**Overview**

CloudPortalHub currently has a social networking site and several applications that work around the networking site.

The following application services have been setup

* Cloud\_Content\_Uploader – This service is used to pick up messages which are stored in Azure Blob storage
* Cloud\_Analysis\_Service – This service process the messages picked up from Azure Blob storage. These messages are checked for any inappropriate content.

Both the Cloud\_Content\_Uploader and Cloud\_ Analysis\_Service are deployed as containers using the Azure Container Instance service.

The Cloud\_ Analysis\_Service uses an Azure Function named Check\_Content that performs the actual content check. The Cloud\_ Analysis\_Service is based on an image named contentimage in an Azure Container registry named production-registry

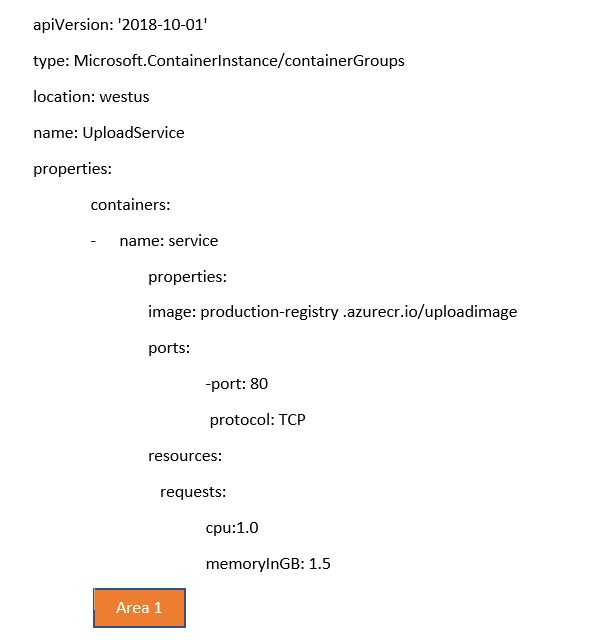
The Azure Function returns a probable value for the content after it has been checked for any inappropriate content. If the value is above a threshold, then the CloudPortalHub employees would need to carry out a manual review of the content.

**Requirements**

Below are the key requirements for the system

* **Manual Review** – To conduct a manual review, the employees would get a web interface , which could be a part of the Cloud\_ Analysis\_Service. This web interface is built using React and all pages and endpoints require authentication. They have to log in using their Azure AD credentials. In order to conduct the review, the employee needs to be part of the “Reviewer” role. All of the completed reviews need to include the reviewer’s email address for auditing purposes.
* **User agreements** – When a user submits content on the social networking site, the user needs to agree to an end user agreement. The end user agreement would allow the company employees to conduct manual reviews and also mention the tracking of the user’s IP address. This information would be used by multiple departments in the CloudPortalHub. The number of agreements is expected to be in millions per hour. The user responses must not be lost and must be available to all parties regardless of the service uptime.
* **Security** – The following security requirements needs to be adhered to
  + All of the websites and services must use SSL from a valid root certificate authority
  + All Internal services must be accessible from Internal Virtual Networks
  + All services must be authenticated using Azure AD
  + Azure Storage access keys must be stored in memory and must be available only to the service
* **Monitoring** – The Cloud\_Content\_Uploader service must be monitored. Alerts must be raised if the CPU percentage utilization goes beyond 80%.
* **High Availability** – All services must run in multiple regions. If there is a service failure in any region, it must not impact the overall application availability.
* **Testing** – When a new version of the Cloud\_Analysis\_Service is available, it must first be available for seven days for testing.

