QUESTION 266
You have two Hyper-V hosts named Host1 and Host2. Host1 has an Azure virtual machine named VM1 that was deployed by using a custom Azure Resource Manager template.
You need to move VM1 to Host2.
What should you do?

A. From the Update management blade, click **Enable**.
B. From the Overview blade, move VM1 to a different subscription.
C. From the Redeploy blade, click **Redeploy**.
D. From the Profile blade, modify the usage location.

Answer: C
Explanation:
When you redeploy a VM, it moves the VM to a new node within the Azure infrastructure and then powers it back on, retaining all your configuration options and associated resources.
Reference:
https://docs.microsoft.com/en-us/azure/virtual-machines/windows/redeploy-to-new-node

QUESTION 267
Drag and Drop Question
Your company's on-premises network includes a Hyper-V host that hosts 10 virtual machines. The host and the virtual machines are running Windows Server 2016.
You have been tasked with making use of Azure Site Recovery to replicate the virtual machines. You have created a Recovery Services vault and a Hyper-V site.
You create a Recovery Services vault named ASR1 and a Hyper-V site named Site1.
You are now required to add the host to the Recovery Services vault.
Which of the following actions should you take, in sequence, to achieve your goal? Answer by dragging the correct option from the list to the answer area.

Options

Download the installation file for the Azure Site Recovery Provider.

Download the storage account key.

Download the vault registration key.

Install the Azure Site Recovery Provider on each virtual machine and register the virtual machines.

Install the Azure Site Recovery Provider on the host and register the server

Answer

Answer:

Options

Download the storage account key.

Install the Azure Site Recovery Provider on each virtual machine and register the virtual machines.

Answer

Download the installation file for the Azure Site Recovery Provider.

Download the vault registration key.

Install the Azure Site Recovery Provider on the host and register the server

Explanation:
https://docs.microsoft.com/en-us/azure/site-recovery/hyper-v-azure-tutorial

QUESTION 268
You are creating an Azure key vault using PowerShell. Objects deleted from the key vault must be kept for a set period of 90 days.
Which two of the following parameters must be used in conjunction to meet the requirement? (Choose two.)

A. `EnabledForDeployment`
B. `EnablePurgeProtection`
C. `EnabledForTemplateDeployment`

AZ-303 Exam Dumps AZ-303 Exam Questions   AZ-303 PDF Dumps   AZ-303 VCE Dumps

https://www.braindump2go.com/az-303.html

D. `EnableSoftDelete`

Answer: BD
Explanation:
https://docs.microsoft.com/en-us/powershell/module/azurerm.keyvault/new-azurermkeyvault
https://docs.microsoft.com/en-us/azure/key-vault/key-vault-ovw-soft-delete

QUESTION 269
You are developing an application to transfer data between on-premises file servers and Azure Blob storage. The application stores keys, secrets, and certificates in Azure Key Vault and makes use of the Azure Key Vault APIs.
You want to configure the application to allow recovery of an accidental deletion of the key vault or key vault objects for 90 days after deletion.
What should you do?

A. Run the `Add-AzKeyVaultKey` cmdlet.
B. Run the `az keyvault update --enable-soft-delete true --enable-purge-protection true` CLI.
C. Implement virtual network service endpoints for Azure Key Vault.
D. Run the `az keyvault update --enable-soft-delete false` CLI.

Answer: B
Explanation:
When soft-delete is enabled, resources marked as deleted resources are retained for a specified period (90 days by default). The service further provides a mechanism for recovering the deleted object, essentially undoing the deletion.
Purge protection is an optional Key Vault behavior and is not enabled by default. Purge protection can only be enabled once soft-delete is enabled.
When purge protection is on, a vault or an object in the deleted state cannot be purged until the retention period has passed. Soft-deleted vaults and objects can still be recovered, ensuring that the retention policy will be followed.
The default retention period is 90 days, but it is possible to set the retention policy interval to a value from 7 to 90 days through the Azure portal. Once the retention policy interval is set and saved it cannot be changed for that vault.
Reference:
https://docs.microsoft.com/en-us/azure/key-vault/general/overview-soft-delete

QUESTION 270
Drag and Drop Question
You have enabled multi-factor authentication for an administrator, who makes use of a web browser to access the Azure portal.
This allows for the administrator to use added security verifications when accessing the Azure portal.
Which of the following are the added security verifications that the administrator is able to use? Answer by dragging the correct option from the list to the answer area.

