Free Questions for AZ-400 by certscare

Shared by Crawford on 22-07-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Task 2

You need to create an instance of Azure Application Insights named az400-38443478-main and configure the instance to receive telemetry data from an Azure web app named az400-38443478-main

You must create a Log Analytics workspace before this task.

Options:

A- See the solution below in explanation

Answer:

A

Explanation:

To create an instance of Azure Application Insights named az400-38443478-main and configure it to receive telemetry data from an Azure web app with the same name, you'll need to follow these steps:

Create a Log Analytics Workspace:

Go to the Azure Portal.

Search for Log Analytics Workspaces and select Add.

Select a Subscription and either use an existing Resource Group or create a new one.

Provide a unique name for your Log Analytics workspace.

Choose the Region that is appropriate for you.

Review the settings and then select Create1.

Create an Azure Application Insights Instance:

In the Azure Portal, navigate to Application Insights.

Click on + Create.

Fill in the instance details, ensuring the name is az400-38443478-main.

Link the instance to the Log Analytics workspace you created in the previous step.

Review and create the Application Insights instance2.

Configure the Azure Web App to Send Telemetry Data:

Go to the Azure Web App az400-38443478-main.

Under Monitoring, select Application Insights.

Choose to use an existing resource and select the Application Insights instance you created.

Follow the prompts to set up the connection, which may involve adding the appropriate SDK to your web app and configuring the connection string or instrumentation key.

Verify Telemetry Data Reception:

After setting up, send some test traffic to your web app.

Then, go to the Application Insights instance and check the Overview or Performance sections to see if telemetry data is being received.

Remember to replace placeholder names with the actual names of your resources where necessary. These steps will help you set up Azure Application Insights to monitor your web app effectively.

Question 2

Question Type: **MultipleChoice**

Task 1

You need to ensure that an Azure Web App named az400-38443478-main can retrieve secrets from an Azure key vault named az400-3844J478-kv1 by using a system managed identity The solution must use the principle of least privilege.

Options:

A- See the solution below in explanation

Answer:

A

Explanation:

To ensure that your Azure Web App named az400-38443478-main can retrieve secrets from an Azure Key Vault named az400-3844J478-kv1 using a system managed identity with the principle of least privilege, follow these detailed steps:

Enable a System Managed Identity for the Azure Web App:

Navigate to the Azure Portal.

Go to the Azure Web App az400-38443478-main.

Select Identity under the Settings section.

In the System assigned tab, switch the Status to On.

Click Save to apply the changes.

Grant the Web App Access to the Key Vault:

Go to the Azure Key Vault az400-3844J478-kv1.

Select Access policies under the Settings section.

Click on Add Access Policy.

Choose Secret permissions and select Get and List. This grants the app the ability to read secrets, adhering to the principle of least privilege.

Click on Select principal, search for your Web App name az400-38443478-main, and select it.

Click Add to add the policy.

Don't forget to click Save to save the access policy changes.

Retrieve Secrets in the Web App Code:

In your Web App's code, use the Azure SDK to retrieve the secrets.

For example, in a .NET application, you can use the Azure.Identity and Azure.Security.KeyVault.Secrets namespaces.

Utilize the DefaultAzureCredential class which will automatically use the system managed identity when running on Azure.

```
using Azure.Identity;

using Azure.Security.KeyVault.Secrets;
```

```
var client = new SecretClient(new Uri('https://az400-3844J478-kv1.vault.azure.net/'), new DefaultAzureCredential());

KeyVaultSecret secret = await client.GetSecretAsync('my-secret-name');

string secretValue = secret.Value;
```

Replace 'my-secret-name' with the actual name of the secret you want to retrieve.

By following these steps, your Azure Web App will be able to securely retrieve secrets from the Azure Key Vault using a system managed identity, without needing to store credentials in the code, and adhering to the principle of least privilege. Remember to replace the placeholder names with the actual names of your Web App and Key Vault.

Question 3

Question Type: **DragDrop**

You have an Azure subscription that contains a project in Azure DevOps named Project1. In Microsoft Azure Active Directory (Azure AD), part of Microsoft Entr

a. you have three users that require access to Project! as shown in the following table.

Name	Title	Requirement
Build Administrators	ect Manager	View repositories.
Contributors	elopment Lead	Create repositories and manage permissions.
Project Administrators	Developer	Create branches and tags.
Readers		

s. The solution must use the principle of least privilege.

user? To answer, drag the appropriate permission groups to the
n once, or not at all. You may need to drag the split bar between

correct selection is worth one point.

Permission Groups

Build Administrators s

Contributors s

Project Administrators rs

Readers

Answer Area

User1:

User2:

User3:

Answer:

Question 4

Question Type: Hotspot

You have an Azure subscription that contains a user named User1.

You have an Azure Resource Manager (ARM) template named Template 1.