**Below is the code for the Cloud\_Content\_Uploader deployment**







**Below is the app manifest file for Cloud\_ Analysis\_Service**

{

"id" : "28c9bdfa-45e8-453c-9804-47bf0d48e664"

"appId" : "01eefe48-04c1-44e9-bc61-02bcb1abb453"

"createdDateTime": "2020-06-14T11:13:49Z",

"logoUrl": null,

"logoutUrl"null,

"name" : "CloudAnalysisService",

"orgRestrictions": [],

"parentalControlSettings": {

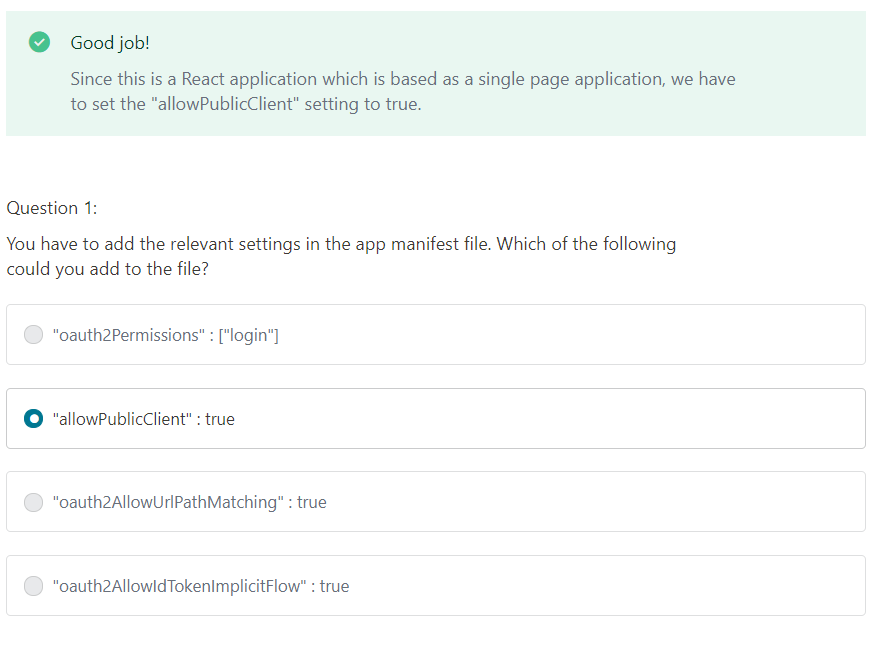
"countriesBlockedForMinors": [],

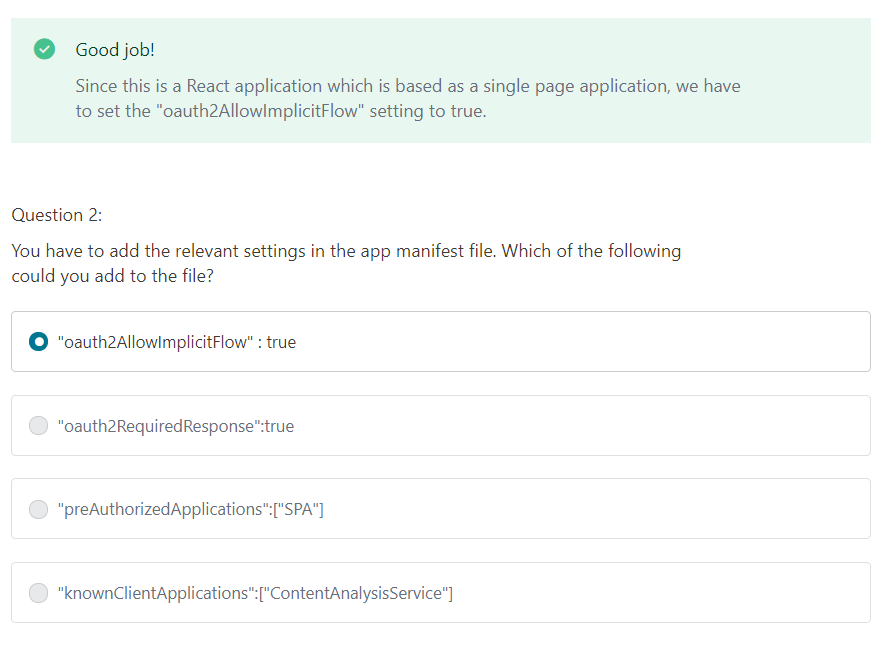
"legalAgeGroupRule": "Allow"