Options

Answer

An app password

An email message that contains a verification code

A text message that contains a verification code

A notification sent from the Microsoft Authenticator app

A notification or a verification code sent from the Microsoft Authenticator app

A text message that contains an app password

A phone call

Answer:

Options

An app password

An email message that contains a verification code

A notification sent from the Microsoft Authenticator app

A text message that contains an app password

Answer

A text message that contains a verification code

A notification or a verification code sent from the Microsoft Authenticator app

A phone call

Explanation:
https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-methods

QUESTION 271
Your network consists of physical and virtual servers located in a datacenter and a public cloud hosted on Microsoft Azure.
The Development department develops a custom application named CorpApp1. The application is hosted in Azure Cloud Services.
The developers release an updated version of CorpApp1.
You need to deploy the updated version of CorpApp1 to Azure cloud services to allow for testing.
You need to meet the following requirements:
- During testing, the current version of CorpApp1 must remain online.
- After testing, the new version must replace the current version as the live version with the minimum amount of downtime.
- When the new version is live, the old version must remain available for a period of time to be redeployed in the event of problems with the new version.
- The solution must minimize costs, administrative effort and application downtime.
Which of the following actions should you perform? (Choose all that apply.)

A. Deploy the new application to a new cloud service.
B. Deploy the new application to the production area.
C. Deploy the new application to the staging area.
D. Move the old version of the application to a new cloud service.
E. Move the new version of the application to the production area.

F.   Move the old version of the application to the staging area.
G.   Perform a Virtual IP swap.

Answer: CG
Explanation:
Once you have uploaded the compiled package to Azure Storage, you would create a new staging deployment. You can then provide the URL to the development team. Once approved, you would promote the new deployment to production by performing a VIP swap. You can then stop the instance of the old production deployment and keep it at hand in the staging slot.
Reference:
http://msdn.microsoft.com/en-us/library/ff803371.aspx

QUESTION 272
Your company has a web app named WebApp1.
You are making use of the WebJobs SDK to design a triggered App Service background task that automatically invokes a function in the code every time new data is received in a queue.
You are preparing to configure the service processes a queue data item.
Which of the following is the service you should use?

A.   Logic Apps
B.   WebJobs
C.   Flow
D.   Functions

Answer: B
Explanation:
https://docs.microsoft.com/en-us/azure/azure-functions/functions-compare-logic-apps-ms-flow-webjobs

QUESTION 273
Note: The question is included in a number of questions that depicts the identical set-up. However, every question has a distinctive result. Establish if the solution satisfies the requirements.
You are in the process of designing an Azure WebJob that supports remote debugging.
You want to make use of a suitable WebJob type.
Solution: You configure the use of the Continuous WebJob type.
Does the solution meet the goal?

A.   Yes
B.   No

Answer: A
Explanation:
https://docs.microsoft.com/en-us/azure/app-service/webjobs-create#webjob-types

QUESTION 274
Note: The question is included in a number of questions that depicts the identical set-up. However, every question has a distinctive result. Establish if the solution satisfies the requirements.
You are making use of Azure technologies to design a workflow solution.
You need to make sure that Visual Studio can be used to debug the solution.
Solution: You should make use of Logic Apps.
Does the solution meet the goal?

A.   Yes
B.   No

Answer: B

QUESTION 275

Drag and Drop Question
Your company has an Azure subscription that includes a number of Azure virtual machines, which are all part of the same virtual network.
Your company also has an on-premises Hyper-V server that hosts a virtual machine, named VM1, which must be replicated to Azure.
To achieve this, additional objects must be created in the Azure subscription.
Which of the following are the objects that must be created? Answer by dragging the correct option from the list to the answer area.

