Custom View Settings

Question #20 *Topic 4*

DRAG DROP -

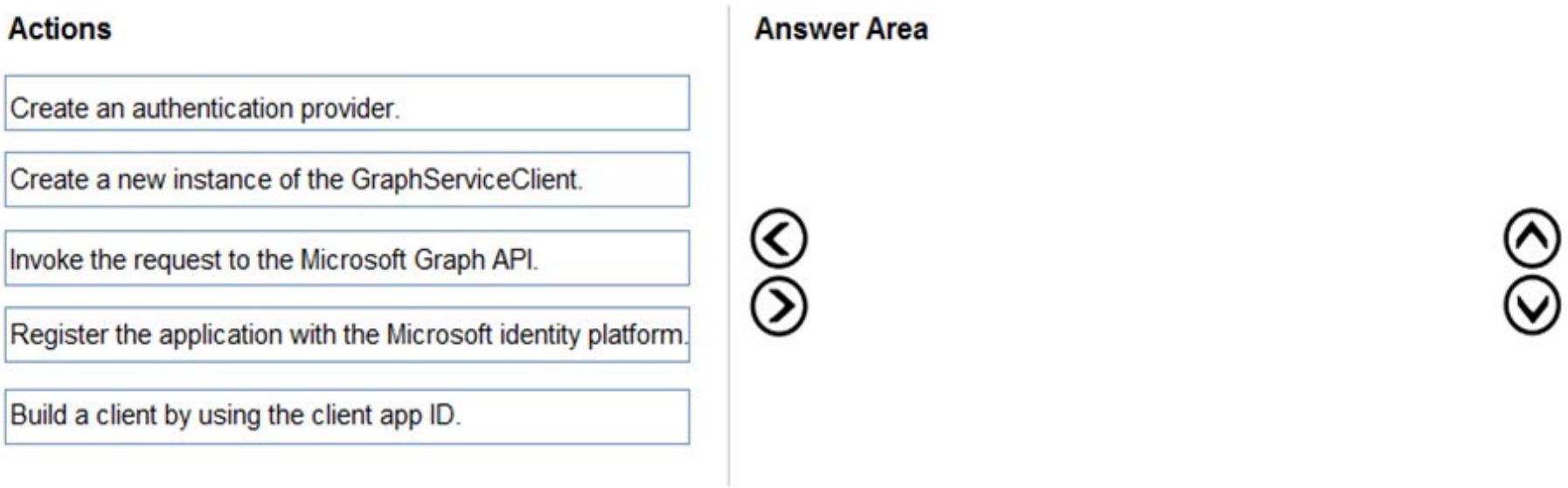
You are developing an application to retrieve user profile information. The application will use the Microsoft Graph SDK.

The app must retrieve user profile information by using a Microsoft Graph API call.

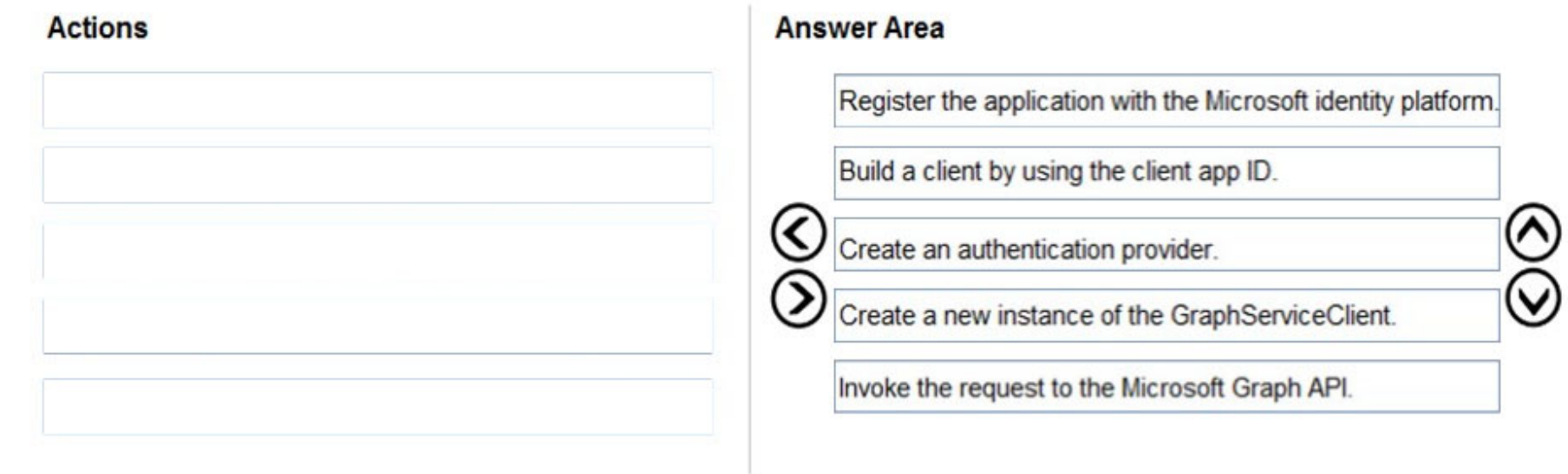
You need to call the Microsoft Graph API from the application.