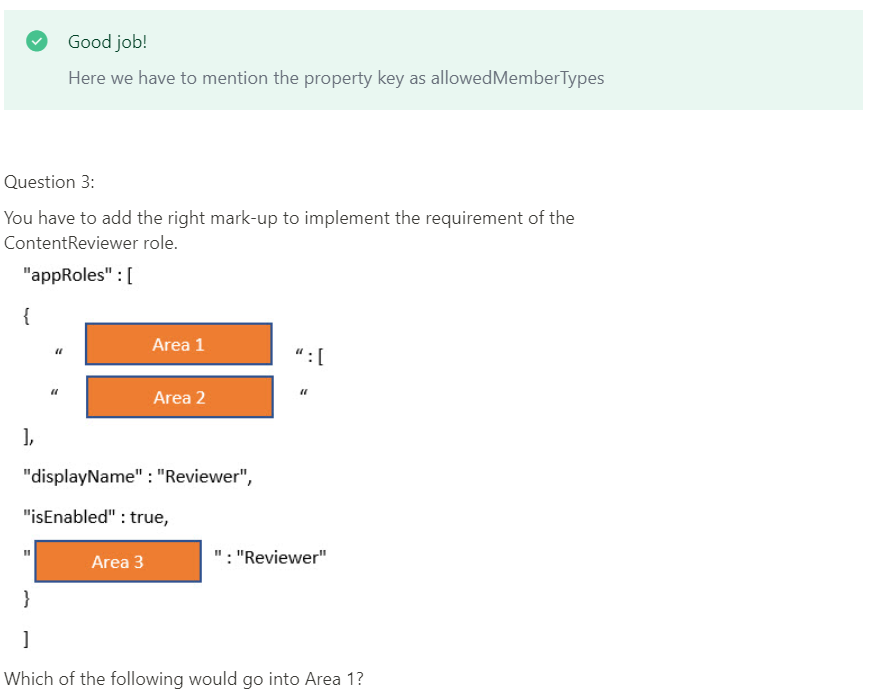
},

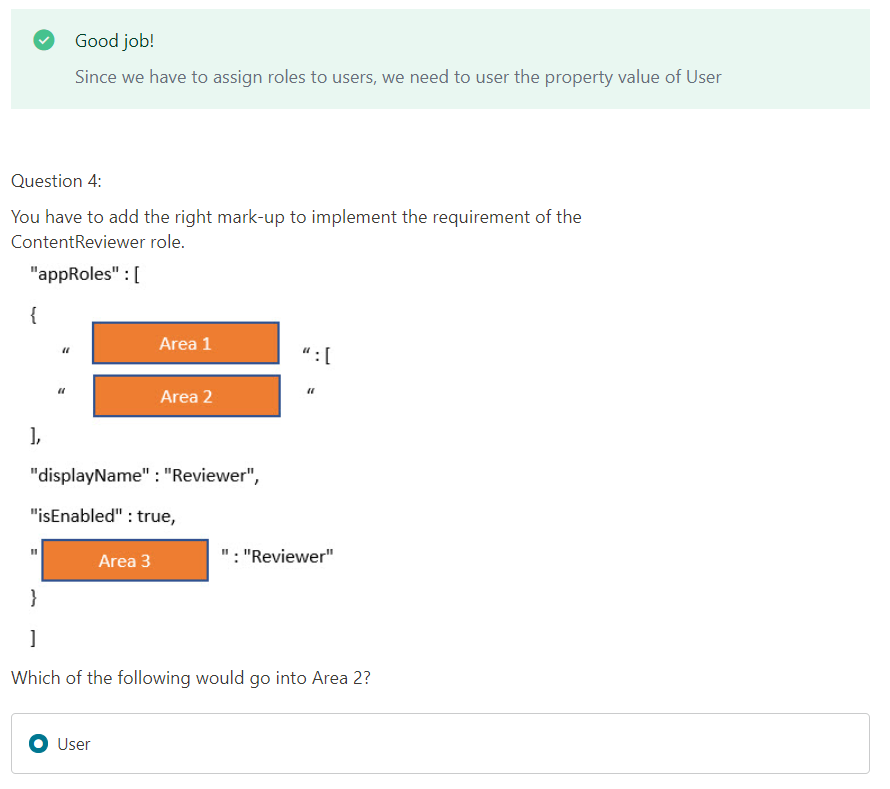
"passwordCredentials": []

