Free Questions for AZ-500 by dumpssheet

Shared by Cline on 09-08-2024

Question 1

Question Type: MultipleChoice

Use the following login credentials as needed:

To enter your username, place your cursor in the Sign in box and click on the username below.

To enter your password, place your cursor in the Enter password box and click on the password below.

Azure Username: User1-10598168@ExamUsers.com

Azure Password: Ag1Bh9!#Bd

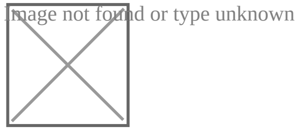
The following information is for technical support purposes only:

Lab Instance: 10598168

Image not found or type unknown

Image not found or type unknown

Image not found or type unknown



The developers at your company plan to create a web app named App10598168 and to publish the app to https://www.contoso.com.

You need to perform the following tasks:

Ensure that App10598168 is registered to Azure Active Directory (Azure AD).

Generate a password for App10598168.

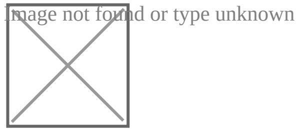
To complete this task, sign in to the Azure portal.

Options:

A) Explanation:

Step 1: Register the Application

1. Sign in to your Azure Account through the Azure portal.
2. Select Azure Active Directory.
3. Select App registrations.
4. Select New registration.



6. Click Register

Step 2: Create a new application secret

If you choose not to use a certificate, you can create a new application secret.

7 Select Certificates & secrets.

8. Select Client secrets -> New client secret.

9. Provide a description of the secret, and a duration. When done, select Add.

After saving the client secret, the value of the client secret is displayed. Copy this value because you aren't able to retrieve the key later.

You provide the key value with the application ID to sign in as the application. Store the key value where your application can retrieve it.

Answer:

A

Explanation:

https://docs.microsoft.com/en-us/azure/active-directory/develop/howto-create-service-principal-portal

Question 2

Question Type: **MultipleChoice**

Use the following login credentials as needed:

To enter your username, place your cursor in the Sign in box and click on the username below.

To enter your password, place your cursor in the Enter password box and click on the password below.

Azure Username: User1-10598168@ExamUsers.com

Azure Password: Ag1Bh9!#Bd

The following information is for technical support purposes only:

Lab Instance: 10598168

Image not found or type unknown

Image not found or type unknown

Image not found or type unknown

Image not found or type unknown

You need to collect all the audit failure data from the security log of a virtual machine named VM1 to an Azure Storage account.

To complete this task, sign in to the Azure portal.

This task might take several minutes to complete You can perform other tasks while the task completes.

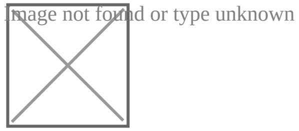
Options:

A) Explanation:

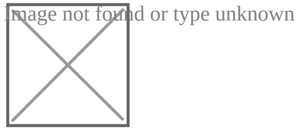
Step 1: Create a workspace

Azure Monitor can collect data directly from your Azure virtual machines into a Log Analytics workspace for detailed analysis and correlation.

1. In the Azure portal, select All services. In the list of resources, type Log Analytics. As you begin typing, the list filters based on your input. Select Log Analytics workspaces.



2. Select Create, and then select choices for the following items:



3. After providing the required information on the Log Analytics workspace pane, select OK.

While the information is verified and the workspace is created, you can track its progress under Notifications from the menu.

Step 2: Enable the Log Analytics VM Extension

Installing the Log Analytics VM extension for Windows and Linux allows Azure Monitor to collect data from your Azure VMs.

1. In the Azure portal, select All services found in the upper left-hand corner. In the list of resources, type Log Analytics. As you begin

typing, the list filters based on your input. Select Log Analytics workspaces.
2. In your list of Log Analytics workspaces, select DefaultWorkspace (the name you created in step 1).
3. On the left-hand menu, under Workspace Data Sources, select Virtual machines.
4. In the list of Virtual machines, select a virtual machine you want to install the agent on. Notice that the Log Analytics connection status for the VM indicates that it is Not connected.
5. In the details for your virtual machine, select Connect. The agent is automatically installed and configured for your Log Analytics workspace. This process takes a few minutes, during which time the Status shows Connecting.
After you install and connect the agent, the Log Analytics connection status will be updated with This workspace.