In which order should you perform the actions? To answer, move all actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place:



Correct Answer:



Step 1: Register the application with the Microsoft identity platform.

To authenticate with the Microsoft identity platform endpoint, you must first register your app at the Azure app registration portal

Step 2: Build a client by using the client app ID

Step 3: Create an authentication provider

Create an authentication provider by passing in a client application and graph scopes.

Code example:

```
DeviceCodeProvider authProvider = new DeviceCodeProvider(publicClientApplication, graphScopes);
// Create a new instance of GraphServiceClient with the authentication provider.
GraphServiceClient graphClient = new GraphServiceClient(authProvider);
```

Step 4: Create a new instance of the GraphServiceClient

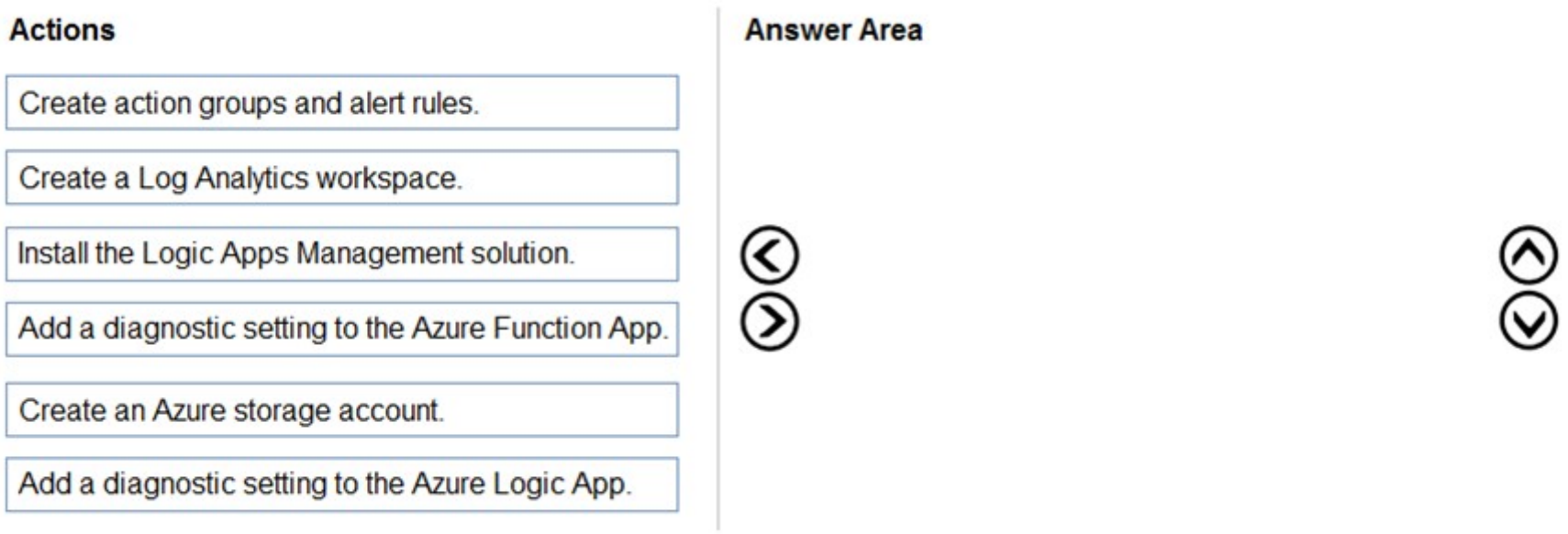
Step 5: Invoke the request to the Microsoft Graph API