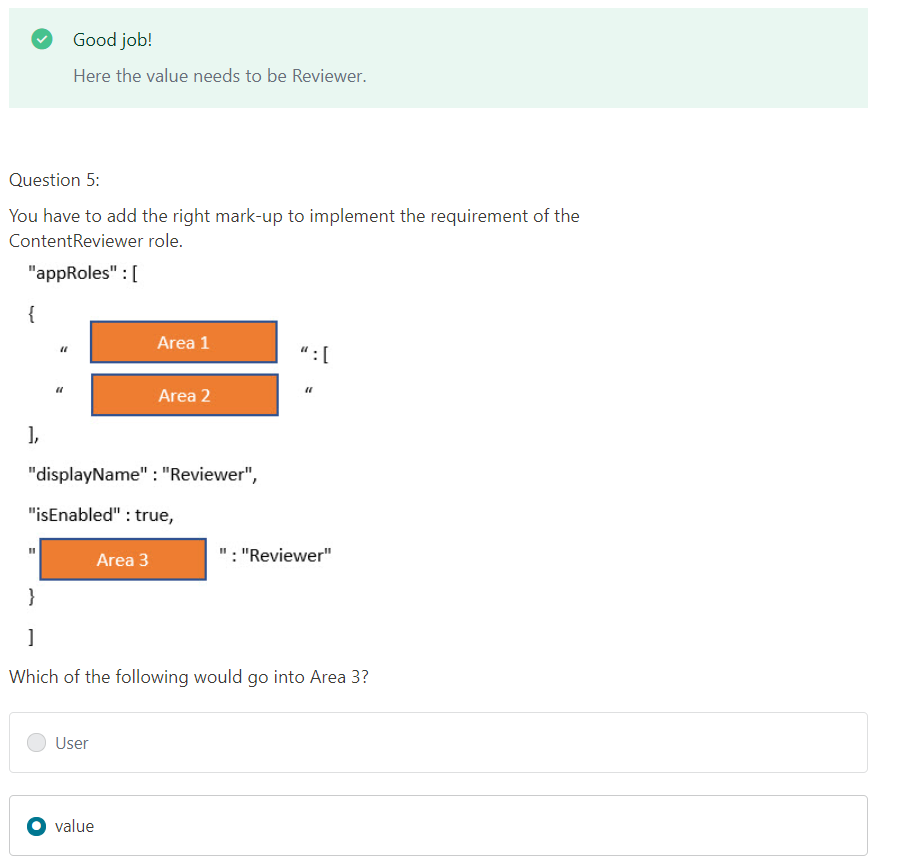
}

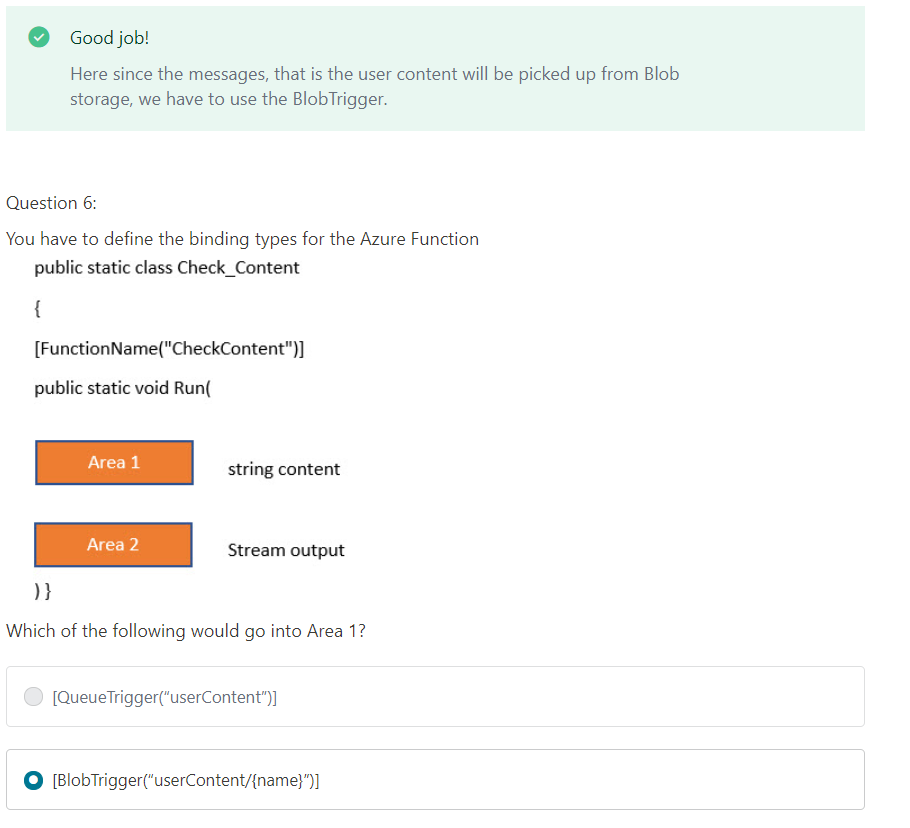


