AZ-104Q&As

Microsoft Azure Administrator

Pass Microsoft AZ-104 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.leads4pass.com/az-104.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Microsoft Official Exam Center

QUESTION 1

You have an Azure subscription named Subscription1 and two Azure Active Directory (Azure AD) tenants named Tenant1 and Tenant2.

Subscription1 is associated to Tenant1. Multi-factor authentication (MFA) is enabled for all the users in Tenant1.

You need to enable MFA for the users in Tenant2. The solution must maintain MFA for Tenant1.

What should you do first?

A. Change the directory for Subscription1.

B. Configure the MFA Server setting in Tenant1.

C. Create and link a subscription to Tenant2.

D. Transfer the administration of Subscription1 to a global administrator of Tenant2.

Correct Answer: C

QUESTION 2

HOTSPOT

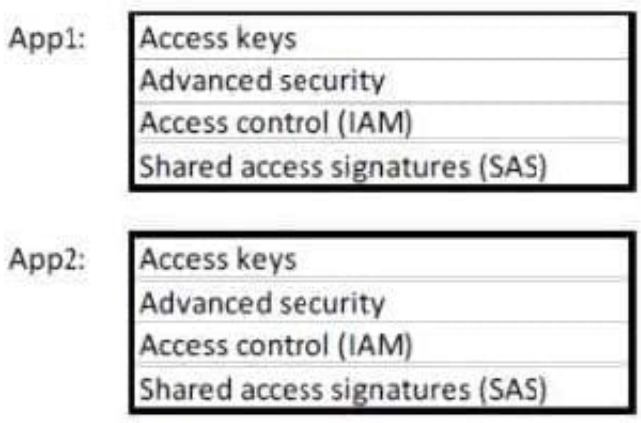
You have an Azure Storage account named storage1.

You have an Azure App Service app named app1 and an app named App2 that runs in an Azure container instance. Each app uses a managed identity.

You need to ensure that App1 and App2 can read blobs from storage1 for the next 30 days.

What should you configure in storage1 for each app?

Hot Area:



Correct Answer:

With Shared access signature you can limit the resources for access and at the same time can control the duration of the access.

A shared access signature (SAS) provides secure delegated access to resources in your storage account without compromising the security of your data. With a SAS, you have granular control over how a client can access your data. You can

control what resources the client may access, what permissions they have on those resources, and how long the SAS is valid, among other parameters.

Reference:

https://docs.microsoft.com/en-us/azure/storage/common/storage-sas-overview

---

QUESTION 3

You have an Azure tenant that contains two subscriptions named Subscription1 and Subscription2.

In Subscription1, you deploy a virtual machine named Server1 that runs Windows Server 2016. Server1 uses managed disks.

You need to move Server1 to Subscription2. The solution must minimize administration effort.

What should you do first?

A. In Subscription2, create a copy of the virtual disk.

B. From Azure PowerShell, run the Move-AzureRmResource cmdlet.

C. Create a snapshot of the virtual disk.

D. Create a new virtual machine in Subscription2.

Correct Answer: B

To move existing resources to another resource group or subscription, use the Move- AzureRmResource cmdlet.

References:

https://docs.microsoft.com/en-in/azure/azure-resource-manager/resource-group-move- resources#moveresources

QUESTION 4

You have an Azure virtual machine named VM1 and an Azure key vault named Vault1.

On VM1, you plan to configure Azure Disk Encryption to use a key encryption key (KEK).

You need to prepare Vault1 for Azure Disk Encryption.

Which two actions should you perform on Vault1? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Select Azure Virtual machines for deployment.

B. Create a new key.

C. Create a new secret.

D. Configure a key rotation policy.

E. Select Azure Disk Encryption for volume encryption.

Correct Answer: BE

Steps:

1.

Creating a resource group, if needed.

2.

Creating a key vault. (B)

3.

Setting key vault advanced access policies. (E)

Set key vault advanced access policies

The Azure platform needs access to the encryption keys or secrets in your key vault to make them available to the VM for booting and decrypting the volumes.

If you didn\\'t enable your key vault for disk encryption, deployment, or template deployment at the time of creation (as demonstrated in the previous step), you must update its advanced access policies.

1.

Select your key vault and go to Access Policies.

2.

Under "Enable Access to", select the box labeled Azure Disk Encryption for volume encryption. ((E))

3.

Select Azure Virtual Machines for deployment and/or Azure Resource Manager for template deployment, if needed.

4.

Click Save. https://learn.microsoft.com/en-us/azure/virtual-machines/windows/disk-encryption-key-vault?tabs=azure-portal

QUESTION 5

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while

others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have an Azure virtual machine named VM1 that runs Windows Server 2016.

You need to create an alert in Azure when more than two error events are logged to the System event log on VM1 within an hour.

Solution:

1.

You create an Azure Log Analytics workspace and configure the data settings.

2.

You install the Microsoft Monitoring Agent on VM1.

3.

You create an alert in Azure Monitor and specify the Log Analytics workspace as the source. Does this meet the goal?

A. Yes

B. No

Correct Answer: A

Alerts in Azure Monitor can identify important information in your Log Analytics repository.

They are created by alert rules that automatically run log searches at regular intervals, and if results of the log search match particular criteria, then an alert record is created and it can be configured to perform an automated response. The

Log Analytics agent collects monitoring data from the guest operating system and workloads of virtual machines in Azure, other cloud providers, and on-premises. It collects data into a Log Analytics workspace.

References:

https://docs.microsoft.com/en-us/azure/azure-monitor/learn/tutorial-response

https://docs.microsoft.com/en-us/azure/azure-monitor/platform/agents-overview