Reference:

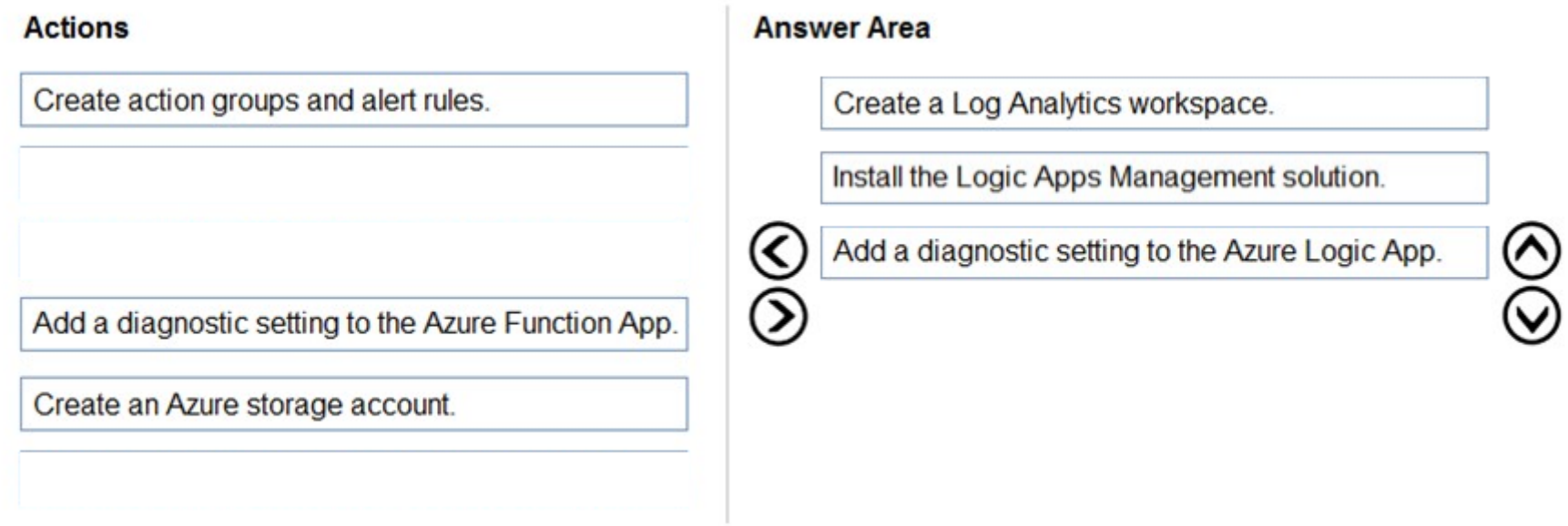
https://docs.microsoft.com/en-us/graph/auth-v2-service
https://docs.microsoft.com/en-us/graph/sdks/create-client

Question #21 *Topic 4*

DRAG DROP -
You develop and deploy an Azure Logic App that calls an Azure Function app. The Azure Function App includes an OpenAPI (Swagger) definition and uses an
Azure Blob storage account. All resources are secured by using Azure Active Directory (Azure AD).
The Logic App must use Azure Monitor logs to record and store information about runtime data and events. The logs must be stored in the Azure Blob storage account.
You need to set up Azure Monitor logs and collect diagnostics data for the Azure Logic App.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.
Select and Place:



Correct Answer:



Step 1: Create a Log Analytics workspace
Before you start, you need a Log Analytics workspace.
Step 2: Install the Logic Apps Management solution
To set up logging for your logic app, you can enable Log Analytics when you create your logic app, or you can install the Logic Apps Management solution in your
Log Analytics workspace for existing logic apps.
Step 3: Add a diagnostic setting to the Azure Logic App

Set up Azure Monitor logs -
1. In the Azure portal, find and select your logic app.
2. On your logic app menu, under Monitoring, select Diagnostic settings > Add diagnostic setting.
Reference:
https://docs.microsoft.com/en-us/azure/logic-apps/monitor-logic-apps-log-analytics

Question #22 *Topic 4*

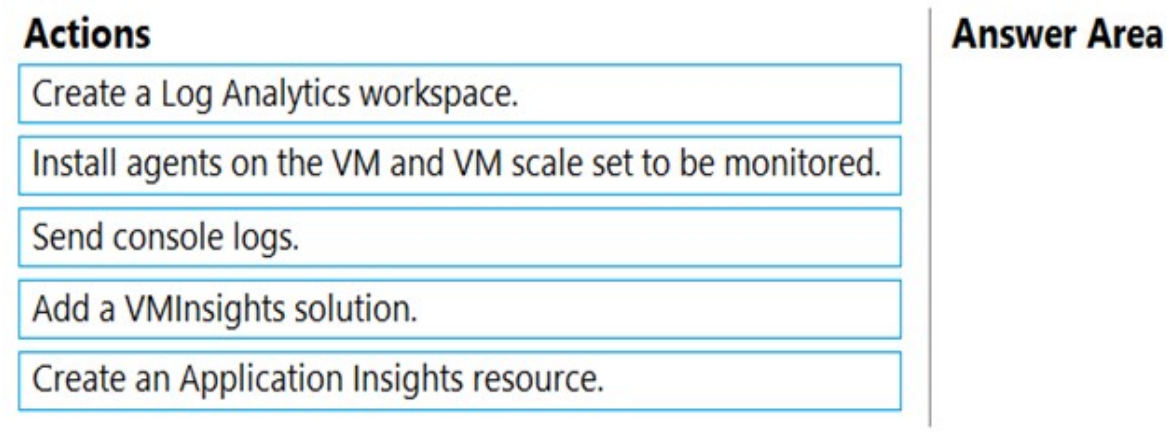
DRAG DROP -

You develop an application. You plan to host the application on a set of virtual machines (VMs) in Azure.

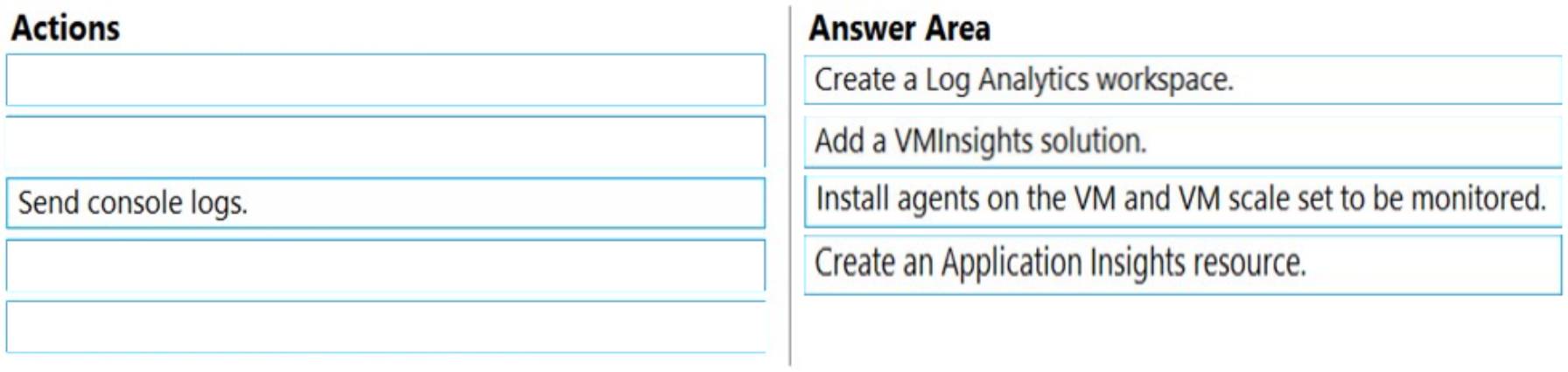
You need to configure Azure Monitor to collect logs from the application.