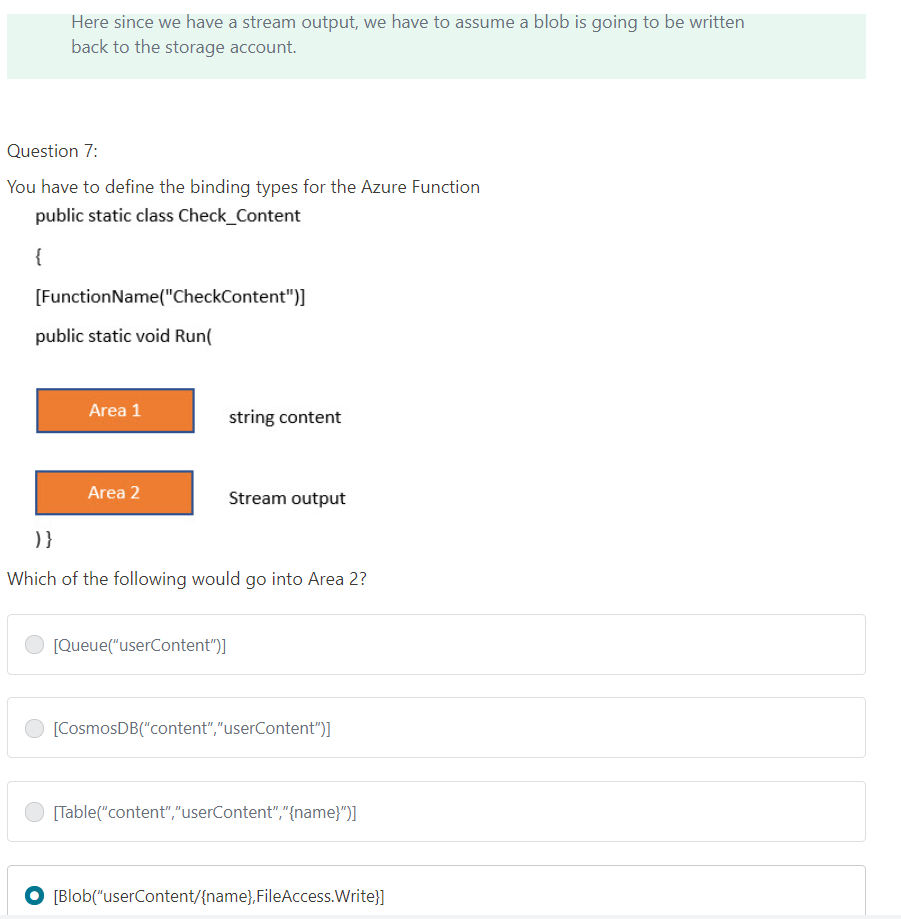


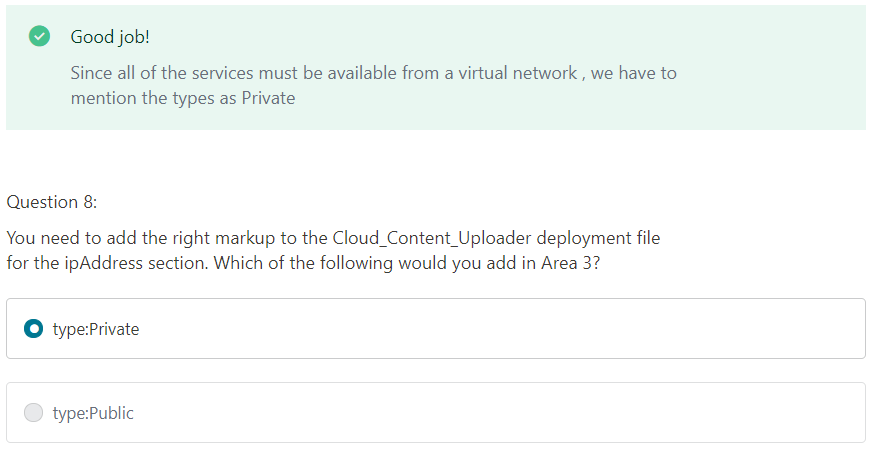