Answer:

A

Question 3

Question Type: **MultipleChoice**

Use the following login credentials as needed:

To enter your username, place your cursor in the Sign in box and click on the username below.

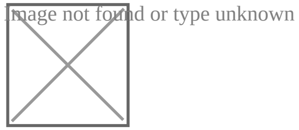
To enter your password, place your cursor in the Enter password box and click on the password below.

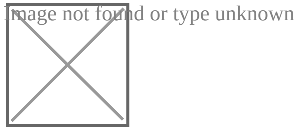
Azure Username: User1-10598168@ExamUsers.com

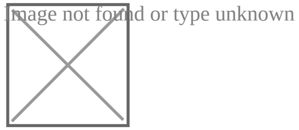
Azure Password: Ag1Bh9!#Bd

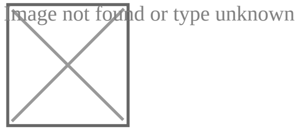
The following information is for technical support purposes only:

Lab Instance: 10598168









You need to email an alert to a user named admin1@contoso.com if the average CPU usage of a virtual machine named VM1 is greater than 70 percent for a period of 15 minutes.

To complete this task, sign in to the Azure portal.

Options:

A) Explanation:

Create an alert rule on a metric with the Azure portal

1. In the portal, locate the resource, here VM1, you are interested in monitoring and select it.
2. Select Alerts (Classic) under the MONITORING section. The text and icon may vary slightly for different resources.
3. Select the Add metric alert (classic) button and fill in the fields as per below, and click OK.

Metric: CPU Percentage

Condition: Greater than

Period: Over last 15 minutes

Notify via: email

Additional administrator email(s): admin1@contoso.com

Image not found or type unknown

Answer:

A

Explanation:

https://docs.microsoft.com/en-us/azure/sql-database/sql-database-insights-alerts-portal

Question 4

Question Type: **MultipleChoice**

Use the following login credentials as needed:

To enter your username, place your cursor in the Sign in box and click on the username below.

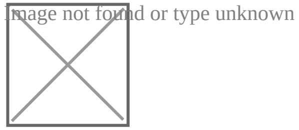
To enter your password, place your cursor in the Enter password box and click on the password below.

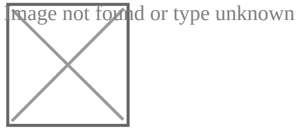
Azure Username: User1-10598168@ExamUsers.com

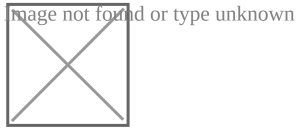
Azure Password: Ag1Bh9!#Bd

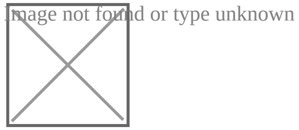
The following information is for technical support purposes only:

Lab Instance: 10598168









You need to ensure that only devices connected to a 131.107.0.0/16 subnet can access data in the rg1lod10598168 Azure Storage account.

To complete this task, sign in to the Azure portal.

Options:

A) Explanation:

Step 1:

1. In Azure portal go to the storage account you want to secure. Here: rg1lod10598168
2. Click on the settings menu called Firewalls and virtual networks.
3. To deny access by default, choose to allow access from Selected networks. To allow traffic from all networks, choose to allow access from All networks.
4. Click Save to apply your changes.

Step 2:

1. Go to the storage account you want to secure. Here: rg1lod10598168
2. Click on the settings menu called Firewalls and virtual networks.
3. Check that you've selected to allow access from Selected networks.
4. To grant access to a virtual network with a new network rule, under Virtual networks, click Add existing virtual network, select Virtual networks and Subnets options. Enter the 131.107.0.0/16 subnet and then click Add.