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

Select and Place:



Correct Answer:



Step 1: Create a Log Analytics workspace.

First create the workspace.

Step 2: Add a VMInsights solution.

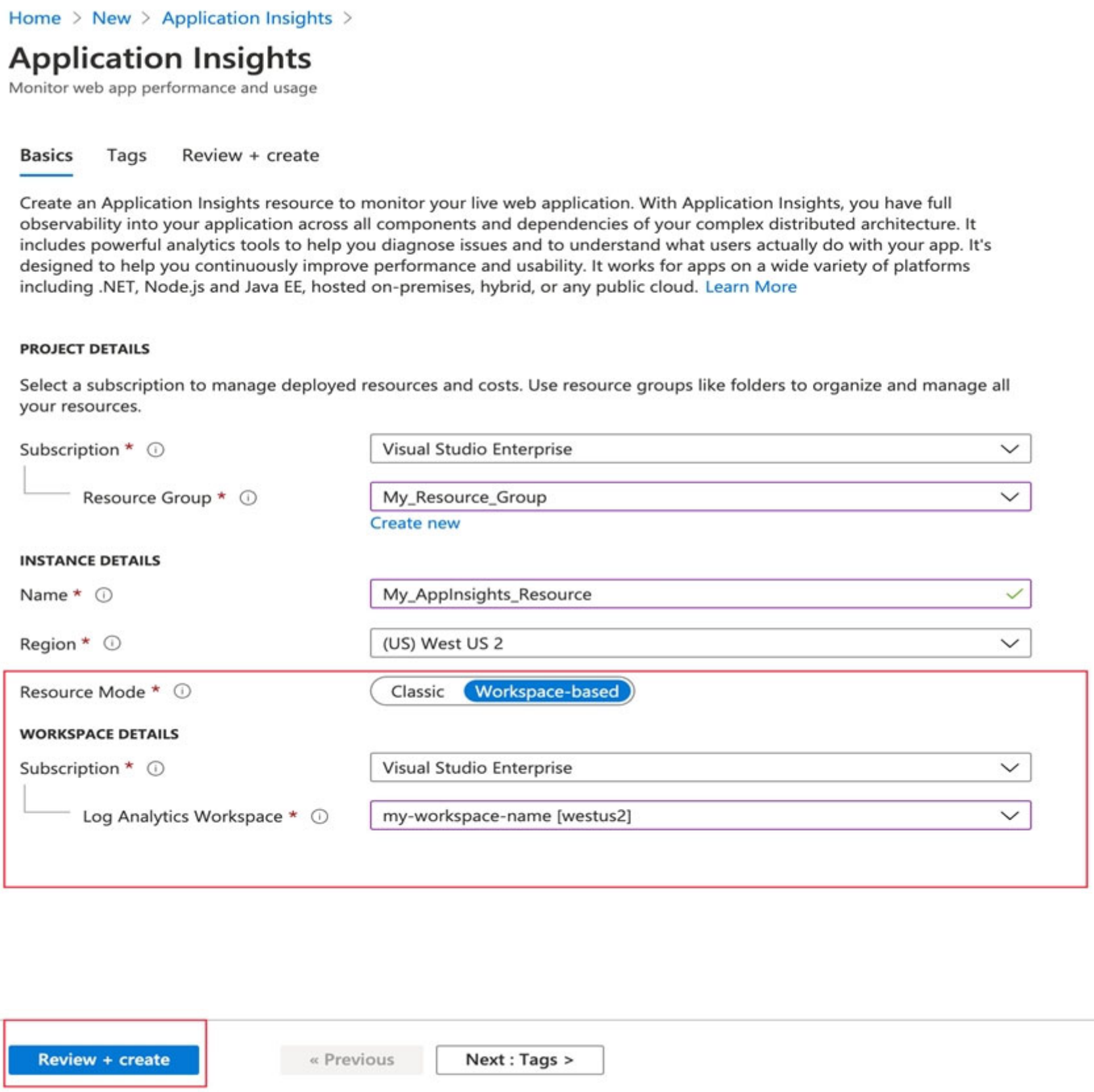
Before a Log Analytics workspace can be used with VM insights, it must have the VMInsights solution installed.