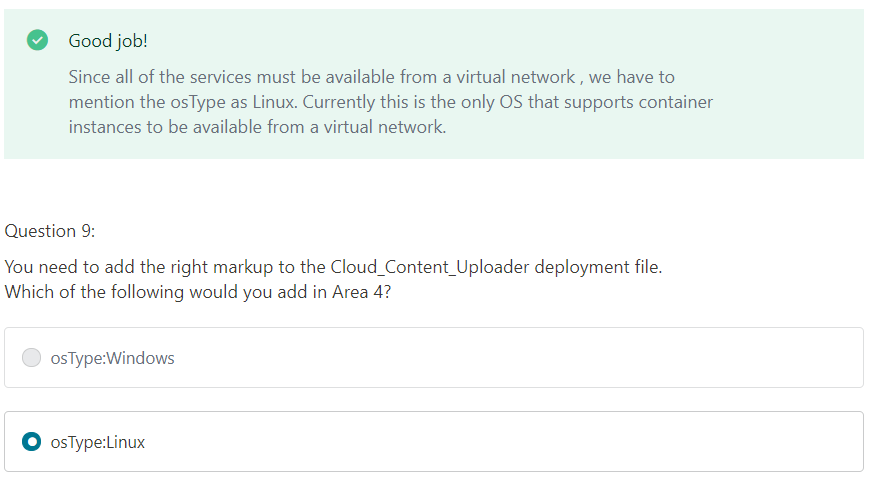


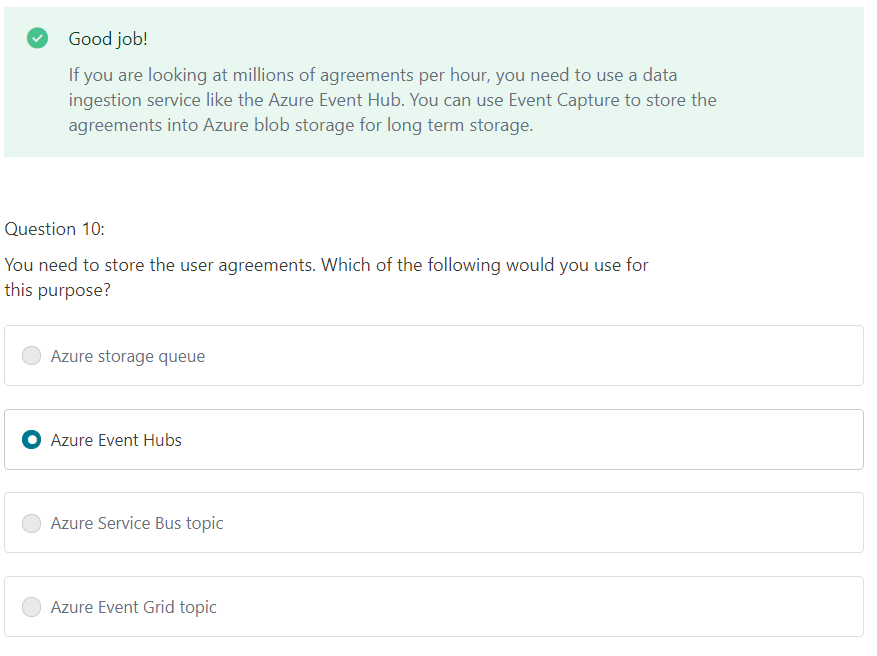