You plan to perform the following actions:

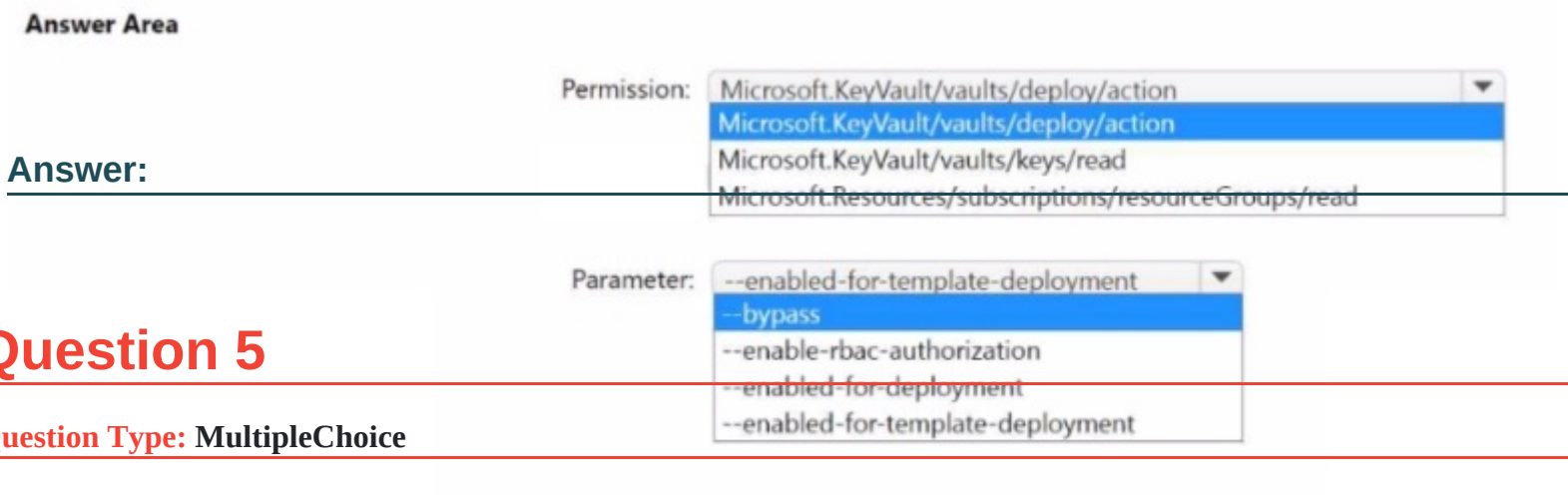
* Deploy an Azure key vault named KV1.

* Deploy Azure resources by using Template1 to retrieve secrets from KV1

You need to ensure that User1 can deploy Template1 The solution must follow the principle of least privilege.

Which permission should you grant to User1, and which parameter should be specified when you create KV1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer:

Question 5

Question Type: MultipleChoice

You use Azure Pipelines to build and deploy an app named Appl. You plan to monitor App1 by using Application Insights. You create an Application Insights instance named All. You need to configure App1 to use All. Which file should you modify?

Options:

A- appsettings.son

B- launchSettings.json

C- startup.cs

D- project.son

Answer:

A

Question 6

Question Type: **DragDrop**

You have a tendril in Microsoft Azure Active Directory (Azure AD), part of Microsoft Entr

a. The tenant contains three groups named Group1. Group2, and Group3.

You create a new project in Azure DevOps named Project1.

You need to secure the service connections for Project1. The solution must meet the following requirements:

* The members of Group1 must be able to share and unshare a service connection with other projects.

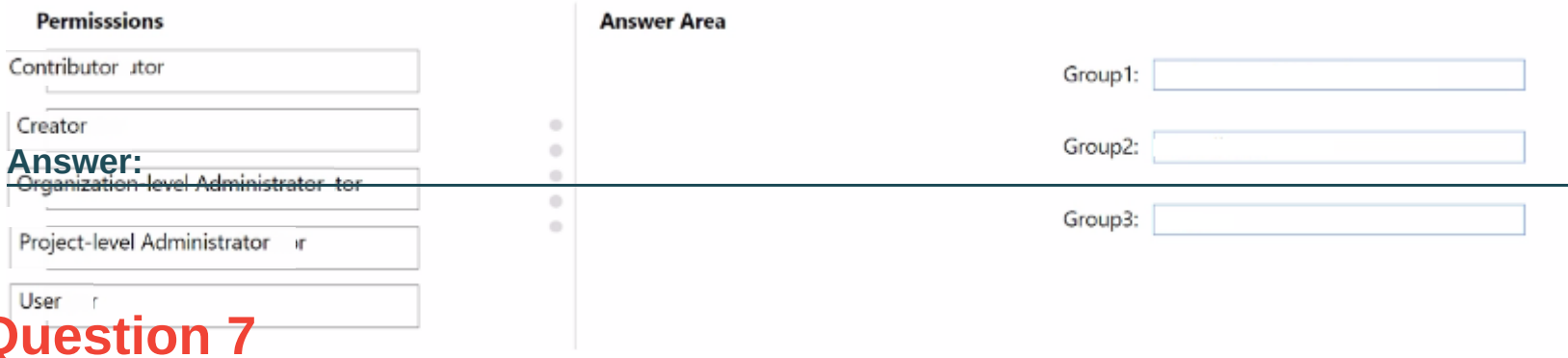
* The members of Group2 must be able to rename a service connection and update the description.