Step 3: Install agents on the VM and VM scale set to be monitored.

Prior to onboarding agents, you must create and configure a workspace. Install or update the Application Insights Agent as an extension for Azure virtual machines and VM scalet sets.

Step 4: Create an Application Insights resource

Sign in to the Azure portal, and create an Application Insights resource.



Once a workspace-based Application Insights resource has been created, configuring monitoring is relatively straightforward.

Reference:

https://docs.microsoft.com/en-us/azure/azure-monitor/vm/vminsights-configure-workspace https://docs.microsoft.com/en-us/azure/azure-monitor/app/create-workspace-resource

Topic 5 - Question Set 5

Question #1 *Topic 5*

DRAG DROP -

You have an application that provides weather forecasting data to external partners. You use Azure API Management to publish APIs.

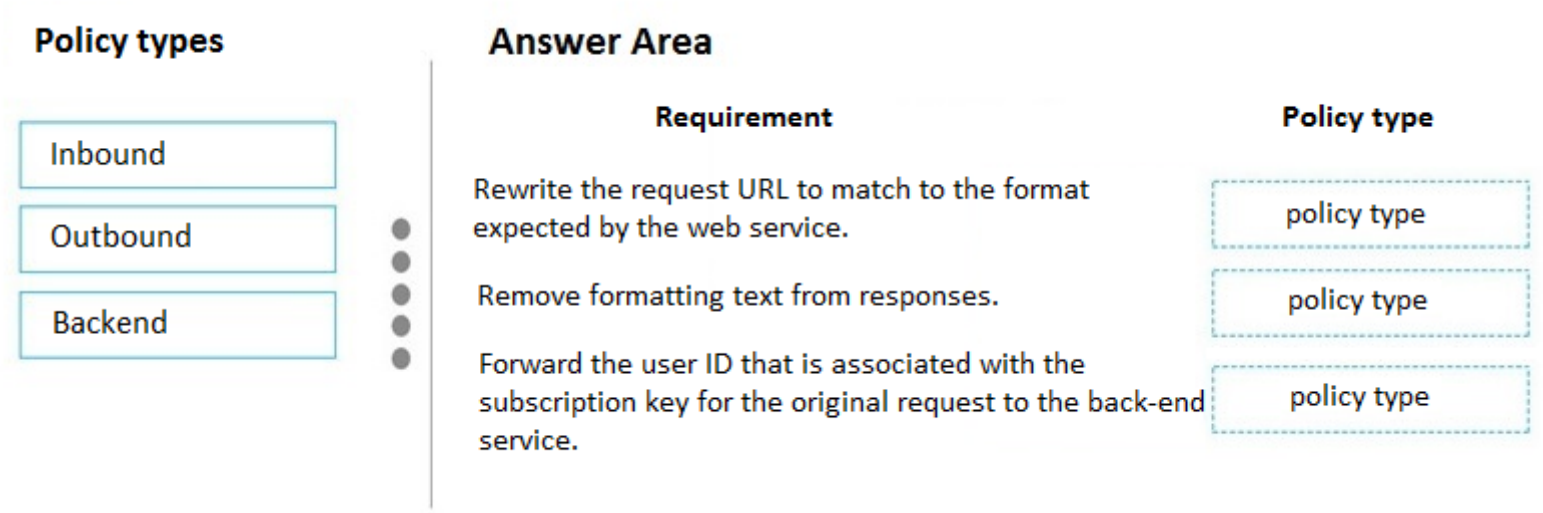
You must change the behavior of the API to meet the following requirements:

