHandlers.Add(new AuthenticationTestHandler());`

E) Use `foreach (var category in categories) {templateParams["messageParam"] = "Breaking " + category + " News!"; await hub.SendTemplateNotificationAsync(templateParams, category);}`

Explanation

You would not choose `Config.MessageHandlers.Add(new AuthenticationTestHandler());`, because with that code snippet, you register the message handler to use a push notification for Firebase Cloud Messaging. You do not need to do push notifications to all registrations and push notifications to registered devices.

You would add: `apply plugin: 'com.google.gms.google-services'` in the build.gradle file, because to push notifications to all registrations, you have to add that code line to the build.gradle file.

You would add: `implementation 'com.google.firebase:firebase-core:16.0.8'; implementation 'com.google.firebase:firebase-messaging:17.3.4` in the build.gradle file, because you have to add that code line to the build.gradle file to push notifications to all registrations.

You would add: `classpath 'com.google.gms:google-services:4.0.1'` in the build.gradle file, because you have to add that code line to the build.gradle file to push notifications to all registrations.

You would use `foreach (var category in categories)`

`{templateParams["messageParam"] = "Breaking " + category + " News!"; await hub.SendTemplateNotificationAsync(templateParams, category);}`, because with that, you can implement push notification to specific devices through categories and tags.

Objective:
Connect to and consume Azure services and third-party services

Sub-Objective:
Develop event-based solutions

References:

Microsoft Azure > Notification Hubs > Tutorial: Send push notifications to Android devices using Firebase

Microsoft Azure > Notification Hubs > Tutorial: Send push notifications to specific Android apps using Azure Notification Hubs

---

Question #130 of 135

Question ID: 1403556

You have a Kubernetes cluster in AKS and you deployed an app called **MyApp.** You increase the number of nodes from one to three in the Kubernetes cluster by using the following command:

[ ] `--resource-group=myResourceGroup --name=myAKSCluster --node-count 3`

The output of the command is as follows:

```
"agentPoolProfiles": [
  {
    "count": 3,
    "dnsPrefix": null,
    "fqdn": null,
    "name": "myAKSCluster",
    "osDiskSizeGb": null,
    "osType": "Linux",
    "ports": null,
    "storageProfile": "ManagedDisks",
    "vmSize": "Standard_D2_v2",
    "vnetSubnetId": null
  }
```

In the space provided above, type the missing part of the command.

Explanation

Acceptable answer(s) for field 1:

- az aks scale

You would type the `az aks scale` command. This command is used to scale the node pool in a Kubernetes cluster. The `--name` parameter specifies the name of the cluster. The `--resource group` specifies the name of the resource group. The `--node` parameter specifies the number of nodes in the pool.

Objective:
Develop Azure compute solutions

Sub-Objective:
Implement IaaS solutions

References:

Microsoft Azure > AKS > Tutorial: Scale application in Azure Kubernetes Service (AKS)

Microsoft Azure > CLI > Extensions Reference > az aks

Question #131 of 135

Question ID: 1403567

You are the administrator of the Nutex Corporation. You have created an Azure function app with Visual Studio. You want to upload the required settings to your function app in Azure. For that, you use the Manage Application Settings link. However, the Application Settings dialog is not working as you expected.

What is a possible solution for this?

A) manually create the **host.json** file in the project root.

B) install the Azure storage emulator.

C) manually create an Azure storage account.

D) manually create the **local.settings.json** file in the project root.

Explanation

You would manually create the **local.settings.json** file in the project root because by default the **local.settings.json** file is not checked into the source control. When you clone a local functions project from source control, the project does not have a **local.settings.json** file. In this case you need to manually create the **local.settings.json** file in the project root so that the Application Settings dialog will work as expected.

You would not manually create the **host.json** file in the project root because this file lets you configure the functions host. The settings apply both when running locally and in Azure.

You would not manually create an Azure storage account because, although Azure functions require a storage account, it is automatically created so you not have to create it manually.

You would not install the Azure storage emulator because with that you cannot upload the required settings.