Note: When network rules are configured, only applications requesting data over the specified set of networks can access a storage account. You can limit access to your storage account to requests originating from specified IP addresses, IP ranges or from a list of subnets in an Azure Virtual Network (VNet).

Answer:

A

Explanation:

https://docs.microsoft.com/en-us/azure/storage/common/storage-network-security

Question 5

Question Type: MultipleChoice

You need to ensure that web11597200 is protected from malware by using Microsoft Antimalware for Virtual Machines and is scanned every Friday at 01:00.

To complete this task, sign in to the Azure portal.

Options:

A) Explanation:

You need to install and configure the Microsoft Antimalware extension on the virtual machine named web11597200.

In the Azure portal, type Virtual Machines in the search box, select Virtual Machines from the search results then select web11597200.

Alternatively, browse to Virtual Machines in the left navigation pane.

In the properties of web11597200, click on Extensions.

Click the Add button to add an Extension.

Scroll down the list of extensions and select Microsoft Antimalware.

Click the Create button. This will open the settings pane for the Microsoft Antimalware Extension.

In the Scan day field, select Friday.

In the Scan time field, enter 60. The scan time is measured in minutes after midnight so 60 would be 01:00, 120 would be 02:00 etc.

Click the OK button to save the configuration and install the extension.

Answer:

A

Question 6

Question Type: MultipleChoice

You need to configure a Microsoft SQL server named Web11597200 only to accept connections from the Subnet0 subnet on the VNET01 virtual network.

To complete this task, sign in to the Azure portal.

Options:

A) Explanation:

You need to allow access to Azure services and configure a virtual network rule for the SQL Server.

In the Azure portal, type SQL Server in the search box, select SQL Server from the search results then select the server named web11597200. Alternatively, browse to SQL Server in the left navigation pane.

In the properties of the SQL Server, click Firewalls and virtual networks.

In the Virtual networks section, click on Add existing. This will open the Create/Update virtual network rule window.

Give the rule a name such as Allow_VNET01-Subnet0 (it doesn't matter what name you enter for the exam).

In the Virtual network box, select VNET01.

In the Subnet name box, select Subnet0.

Click the OK button to save the rule.

Back in the Firewall / Virtual Networks window, set the Allow access to Azure services option to On.

Answer:

A

Question 7

Question Type: **MultipleChoice**

You need to ensure that a user named Danny11597200 can sign in to any SQL database on a Microsoft SQL server named web11597200 by using SQL Server Management Studio (SSMS) and Azure Active Directory (Azure AD) credentials.

To complete this task, sign in to the Azure portal.

Options:

A) Explanation:
You need to provision an Azure AD Admin for the SQL Server.
In the Azure portal, type SQL Server in the search box, select SQL Server from the search results then select the server named web11597200. Alternatively, browse to SQL Server in the left navigation pane.
In the SQL Server properties page, click on Active Directory Admin.
Click the Set Admin button.
In the Add Admin window, search for and select Danny11597200.
Click the Select button to add Danny11597200.
Click the Save button to save the changes.

Answer:

A

Explanation:

https://docs.microsoft.com/en-us/azure/azure-sql/database/authentication-aad-configure?tabs=azure-powershell

Question 8

Question Type: **MultipleChoice**

You need to prevent administrators from performing accidental changes to the Homepage app service plan.

To complete this task, sign in to the Azure portal.

Options:

A) Explanation:

You need to configure a 'lock' for the app service plan. A read-only lock ensures that no one can make changes to the app service plan without first deleting the lock.

In the Azure portal, type App Service Plans in the search box, select App Service Plans from the search results then select Homepage.

Alternatively, browse to App Service Plans in the left navigation pane.

In the properties of the app service plan, click on Locks.

Click the Add button to add a new lock.

Enter a name in the Lock name field. It doesn't matter what name you provide for the exam.

For the Lock type, select Read-only.

Click OK to save the changes.

Answer:

A