Options

Hyper-V site
Storage account
Azure Recovery Services Vault
Azure Traffic Manager instance
Replication policy
Endpoint

Answer

Answer:

Options

Answer

Hyper-V site

Storage account

Azure Recovery Services Vault

Replication policy

Azure Traffic Manager instance

Endpoint

QUESTION 276
You have an Azure subscription that contains a general purpose v2 storage account named storage1.
In storage1, you create a file share named share1.
You need to control access to share1 by using Azure role-based access control (Azure RBAC).
What should you do first?

A. Configure data protection for storage1
B. Generate a shared access signature (SAS) for storage1
C. Domain join storage1

Answer: C
Explanation:
Storage1 needs to be in the domain.
Note: To register your storage account with AD DS, create an account representing it in your AD DS. You can think of this process as if it were like creating an account representing an on-premises Windows file server in your AD DS.
When the feature is enabled on the storage account, it applies to all new and existing file shares in the account.
Reference:
https://docs.microsoft.com/en-us/azure/storage/files/storage-files-identity-ad-ds-enable

QUESTION 277
Hotspot Question
You have an Azure subscription that contains the resources shown in the following table.

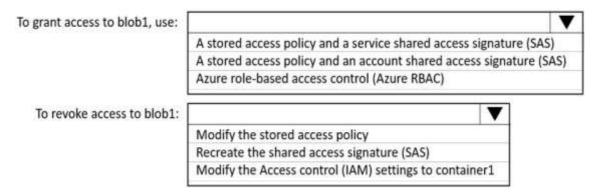| Name	Type
storage1	General purpose v2 storage account
container1	Blob container
blob1	Blob
blob2	Blob

AZ-303 Exam Dumps AZ-303 Exam Questions AZ-303 PDF Dumps AZ-303 VCE Dumps

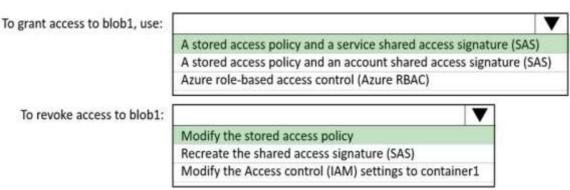**https://www.braindump2go.com/az-303.html**

You need to recommend an authorization mechanism for controlling access to blob1. The solution must ensure that access to blob1 can be configured without affecting the other resources in storage1.
What should you recommend? To answer, select the appropriate options in the answer area.

Answer Area

To grant access to blob1, use: ▼

A stored access policy and a service shared access signature (SAS)
A stored access policy and an account shared access signature (SAS)
Azure role-based access control (Azure RBAC)

To revoke access to blob1: ▼

Modify the stored access policy
Recreate the shared access signature (SAS)
Modify the Access control (IAM) settings to container1

Answer:

Answer Area

To grant access to blob1, use: ▼

A stored access policy and a service shared access signature (SAS)
A stored access policy and an account shared access signature (SAS)
Azure role-based access control (Azure RBAC)

To revoke access to blob1: ▼

Modify the stored access policy
Recreate the shared access signature (SAS)
Modify the Access control (IAM) settings to container1

Explanation:
Box 1: A stored access policy and a service shared access signature (SAS)
A stored access policy provides an additional level of control over service-level shared access signatures (SAS) on the server side. Establishing a stored access policy serves to group shared access signatures and to provide additional restrictions for signatures that are bound by the policy.
The following storage resources support stored access policies:
• Blob containers
• File shares
• Queues
• Tables
Box 2: Modify the stored access signature (SAS)
You can use a stored access policy to change the start time, expiry time, or permissions for a signature, or to revoke it after it has been issued.
Reference:
https://docs.microsoft.com/en-us/rest/api/storageservices/define-stored-access-policy