Objective:
Develop Azure compute solutions

Sub-Objective:
Implement Azure functions

References:

Microsoft Azure > Functions > Develop Azure Functions using Visual Studio

---

Question #132 of 135

Question ID: 1403594

You need to create and deploy an Azure managed application. You want to add a managed application to an internal catalog for users in your organization, and then you will deploy that application to your subscription.

Choose the appropriate steps and place them in the correct order.

{UCMS id=5706946579529728 type=Activity}

Explanation

You would choose the following:

1. Create a resource group for the application definition.
2. Create the managed application definition resource.
3. Create a resource group for the managed application.
4. Us the `az managedapp create` command to deploy the managed application.

You would first create a resource group for the application definition. The application definition must have a resource group where the definition will reside before the application definition resource is defined. Groups or users will manage the resources of the managed application. The following uses the `az group create` command to create a resource group for the application definition in the WestCentralUs region:

```
az group create --name appDefinitionGroup --location westcentralus
```

Once you have obtained the object ID of the user or group that will manage the resources, you can use the `az managedapp definition create` command to create the managed application definition resource, as follows:

```
az managedapp definition create \
  --name "ManagedStorage" \
  --location "westcentralus" \
  --resource-group appDefinitionGroup \
  --lock-level ReadOnly \
  --display-name "Managed Storage Account" \
  --description "Managed Azure Storage Account" \
  --authorizations "$userid:$roleid" \
  --package-file-uri "https://raw.githubusercontent.com/Azure/azure-managedapp-samples/master/samples/201-managed-storage-account/managedstorage.zip"
```

Once the application definition resource has been created, you can deploy the managed application. However, you will need to have a resource group for the managed application.

To create a resource group for the managed application, you can use the `az group create` command. The following creates a resource group named **applicationGroup**:

```
az group create --name applicationGroup --location westcentralus
```

Once the resource group has been created for the managed application, you can deploy the application. You can use the command `az managedapp create` to deploy the application. The following deploys the app named **storageApp** in the **applicationGroup** resource group:

```
appid=$(az managedapp definition show --name ManagedStorage --resource-group appDefinitionGroup --query id --output tsv)
subid=$(az account show --query id --output tsv)
managedGroupId=/subscriptions/$subid/resourceGroups/infrastructureGroup

az managedapp create \
  --name storageApp \
  --location "westcentralus" \
  --kind "Servicecatalog" \
  --resource-group applicationGroup \
  --managedapp-definition-id $appid \
  --managed-rg-id $managedGroupId \
  --parameters "{\"storageAccountNamePrefix\": {\"value\": \"storage\"}, \"storageAccountType\": {\"value\":
\"Standard_LRS\"}}"
```

You would not use the `az managedapp show` command to deploy the managed application. This command only retrieves a managed application.

Objective:
Connect to and consume Azure services and third-party services

Sub-Objective:
Implement API management

References:

Azure > Managed Applications > Quickstart: Create and publish a managed application definition

Azure > Resource Manager > Managed Applications > Deploy a managed application for service catalog with Azure CLI

Question #133 of 135

Question ID: 1403580

You work as an Azure architect for your company and are involved in an application review that backs up DNA blob data to the storage account archive tier. There are business requirements that, once a month, random DNA from a probe two years ago must be restored within two hours.

You use the following command to retrive the DNA blob to a hot tier:

```
Start-AzStorageBlobCopy -SrcContainer $srcContainerName -SrcBlob $srcBlobName -DestContainer $destContainerName -DestBlob
$destBlobName -StandardBlobTier Hot -RehydratePriority Standard -Context $ctx
```

Data is not being resolved within a two-hour period. What is your suggestion to resolve the problem?

A) Use CloudBlob.StartCopyAsync.

B) Modify your code not to use the archive tier.

C) Use CloudBlob.StartCopy.

D) Add the parameter `-Force $true`.

Explanation

You would modify your code not to use the archive tier. Data in this scenario is stored in the storage account archive tier. You need to restore specific data from the account archive tier within two hours. Data in the archive tier can take several hours to retrieve, which may not be within the required two-hour

period. Data in this scenario should be in cool access tier instead of the archive access tier.