- ☞ Support alternative input parameters
- ☞ Remove formatting text from responses
- ☞ Provide additional context to back-end services

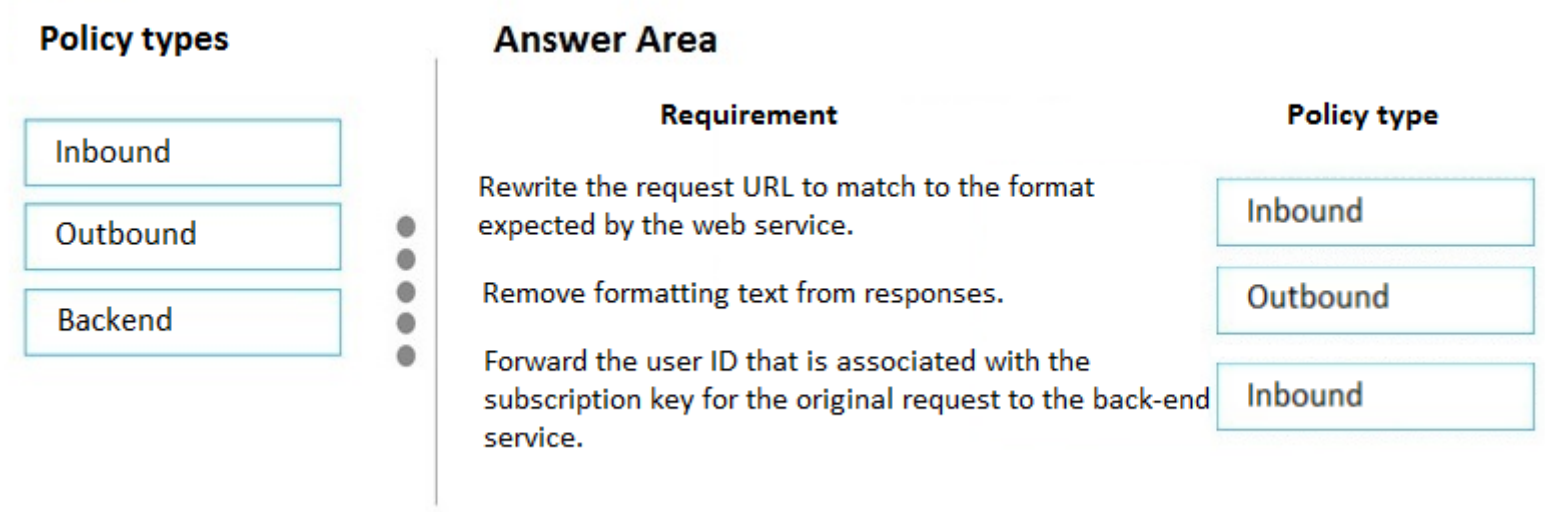
Which types of policies should you implement? To answer, drag the policy types to the correct scenarios. Each policy type may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:



Correct Answer:



Reference:

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

Question #2 *Topic 5*

You are developing an e-commerce solution that uses a microservice architecture.
You need to design a communication backplane for communicating transactional messages between various parts of the solution. Messages must be communicated in first-in-first-out (FIFO) order.
What should you use?

A. Azure Storage Queue

B. Azure Event Hub

C. Azure Service Bus

D. Azure Event Grid

Correct Answer: *A*
As a solution architect/developer, you should consider using Service Bus queues when:
☞ Your solution requires the queue to provide a guaranteed first-in-first-out (FIFO) ordered delivery.
Reference:
https://docs.microsoft.com/en-us/azure/service-bus-messaging/service-bus-azure-and-service-bus-queues-compared-contrasted

Previous Questions Next Questions