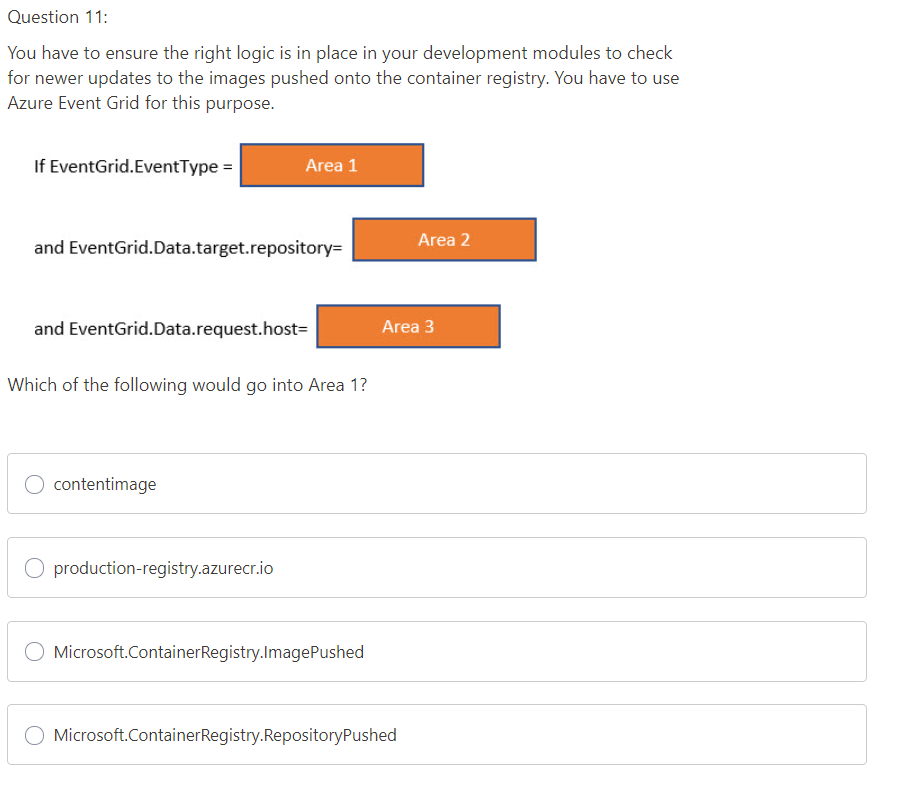












1= Imagepushed, 2=contentimage , 3= hostname