The following is an explanation of each access tier:

- **Hot –** this tier is used for data that is frequently accessed. It is more expensive to store data here, compared to the Cool and Archive tiers, but cheaper to access.
- **Cool** – this tier is used for storing less frequently accessed data, such as archived files, backups, and raw or unprocessed data. Cool is designed for data that is likely to be stored for at least 30 days. Cool storage costs less than Hot storage per GB.
- **Archive –** this tier is the most cost-effective option for storing data, but is typically more expensive for data retrieval than the Hot and Cool tiers. Archive is designed for data that is likely to be stored for at least 180 days, and for systems or scenarios where retrieval latency can be tolerated.

All other options do not resolve the problem of moving data from the Archive tier to the Hot tier.

You would not use CloudBlob.StartCopyAsync or CloudBlob.StartCopy. Both allow you to copy blobs between storage accounts. However, if there are any changes to the source while the copy is in progress using either method, the copy will fail.

You would not add the parameter `-Force $true`. Adding the parameter `-Force $true` overwrites the destination blob without prompting you for confirmation. Just because the parameter forces an overwrite of the destination, it does not speed up the process of moving the data from the Archive tier to the Hot tier.

Objective:
Develop for Azure storage

Sub-Objective:
Develop solutions that use blob storage

References:

Microsoft Docs > Azure > Storage > Blobs > Azure Blob storage: hot, cool, and archive access tiers

---

Question #134 of 135

Question ID: 1287174

You have a blob in Azure storage. You need to set the permissions in a way that the user can have anonymous access to the blob, but not the ability to enumerate other blobs in the same container.

Which permission should you set?

A) Container

B) Blob

C) Private/Off

D) Anonymous access is not allowed in this scenario.

Explanation

You would give the user the blob permission. This will allow an anonymous user to read all the blobs in the container but not enumerate them. Users that have the URL to a blob in the container where the blob permission is set can read the blob, the properties of the blob, and the metadata of the blob. Users cannot write to the blob, retrieve any information about the blob's container, nor retrieve a list of blobs in the container unless they use a shared access signature with the appropriate permissions.

You would not use the container permission. With this permission, in addition to the ability to read the blobs in the container, the anonymous user is able to enumerate them.

The Private/Off option does not work for anonymous users. It requires the user to authenticate to the storage account.

You would not select the option Anonymous access is not allowed in this scenario. Actually, it is enabled through the blob or container permission.

Objective:
Develop for Azure storage

Sub-Objective:
Develop solutions that use blob storage

References:

Redgate Hub > Azure Blob Storage Part 9: Shared Access Signatures

Microsoft Docs > Azure > Storage > Grant limited access to Azure Storage resources using shared access signatures (SAS)

Convective > Access Control for Azure Blobs

Question #135 of 135

Question ID: 1287206

You are the administrator of the Nutex Corporation. You have a web application hosted in Azure. You need to set up your project for Application Insights exception reporting for IIS web servers.

Which tasks should you perform?

A) Run an Azure Pipline agent.
B) Add Application Monitoring Extension.
C) Ensure Application Insights Extension site extension is updated.
D) Install the JavaScript snippet in your web pages.
E) Install Application Insights SDK in your app code.

Explanation

To set up exception reporting, you will need the following:

- Ensure Application Insights Extension site extension is updated.
- Add Application Monitoring Extension.
- Install Application Insights SDK in your app code.

You would need to add the Application Monitoring Extension for exception reporting of Azure VMs and Azure virtual machine scale set IIS-hosted apps.

You would ensure that the Application Insights site extension is installed and updated. The extension installation is dependent on you manually updating it. The extension is now part of the App Service image.

To exceptions reported from your server app, you can have either the Applications Insights SDK installed in your app code, run the Application Insights Agent on your IIS web servers, or install the Java agent on your Java web apps.

You would not run Azure Pipeline agents. Azure Pipelines is a service that is used to test your code project and build that project. Azure Pipeline agents are not needed for Application Insights exception reporting.

You do not have to install the JavaScript snippet in your web pages to have exceptions reported from your server app. This action will catch browser exceptions.

Objective:
Monitor, troubleshoot, and optimize Azure solutions

Sub-Objective:
Instrument solutions to support monitoring and logging

References:

Microsoft Azure > Azure Monitor > Diagnose exceptions in your web apps with Application Insights

Microsoft Azure > Azure Monitor > Monitor Azure App Service performance