* The members of Group3 must be able to use the service connection within build or release pipelines.

* The principle of least privilege must be followed.

Which permission should you grant to each group? To answer, drag the appropriate permissions to the correct groups. Each permission 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.



Answer:

Question 7

Question Type: MultipleChoice

You use Git for source control.

You enable GitHub code scanning.

You raise a pull request from a non-default branch. In the code scanning output you receive the following error message: "Analysis not found."

You need to ensure that the code scanning completes successfully for the pull request.

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

NOTE: Each correct selection is worth one point.

Options:

A- Add a new workflow for code scanning.

B- Add the name of the non-default branch to the on: push specification in the code scanning workflow.

C- Update the code in the pull request.

D- Add the name of the default branch to the on: push specification in the code scanning workflow.

E- Delete the pull request, and then raise the request again from the default branch.

Answer:

C, D

Question 8

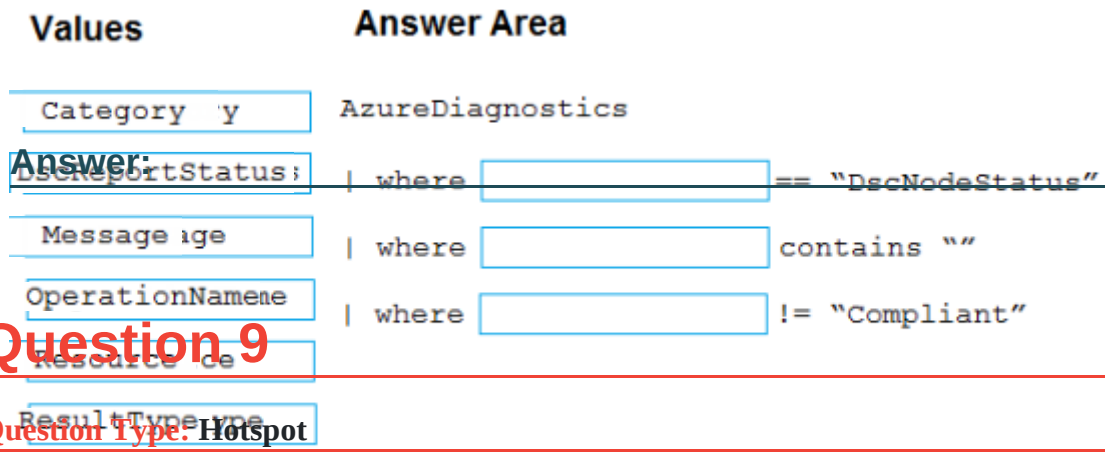
Question Type: **DragDrop**

You have an Azure subscription that uses Azure Automation State Configuration to manage the configuration of virtual machines.

You need to identify which nodes are noncompliant.

How should you complete the query? To answer, drag the appropriate values to the correct targets. Each value 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.



Answer:

Question 9

Question Type: Hotspot

You have a virtual machine that runs Windows Server 2019 and is managed by using Desired State Configuration (DSC).

You have the following DSC configuration.

```
configuration WebConfiguration
{
 LocalConfigurationManager
 {
     ConfigurationMode = "ApplyAndMonitor"
```

wise, select No.

Statements	Yes	No
The Index.htm file will be copied to the C:\Test folder before the Web-Server Windows feature is installed.	○	○
If manual changes are made to the configuration of the virtual machine, the configuration will reapply automatically.	○	○
If the Web-Server Windows feature is uninstalled from the virtual machine, the discrepancy will be reported in a log entry within 60 minutes.	○	○

Answer:

Question 10

Question Type: MultipleChoice

You have an on-premises app named App1 that accesses Azure resources by using credentials stored in a configuration file.

You plan to upgrade App1 to use an Azure service principal.

What is required for App1 to programmatically sign in to Azure Active Directory (Azure AD)?

Options:

A- the application ID, a client secret, and the object ID

B- a client secret, the object ID, and the tenant ID

C- the application ID, a client secret, and the tenant ID

D- the application ID, a client secret, and the subscription ID

Answer:

C

Explanation:

https://docs.microsoft.com/en-us/azure/active-directory/develop/app-objects-and-service-principals 'When you've completed the app registration, you've a globally unique instance of the app (the application object) which lives within your home tenant or directory. You also have a globally unique ID for your app (the app or client ID). In the portal, you can then add secrets or certificates and scopes to make your app work, customize the branding of your app in the sign-in dialog, and more.'